Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de “ donnée à caractère personnel ”

Julien Rossi

Par **Julien ROSSI**

Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de « donnée à caractère personnel »

Thèse présentée
pour l'obtention du grade
de Docteur de l'UTC

Soutenue le 2 juillet 2020
Spécialité : Sciences de l'Information et de la Communication et Science Politique : Unité de recherche COSTECH (EA-2223)
D2549

Université de technologie de Compiègne

École doctorale « Sciences de l'ingénieur »

Laboratoire COSTECH, EA 2223

Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de « donnée à caractère personnel »

Thèse de doctorat en
Sciences de l'information et de la communication et Science politique

Présentée par :

Julien Rossi

sous la direction de :

Virginie Julliard et Jérôme Valluy

Soutenue publiquement le 2 juillet 2020

Membres du jury :

Serge BOUCHARDON – Professeur des Universités à l'Université de Technologie de Compiègne

Isabelle GARCIN-MARROU – Professeure des Universités à Sciences Po Lyon

Gloria GONZÁLEZ FUSTER – Professeure de recherche à la Vrije Universteit Brussel

Virginie JULLIARD – Professeure des Universités à Sorbonne Université

Valérie SCHAFER – Professeure des Universités à l'Université du Luxembourg

Jérôme VALLUY – Maître de conférences HDR à l'Université Paris 1 Panthéon-Sorbonne, chercheur au COSTECH-UTC

Protection des données personnelles et droit à la vie privée

Enquête sur la notion controversée de
« donnée à caractère personnel »

Remerciements

Le « nous » académique choisi dans cette thèse n’est pas qu’une façon d’écrire un peu ampoulée et désuète. Il sert aussi à rappeler qu’un travail de recherche n’est jamais produit par le supposé génie d’un·e chercheur·e isolé·e, mais est, en réalité, le fruit d’un effort collectif auquel de nombreuses personnes contribuent.

Je tiens à commencer par Jérôme Valluy et Virginie Julliard, mes directeur et directrice de thèse. Je leur suis redevable de nombreux conseils avisés, de nombreuses relectures attentives, de nombreuses idées qui ont fait progresser ma réflexion.

Je remercie les membres du jury qui me font l’honneur de lire et commenter ce travail, d’autant qu’ils ont accepté ce travail supplémentaire en plein milieu d’une période particulièrement incertaine.

Cette thèse ne serait pas elle-même sans la thèse T.A.C., sans la découverte de la recherche technologique, et sans les moments de convivialité partagés au Minibar ou à la terrasse du bistrot en face de la gare de Compiègne. Le COSTECH, qui m’a financé, est un excellent endroit pour y faire sa thèse. Je remercie chaleureusement tou·te·s celles et ceux que j’y ai côtoyé·e·s : Charles, 春梅, Clément, Cléo, Édouard, Églantine, Gaëlle, Hugues, Isabel, Jean-Édouard, Karl, Manon, Nina, Peppe, Serge, Yann et tant d’autres. Je remercie en particulier Xavier Guchet, pour son travail de référent de l’école doctorale, sans oublier Christine Bry, pour sa disponibilité et l’impressionnante efficacité avec laquelle elle a répondu à toutes mes questions administratives.

Merci aussi à tant de collègues universitaires avec qui j’ai travaillé, qui m’ont soutenu, m’ont fait réfléchir, me rappeler que j’ai encore moult progrès à faire… Je n’ai pas l’espace d’être exhaustif, mais je pense en particulier à Francesca Musiani et aux autres membres du groupe « Gouvernance d’Internet » du GDR Internet, IA et Société. Je pense aussi à tous les collègues rencontrés à Bruxelles, et notamment celles et ceux du LSTS avec qui j’ai eu la chance de travailler.

Je voudrais adresser de chaleureux remerciements aux collègues du Département de communication de Rennes 2. Même si les étudiant·e·s y produisent assez de copies à corriger pour pouvoir nager dedans comme Picsou au milieu de ses billets de banque, je garderai de très bons souvenirs de ces années d’ATER et j’espère que nous nous reverrons quand cette histoire de virus sera derrière nous.

Merci aux projets ENEID et Sensibdata pour avoir contribué financièrement à mes travaux de recherche.

Je voudrais aussi exprimer ma gratitude envers toutes les personnes qui ont accepté, gratuitement, de me donner du temps, pour un entretien, pour un conseil, pour m’aider à accéder à des informations, ou encore pour compléter un questionnaire.

Il ne faudrait pas oublier toutes celles et ceux qui sans qui il n’y aurait même pas eu de projet de thèse. Je dois des remerciements tout d’abord à Jean-Jacques Lavenue, qui fut mon directeur de mémoire à Sciences Po Lille. C’est lui qui m’a fait tomber dans la marmite de la protection des données. Je remercie aussi Clément Fontan. Sans ses conseils je n’aurais probablement jamais réussi à faire aboutir mon projet.

Je n’oublie pas non plus le soutien que Gloria Origgi et Iván Székely m’ont apporté au moment décisif de chercher des financements pour la thèse.

Je dois aussi des remerciements à Attila Péterfalvi, Júlia Sziklay, et tous les collègues de l’Autorité nationale pour la protection des données et la liberté de l’information de Hongrie, qui m’ont beaucoup apporté et qui ont continué à me soutenir pendant la thèse. Je voudrais aussi saluer mes anciens collègues de la CNIL et du Centre des hautes études du Ministère de l’intérieur. J’ai beaucoup appris à leur contact.

Ces pages de remerciements seraient incomplètes si elles ne mentionnaient pas les collègues et ami·e·s de l’Université de Szeged, qui m’ont fait découvrir et aimer le métier d’enseignant-chercheur l’année avant le début de la thèse : Péter Kruzslicz, Laureline Congnard, Souleymane N’Diaye, Andrea Gyivicsán, Tünde Silay et Attila Badó.

Merci aussi à mes proches pour m’avoir soutenu et supporté pendant toute la durée de la thèse.

Il va sans dire que cette thèse n’aurait pas existé sans mes parents. Ils m’ont soutenu, pas seulement dans mes études, mais dans tout le reste.

Merci à Alda, Camille, Grégoire, Kaja, Lune, Marine, Mélanie, Nebiha, Sergio et Souleymane pour vos relectures et vos aides pour certaines traductions. Merci à Guillaume pour toutes ces journées passées à écrire des scripts en Python. Merci enfin à Mélanie de m’avoir tant soutenu et aidé dans le sprint final de la fin de thèse, et de m’avoir offert un refuge fleuri loin de l’enfer de mon studio parisien pendant le confinement. Enfin, puisqu’une page de remerciements sur la protection des données à caractère personnel ne serait pas complète sans un peu de chiffrement : Yahou ! Dru ! Pogolin ! Kneu !

Enfin, je ne peux conclure les remerciements d’une thèse qui porte sur la protection des données, de la vie privée, et plus largement des droits humains, sans remercier celles et ceux qui se sont battu·e·s et continuent à se battre pour les défendre. Merci à vous.

Résumé

La menace qu'Internet et les technologies numériques de l'information et de la communication en général font ou feraient peser sur la vie privée soulève de nombreux débats, tant dans la presse qu'au niveau politique. L'affaire Snowden en 2013, puis l'adoption en 2016 du Règlement général de protection des données (RGPD), ont renforcé la visibilité de ces controverses dans l'espace public.

Cette thèse part d'une triple interrogation : pouvons-nous définir ce qu'est la « vie privée », existe-t-il un consensus autour de la question, et ce consensus évolue-t-il avec des évolutions de notre milieu technique qui affectent nos modes de communication, et donc d'intrusion dans celle-ci ?

En définissant la « vie privée » comme l'objet protégé par des textes normatifs – textes de loi, jurisprudence et standards techno-politiques d'Internet – qui protègent le droit *à la* vie privée, il est possible d'en étudier empiriquement l'évolution et les controverses qui l'accompagnent.

Le droit de la protection des données à caractère personnel a émergé en Europe dans les années 1970 pour protéger une « vie privée » perçue comme menacée par une informatique encore à ses débuts. Aujourd'hui, le RGPD, ou encore certains documents édictés par des organismes de standardisation comme l'Internet Engineering Task Force (IETF) ou le World Wide Web Consortium (W3C), visent à protéger cette vie privée au travers d'un corpus de règles, la « protection des données », qui concerne les « données à caractère personnel ».

Les définitions juridiques de cette notion produites dans des arènes institutionnelles et celles produites dans des arènes de standardisation technique sont identiques. L'étude de la généalogie de la protection des données révèle en outre le rôle déterminant d'informaticiens dans l'invention de la « protection des données » et en particulier des principes qui régissent aujourd'hui encore les dispositions contenues dans le RGPD.

L'analyse des controverses qui ont eu lieu dans les arènes d'élaboration de ces normes montre que la notion de « donnée à caractère personnel » inscrite dans les textes de notre corpus reflète essentiellement le système de convictions d'une coalition d'acteurs inspirés par des idéaux libéraux utilitaristes, attachés à l'autonomie de l'individu et accordant de l'importance au respect de son consentement. Ce paradigme s'est imposé dans les arènes étudiées face à d'autres conceptions de la « vie privée », notamment celles qui la définissent comme un espace collectivement défini ôté au regard de l'espace public, ou encore celles qui préconisent une patrimonialisation de ces données.

Ce n'est donc pas l'informatique qui a directement déterminé une évolution dans l'objet de la protection du droit de la vie privée, mais ses perceptions par un groupe d'acteurs. Convaincus de l'utilité sociale de la protection de leur conception libérale de la vie privée, ces derniers sont parvenus à faire émerger, en Europe, dans les années 1970, une nouvelle catégorie juridique : le

droit à la protection des données. Le RGPD, adopté en 2016, tout comme les projets de standards du Web visant à protéger la vie privée et étudiés dans cette thèse, reprennent les principes issus de ces premiers débats. Ce faisant, l'arrivée de l'informatique a, indirectement mais effectivement, été un élément déclencheur dans l'évolution de la « vie privée » définie comme objet du droit à la vie privée.

Mots-clefs : informatisation de la communication, vie privée, protection des données, données à caractère personnel, approches communicationnelles du droit et des politiques publiques

English summary

Internet and digital information and communication technologies in general are often portrayed as a threat to privacy. This gives rise to many debates, both in the media and among decision-makers. The Snowden revelations, in 2013, followed by the adoption in 2016 of the General Data Protection Regulation (GDPR), have moved these discussions under the spotlight of the public sphere.

The research presented in this dissertation was born out of three questions: can we define what "privacy" is? Is there any consensus on its definition? And does this consensus change with the evolution of the technical milieu transforming our ways of communicating, and by doing so, the way in which our privacy can be intruded upon?

By defining "privacy" as the object which is protected by normative texts – laws, court decisions, techno-political standards of the Internet – protecting the right to privacy, it becomes possible to conduct an empirical study of how it evolved and how it has been a topic of contention.

Data protection law emerged in Europe during the 1970's. Its aim was to protect a "privacy" that was perceived as under threat by the advent of computers. Currently, the GDPR, or some documents adopted by standards-settings organisations like the Internet Engineering Task Force (IETF) or the World Wide Web Consortium (W3C), are written with the intention that they protect this privacy through a set of rules and principles referred to as "data protection", that apply to "personal data".

The legal definitions of this notion produced by political institutions and those crafted in standards-settings bodies are identical. Furthermore, the study of the genealogy of data protection reveals that computer scientists have played a pivotal role in the invention of the principles that "data protection" still relies on, for instance in the GDPR.

The analysis of the controversies that took place in the shaping of these rules shows that the notion of "personal data" written down in the normative texts we analysed essentially reflects the beliefs system of a coalition inspired by liberal utilitarian ideals, valuing individual autonomy and granting importance to the respect of one's consent. This framing of "privacy" has become

the paradigm on the field. Other theories, such as those defining “privacy” as a space bound by collectively defined borders protecting it from the public eye, or those advocating the recognition of private property rights on personal data, have been less successful in shaping policy outcomes.

The advent and spread of networked computers have not directly determined the evolution of the object that is protected by the right to privacy. It is, rather, the perceptions a group of actors had of computers, that caused such an evolution. Convinced that their liberal conception of privacy is socially valuable, they managed to craft a new legal category during the 1970’s in Europe: the right to the protection of personal data. The GDPR, adopted in 2016, just like Web standards aiming at enhancing the protection of privacy, rely those same principles that were invented during these early debates. Therefore, it can be said that the emergence of computers has indeed, but indirectly, been a triggering factor in the evolution of “privacy” defined as the object protected by the right to privacy.

Keywords : digitisation of communication, privacy, data protection, personal data, communicational theories of Law and public policy

Table des matières

Table des abréviations

A… à H…	
AB	Advisory Board (W3C)
AC	Advisory Committee (W3C)
ACCIS	Association of Consumer Credit Information Suppliers
ACF	Advocacy Coalition Framework
ACM	Association for Computer Machinery
ACT	Association for Competitive Technology
AEPD	Agencia Española de Protectión de Datos
AFCDP	Association française des correspondants à la protection des données à caractère personnel
AFPA	Agence nationale pour la formation professionnelle des adultes (France)
AGLOSO	Attorney General's List of Subversive Organizations
AmCham EU	American Chamber of Commerce to the European Union
ANSSI	Agence nationale de la sécurité des systèmes d'information (France)
API	Application Programming Interface
ASNEF	Asociación Nacional de Establecimientos Financieros de Crédito
ATI	Agence tunisienne de l'Internet
BCS	British Computer Society

I… à W…	
IAB	Interactive Advertisement Bureau
IAPP	International Association of Privacy Professionals
IBM	International Business Machines Corporation
ICANN	Internet Corporation for Assigned Names and Numbers
ICCP	Comité de la politique de l'information, de l'informatique et des communications (OCDE)
ICDP	Industry Coalition for Data Protection
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICO	Information Commissioner's Office
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMCO	Commission du marché intérieur et de la protection des consommateurs du Parlement européen
INRIA	Institut national de recherche en informatique et en automatique
INSEE	Institut national de la statistique et des études économiques
INWG	International Network Working Group
IP	Internet Protocol
IPv4	IP version 4

BEUC	Bureau européen des unions de consommateurs
BSA	Business Software Alliance
C. Cass.	Cour de Cassation (France)
CAEM	Comité d’assistance économique mutuelle
CCJ	Comité de coopération juridique du Conseil de l’Europe
CDT	Center for Democracy and Technology
CECA	Communauté européenne du charbon et de l’acier
CECIL	Centre d'Études sur la Citoyenneté, l'Informatisation et les Libertés
CEDH	Cour européenne des droits de l’Homme
CEE	Communauté économique européenne
CEPD	Comité européen de la protection des données
CERN	Centre européen de recherche nucléaire
CFDT	Confédération française démocratique du travail
CJCE	Cour de justice des Communautés européennes
CJUE	Cour de justice de l’Union européenne (ex-CJCE)
CLODO	Comité de libération et de détournements d’ordinateurs
CNIL	Commission nationale de l’informatique et des libertés (France)
COINTELPRO	Counter INTelligence PROgram
Convention EDH	Convention de sauvegarde des droits de l’Homme et des libertés

IPv6	IP version 6
IRC	Internet Relay Chat
ISFE	Interactive Software Federation of Europe
ISO	Organisation internationale de normalisation
ISOC	Internet Society
JAI	Justice et affaires intérieures
JBCE	Japan Business Council in Europe
JOCE	Journal officiel des Communautés européennes
JSON	JavaScript Object Notation
LIBE	Commission des libertés civiles, de la justice et des affaires intérieures
NCP	Network Control Protocol
NDA	Note de l’auteur
NDT	Note de traduction
NDT	Note de tradution
NIR	Numéro d’inscription au répertoire des personnes physiques
NIS	Network and Information Systems
NOYB	None Of Your Business
NSA	National Security Agency (États-Unis d’Amérique)
NTIA	National Telecommunications and Information Administration

	fondamentales
CPDP	Computers, Privacy and Data Protection (conférence)
CSV	Comma-Separated Values
CUG	Computer Utilization Group de l'OCDE
CWV	Comité Waakzaamheid Volkstelling
DAPIX	Groupe « échange d'informations et protection des données » (Conseil de l'UE)
DARPA	Defense Advanced Research Projects Agency
DG	Direction générale
DG JUST	Direction générale de la justice et des consommateurs (Commission européenne)
DNS	Domain Name System
DNT	Do Not Track
DPD	Délégués à la protection des données
DSK	Datenschutzkomision (Autriche)
DSTI	Direction de la science, de la technologie et de l'innovation (OCDE)
DUDH	Déclaration universelle des droits de l'Homme
EDPB	European Data Protection Board (voir : CEPD)
EDPS	European Data Protection Supervisor (Contrôleur européen de la protection des données)
EDRi	European Digital Rights
EFF	Electronic Frontier Foundation

	(États-Unis d'Amérique)
NWG	Network Working Group
OASIS	Organization for the Advancement of Structured Information Standards
OCDE	Organisation de coopération et de développement économiques
OECE	Organisation européenne de coopération économique
ONG	Organisation non gouvernementale
OPA	Online Publishers Association
OSI	Open Systems Interconnection
P3P	Platform for Privacy Preferences
PIB	Produit intérieur brut
PII	Personnally Identifiable Information
PING	Privacy Interest Group (du W3C)
PME	Petites et moyennes entreprises
PRISM	Nom de code d'un projet de surveillance de la NSA
RFA	République fédérale d'Allemagne
RFC	Request for Comments
RFID	Radio-frequency identification
RGPD	Règlement général de protection des données
SAFARI	Système automatisé pour les fichiers administratifs et le répertoire des individus

EMOTA	European Multi-channel and Online Trade Association
EPC	European Publishers Council
EPIC	Electronic Privacy Information Center
Euratom	Communauté européenne de l'énergie atomique
euroISPA	Europe Internet Service Providers Association
F2F	Face-to-face Meetings (W3C)
FBI	Federal Bureau of Investigation
FECEMD	Federación de Comercio Electrónico y Marketing Directo
FEDMA	Federation of European Direct and Interactive Marketing
FPF	Future of Privacy Forum
FTC	Federal Trade Commission
G29	Groupe de travail de l'Article 29
GAFA	Google Amazon Facebook Apple
GAMIN	Gestion automatisée de médecine infantile
HEW	Health, Education and Welfare
HRPC	Human Rights Protocol Considerations (IRTF)
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
HUAC	House Committee on Un-American Activities

SIS	Système d'information Schengen
SPT	Comité de la politique scientifique et technologique (OCDE)
SSRC	Social Science Research Council
TAG	Technical Architecture Group (W3C)
TCE	Traité instituant la Communauté européenne
TCP	Transmission Control Protocol
TFUE	Traité sur le fonctionnement de l'Union européenne
TIC	Techniques (ou technologies) de l'information et de la communication
TPAC	Technical Plenary and Advisory Committee (W3C)
TPE	Tracking Preference Expression
TPS	Tracking Compliance and Scope
TPWG	Tracking Protection Working Group (du W3C)
TUE	Traité sur l'Union européenne
UE	Union européenne
UNIVAC	UNIVersal Automatic Computer
URL	Uniform Resource Locator
URSS	Union des républiques socialistes soviétiques
W3C	World Wide Web Consortium
WFA	World Federation of Advertisers
WHATWG	Web Hypertext Application Technology Working Group

Table des tableaux et illustrations

Suite de la table des illustrations

Introduction générale

> *« Les Français vont […] vivre dans une civilisation de l'information. La recherche de l'information devient une activité rentable, sa détention une source de puissance. Le renseignement qui lui sert de matière première est dorénavant recherché ; une pression croissante s'exerce pour que soient recueillies des données nouvelles, dont la veille encore il aurait été techniquement et financièrement inconcevable d'envisager l'utilisation. L'information circule, empruntant de nouveaux circuits »* (Conseil d'État (France), 1970, p. 5)

> « *Difficile […] pour les adolescents de ne pas trop exposer leur vie privée sur les réseaux. Nombre d'entre eux n'hésitent pas à dévoiler des photos d'eux (88%) sur leur profil, leur adresse mail (68%), s'ils sont célibataires ou non (58%), leur adresse postale (27%). Une impudeur d'autant plus préjudiciable qu'un ado compte en moyenne 210 amis sur Facebook et que 31% des sondés avouent avoir accepté dans leurs contacts des personnes qu'ils n'avaient jamais rencontrées.* » (Bancaud, 2011, non paginé, dans le journal *20 Minutes*)

Les craintes suscitées par la diffusion de l'Internet pour la vie privée ne datent pas d'hier. Les plus anciens fournisseurs d'accès à Internet (FAI) français remontent au milieu des années 1990. Dès septembre 1998, *Le Monde Diplomatique* publiait un article de Mathieu O'Neil intitulé « Internet, ou la fin de la vie privée » (O'Neil, 1998). Loin de disparaître, ces craintes semblent s'être intensifiées. En 2011, Alex Türk, alors président de la Commission nationale informatique et libertés (CNIL) française publiait un livre sous le titre de : « La vie privée en péril » (Türk, 2011). En 2012, un journaliste du *Guardian* titrait l'un de ses articles : « La fin de la vie privée en ligne ?[1] » (Arthur, 2012). Selon un sondage réalisé par BVA en France en 2018, « qu'il s'agisse de leurs coordonnées personnelles (numéros de téléphone, adresse ...) (78 %) ou de leurs documents privés (photos, vidéos …) (67 %), la majorité des Français se montrent inquiets quant à la protection de leur vie privée sur Internet » (BVA, 2018, p. 3). Nous pourrions multiplier de

1 Traduction de l'auteur. Texte original : « The end of online privacy? »

Note sur les traductions :
Lorsqu'une traduction a été faite par nos soins, cela sera indiqué comme ici en note de bas de page. Les autres traductions ont été réalisées par une traductrice professionnelle, Camille Thompson, puis relues et corrigées par l'auteur. Les quelques exceptions – notamment pour les traductions depuis l'allemand – sont également précisées.
Le travail d'analyse a toujours porté sur le texte original, et jamais sur des traductions, sauf pour les langues autres que le français, l'anglais, le néerlandais, l'espagnol, l'italien, le hongrois ou, selon le niveau de difficulté, l'allemand. Les traductions sont données à titre indicatif et sont insérées dans le corps du texte pour faciliter la lecture.

tels exemples. Les révélations d'Edward Snowden, en 2013, sur les programmes de surveillance secrets de la *National Security Agency* (NSA) des États-Unis d'Amérique, auxquels de grandes entreprises multinationales comme Facebook et Microsoft ont participé (Greenwald, 2013 ; Lyon, 2015), ne sont pas étrangères au renforcement de ces craintes et de leur visibilité médiatique et politique accrue.

La figure de *Big Brother* dans *1984* de George Orwell (1949) continue à être une métaphore socialement répandue de la surveillance. Des *Big Brother Awards* sont régulièrement décernés à des entreprises ou à des personnalités accusées par des associations d'avoir particulièrement contribué au renforcement de dispositifs de surveillance[2]. Des films comme *Minority Report* en 2002, tiré d'une nouvelle de Philip K. Dick (1956), ou encore nombre d'épisodes de la série *Black Mirror*, montrent que la question de la surveillance continue à inspirer les réalisateurs. Cette inspiration se retrouve également dans d'autres domaines artistiques. L'exposition financée par l'*Open Society Foundation* et intitulée « *Watching You, Watching Me* » a parcouru plusieurs pays dont les États-Unis, la Hongrie, la Belgique et l'Allemagne depuis 2014[3].

À l'âge de l'« hyper-affichage de soi » (Carré et Panico, 2012), la crainte de l'érosion ou de la disparation de la vie privée est partagée par de nombreux chercheurs, comme Susan B. Barnes, qui s'inquiétait dans un article de 2006 du fait que les adolescents dévoilent leur vie privée sur des réseaux sociaux comme Facebook (Barnes, 2006). Une partie non négligeable de ces craintes se concentre sur les enfants et les adolescents, qui seraient imprudents et vivraient dans un contexte d'extinction de la vie privée :

> « La masse de millions de données personnelles dévoilées en public [sur les réseaux sociaux] aboutit à fortement fragiliser la vie privée dans le monde entier pour des générations entières, et en particulier pour les jeunes[4]. » (Sziklay, 2016, p. 57)

D'autres travaux de recherche ont mis en évidence un « paradoxe de la vie privée » ou « *privacy paradox* » dans les comportements en ligne (Acquisti et Gross, 2006 ; Acquisti, Ida et Rochelandet, 2011 ; Estienne, 2011 ; Martin-Juchat et Pierre, 2011 ; Norberg, Home et Home, 2007). Les personnes observées au cours de ces travaux manifestaient un comportement de divulgation de soi en contradiction apparente avec la valeur qu'ils affirmaient accorder à la vie privée. Du point de vue de l'analyse économique, les internautes n'agissent donc pas en consommateurs rationnels sur le marché de la vie privée (Rochelandet, 2010). Il y aurait une

2 Voir la liste de toutes les cérémonies de remise de ces « prix » à travers le monde sur : http://www.bigbrotherawards.org/ (page consultée le 28 juillet 2019).

3 Voir par exemple sur le site du *Staatliche Museum zu Berlin* : https://www.smb.museum/en/exhibitions/detail/watching-you-watching-me-a-photographic-response-to-surveillance.html (page consultée le 28 juillet 2019).

4 Traduction de l'auteur. Texte original : « A milliós nagyságrendben nyilvánosságra hozott személyes adatok tömege egyrészt igen sérülékeny magánszférát eredményez globális mértékben meghatározott teljes – elsősorban fiatal – generációk vonatkozásában. »

baisse de l'intériorisation des normes de la pudeur, une perte de contrôle informationnel (voir : Klein, 2012) que les entreprises du « Web 2.0 », dont Facebook (boyd, 2010), favoriseraient pour des raisons d'intérêt commercial (Fuchs, 2012). Nous assistons parfois de la part de leurs dirigeants à des discours hostiles à la vie privée, présentée comme dépassée, désuète. Mark Zuckerberg a pu ainsi affirmer, prenant acte du comportement des utilisateurs inscrits sur Facebook, que la vie privée en tant que norme sociale avait disparu (Johnson, 2010). D'autres, comme Vint Cerf, *Chief Internet Evangelist* chez Google, ont exprimé l'opinion selon laquelle la vie privée serait une anomalie historique (Cerf, 2013).

La littérature académique fournit quelques facteurs d'explication au « paradoxe de la vie privée ». Il s'explique par exemple par les services et bénéfices souvent sans contrepartie financière attendus en échange du partage d'informations (Gerber, Gerber et Volkamer, 2018). D'autres pointent du doigt l'absence de choix réel dont bénéficient les individus qui « consentent » à utiliser des services en ligne les dépossédant de leur « vie privée », malgré l'importance qu'ils y accordent, et parlent de « consentement résigné » (Hémont et Gout, à paraître). Un part grandissante de la littérature s'intéresse aux phénomènes de manipulation qui visent à extorquer une forme de consentement des utilisateurs à partager des informations qui les concernent (Gray et al., 2018 ; Susser, Roessler et Nissenbaum, 2018). D'autres encore ont montré que l'augmentation progressive de la pression de la surveillance dans les démocraties libérales érodait la résilience de la vie privée comme valeur sociale bien mieux que l'instauration brutale d'une surveillance policière, comme il en survint en Europe centrale et orientale dans la deuxième moitié des années 1940 (voir : Jones, Raab et Székely, 2018 ; Raab, Jones et Székely, 2015).

Notre questionnement s'inscrit lui aussi dans une tentative de compréhension de ce paradoxe, et commence par l'interrogation suivante : **de quelle « vie privée » parle-t-on lorsque l'on parle de paradoxe de la « vie privée » ?** Bien qu'il y ait des exceptions, nombre de travaux académiques éludent la question de la définition de la vie privée. Ce concept échapperait d'ailleurs selon certains « par essence » à toute tentative sérieuse de définition, ou à tout le moins de consensus sur sa définition (Mulligan, Koopman et Doty, 2016).

La question est loin d'être triviale. Est-ce vraiment la « vie privée » qui *disparaît*, ou bien assistons-nous, de façon corrélée à la diffusion de l'informatique, à une *transformation* de cette « vie privée » et de notre rapport individuel comme collectif à cet objet, qu'à ce stade de l'introduction nous n'arrivons pas encore à définir ? Lorsque des chercheurs font une enquête sur le sentiment des individus sur leur « vie privée », et « l'importance » qu'ils leur accordent, tous évoquent-ils bien la même chose ? Ou bien projettent-ils sur eux leurs propres définitions ? Et si cela pouvait aussi contribuer à expliquer le paradoxe de la vie privée ?

À ce sujet, il convient dès à présent de préciser la terminologie qui nous accompagnera tout au long de ce mémoire de thèse.

Nous utilisons le terme « vie privée » comme synonyme du mot anglais « *privacy* », et ce malgré les nuances qui existent (discutées dans : Rey, 2012) entre les deux termes. En français, la « vie privée » peut désigner l'intimité, la sphère privée, mais aussi être synonyme de « vie personnelle » en opposition à la « vie publique » comme à la « vie professionnelle », par exemple[5]. En anglais, le mot « *privacy* » est d'abord lié à l'idée d'intimité, du *lieu* où se déroule la vie personnelle d'une personne en dehors du regard de l'autre, de confidentialité. Bénédicte Rey (2009) préfère ainsi directement parler de « *privacy* à l'heure du numérique » et non de « vie privée à l'heure du numérique » dans une thèse par ailleurs rédigée en français. D'autres préfèrent utiliser le néologisme « privacité » (Latzko-Toth et Pastinelli, 2014). Nous avons préféré garder le terme de « vie privée » et l'utiliser de façon interchangeable avec celui de « *privacy* » pour deux raisons. La première est que la difficulté à les définir l'un comme l'autre fait que, selon le point de vue adopté, ils peuvent avoir une aire d'intersection sémantique telle que nous pouvons dans de nombreux cas les considérer comme synonymes. La deuxième est que leurs sens contemporains se sont calqués l'un sur l'autre, car lors de la traduction de textes juridiques internationaux de référence, « *privacy* » traduit désormais le français « vie privée », et vice-versa (González Fuster, 2014a). Pour nos terrains, où le droit joue un rôle prépondérant, et pour nos corpus de discours d'acteurs, pour la plupart d'entre eux en anglais, la différence entre « *privacy* » et « vie privée » est marginale. Nous n'avons donc pas voulu compliquer la lecture inutilement en cherchant à différencier les deux termes.

Une autre précision importante est que nous utiliserons le terme de « vie privée » par opposition à « vie publique », et non par opposition à « vie professionnelle », que nous opposerons à « vie personnelle ». Cette « vie privée » « est de fait un comportement plutôt qu'un état » (Rey, 2012, paragr. 20). Elle est constituée par un ensemble de comportements en réaction à un sentiment d'intrusion (Rey, 2012, paragr. 20). Cette définition ne nous dit rien sur les circonstances dans lesquelles de telles réactions ont lieu, ni sur la façon dont elles parviennent à constituer cet « espace » (matériel ou symbolique) ôté à l'œil du public, et sur les limites d'un tel espace. Elle fournit toutefois une première base utile à la construction de notre objet de recherche.

Enfin, nous ferons toute au long de ce mémoire une distinction entre « vie privée », « droit *à la* vie privée » et « droit *de la* vie privée ». La « vie privée » est cette chose polysémique à la définition contestée que nous n'arrivons pas encore à cerner, mais qui semble pour l'instant s'opposer à la « vie publique », et dont nous admettons qu'elle traduise – à quelques nuances près – la notion en anglais de « *privacy* ». Le « droit *à la* vie privée » est le droit fondamental qui

5 Ainsi, lorsque Hannah Arendt oppose la « vie privée » (de l'espace domestique) à la « vie publique », elle n'oppose pas l'intime au non-intime, mais la part de la vie active consacrée à soi dans l'espace domestique à la part de la vie consacrée au travail dans la Cité. Dans *The Human Condition* (titre original de *La condition de l'Homme moderne*), elle ne parle donc pas de « *privacy* » mais de « *private life* » (voir : Arendt, 1998 [1958], p. 29).

octroie aux individus le droit *à* cette chose. De la même façon, il existe par exemple dans la Déclaration universelle des droits de l'Homme (DUDH) de 1948 un « droit *à la* liberté d'expression » (art. 18), ou un « droit *à la* liberté de pensée, de conscience et de religion » (art. 19). Mais le « droit *à la* vie privée » est une déclaration de principe, là où le « droit *de la* vie privée » correspond au corpus de règles juridiques et de procédures précises qui encadrent la façon dont les individus peuvent exercer le « droit *à la* vie privée ». Concrètement, il peut par exemple s'agir de textes dans des lois, des règlements, des décisions de justice faisant jurisprudence, ou encore, dans certaines juridictions, de règles coutumières.

Nous avons vu que la « vie privée » était perçue comme menacée par la diffusion de certaines pratiques en ligne, d'Internet, et plus largement, des technologies numériques de l'information et de la communication. Il convient maintenant de nous pencher sur le rapport entre « vie privée » et milieu technique.

Vie privée et milieu technique

Les objets techniques sont souvent présentés comme déontologiquement neutres, et les décisions techniques comme apolitiques. Ce genre de présentation est critiquable, et sert souvent à dissimuler des enjeux de pouvoir ou une responsabilité politique. Marie Goupy (2014) a par exemple montré dans son étude qu'après la destitution de Ben Ali en Tunisie, les dirigeants de l'Agence tunisienne de l'Internet (ATI) ont développé une stratégie de communication visant à souligner l'absence de responsabilité de ses ingénieurs dans la surveillance policière d'Internet, l'ATI ne faisant, selon les mots de son directeur M. Chakchouk, « pas de politique[6] ». Cette présentation est démentie par le fait que cette agence ait mis en place, à la demande du pouvoir politique, les moyens techniques ayant facilité et permis le travail de services de renseignement tunisiens (Goupy, 2014). La neutralité sociale et politique de la technologie est bien un leurre.

L'on ne peut pas dire que les objets techniques soient pour autant des « acteurs » politiques, car leur reconnaître une intentionnalité serait tomber dans un excès inverse. Ils contribuent plutôt à façonner les relations de pouvoir entre individus. Agir sur eux, transformer leur configuration matérielle, est une façon de « faire de la politique » (Akrich, 1993 ; Lavelle, 2009 ; Winner, 1980). Il serait aussi faux de dire, comme l'ont fait Karl Marx et Friedrich Engels, que « l'infrastructure » matérielle *détermine* la « superstructure » idéologique et sociale (Engels, 1978 [1872] ; Marx, 2002 [1859]). À ce titre, nous souscrivons à la critique du marxisme classique d'auteurs comme Antonio Gramsci et Cornelius Castoriadis qui réhabilitent le rôle de l'idéologie, et des imaginaires sociaux en général, dans la compréhension des chaînes de causalité historiques (Castoriadis, 2006 [1975] ; Gramsci, 2018 [1948]). De nombreuses études en sociologie ont d'ailleurs montré que s'il existait une relation de dépendance à la technique, la

6 Entretien réalisé par Marie Goupy le 25 juin 2013 et cité dans son article « La bienveillante neutralité des technologies d'espionnage des communications : le cas tunisien » (Goupy, 2014).

technique n'en était pas moins une activité humaine, et donc l'infrastructure matérielle de la société est le produit de cette dernière (Bijker, 1995 ; Dupuy, 1982 ; Jauréguiberry et Proulx, 2011 ; Lenert, 2004).

Nous souscrivons largement à la thèse selon laquelle le milieu technique dans lequel évoluent les individus contribue à les « constituer » (Steiner, 2010). La technique est ambivalente en ce qu'elle permet d'agir tout en « arraisonnant » les conditions d'action futures (Bachimont, 2010). Elle ne *détermine* donc certes pas, mais elle joue un rôle dans la constitution tant des sociétés que des subjectivités. Cela, par exemple, Jack Goody l'a montré en expliquant le rôle qu'avait eu l'écriture dans l'avènement de la « raison graphique » (Goody, 1979). Nous ajouterons qu'elle joue aussi un rôle politique indirect à travers les réactions que ses représentations dans des imaginaires sociaux suscitent. Le récit de la genèse du droit *à la* protection des données à caractère personnel l'illustrera : ce droit n'est pas la conséquence directe, nécessaire, mécanique ou téléologique de transformations dans le milieu technique en général et les techniques de l'information et de la communication (TIC) en particulier.

Nous ne nous appesantirons ici pas d'avantage sur les théories cherchant à étudier la relation entre l'être humain et son milieu technique, et préférons renvoyer le lecteur vers les quelques références que nous venons de citer et sur lesquelles nous nous appuyons. Ce détour théorique général nous a toutefois paru nécessaire pour justifier de prendre au sérieux la proposition suivante : **le milieu technique – et donc son évolution – joue un rôle dans la constitution de la « vie privée »**. D'ailleurs, de nombreux auteurs ont montré comment des évolutions par exemple dans l'architecture des habitats et des villes avaient contribué à faire évoluer le rapport à la « vie privée » (Guerrand, 1987 ; Habermas, 1988 [1962] ; Mumford, 1938 ; Prost, 1987 ; Riehl, 1889). L'invention de la chambre à coucher individuelle n'est par exemple absolument pas anecdotique pour comprendre l'évolution historique du concept et des pratiques qu'il désigne. Elle est corrélative à la constitution, selon Jürgen Habermas, d'une séparation entre « espace public » et « espace privé » (Habermas, 1988, p. 55). L'évolution du téléphone offre un autre exemple pour aider à comprendre le rapport entre « vie privée » et milieu technique. Alors qu'au début, le téléphone, fixe, était partagé par un groupe – familial, souvent même villageois ou de quartier – et offrait une intimité d'autant plus limitée aux interlocuteurs que les salariées qui opéraient les connexions dans les centraux téléphoniques pouvaient écouter la conversation (Julliard, 2004), le téléphone portable individuel est devenu un objet intime que l'on protège par mot de passe, voire par des dispositifs biométriques.

Ces quelques exemples illustrent ainsi comment le milieu technique donne ou non des possibilités de réaction à des individus ou des groupes ressentant un sentiment d'intrusion.

En 1890, des juristes états-uniens s'étaient inquiétés de l'impact d'évolutions techniques dans le domaine de la photographie et de la presse sur la possibilité de garantir un droit *à la* vie privée aux individus :

> « Des inventions et méthodes commerciales récentes attirent l'attention sur la prochaine étape qui devra intervenir pour la protection des personnes et pour assurer à l'individu ce que le Juge Cooley appelle le droit d'« être laissé tranquille »[7] » (Warren et Brandeis, 1890, p. 195)

De nombreux travaux, de diverses natures, montrent que la diffusion de technologies numériques transforment en profondeur notre milieu technique, au point d'être qualifiée par certains de nouveau « paradigme » socio-technique (Castells, 1998 ; Freeman, 1988 ; Kranzberg, 1985). Ce nouvel ensemble de techniques est une condition nécessaire aux transformations du capitalisme contemporain. Faisant suite au capitalisme industriel, le capitalisme informationnel (Castells, 1998), ou capitalisme cognitif (Moulier Boutang, 2007), est fondé sur une nouvelle étape d'accumulation primitive poursuivant la grande transformation capitalistique initialement décrite par Károly Polányi (2009 [1944]), par la marchandisation de l'information. Ces dernières années, des travaux portant sur « la grande conversion numérique » (Doueihi, 2008), la « numérisation générale de la société » (George, 2019), ou encore la « culture numérique » (Cardon, 2019) montrent l'existence de nombreuses ramifications sur le plan culturel de la diffusion de l'informatique.

Vu l'abondance de cette littérature, il est loin d'être absurde de faire l'hypothèse que la diffusion de l'informatique, qui transforme radicalement notre milieu technique, fasse évoluer les conditions d'exercice de la « vie privée ». Cela est d'autant plus vrai que la littérature académique dont nous disposons démontre la grande utilité de l'utilisation de l'ordinateur et de l'informatique en réseaux à des fins de surveillance, et vient ainsi restreindre la capacité des individus à se retirer du regard d'autrui dans un espace protégé. Ce qui, sauf à ce que leurs normes en matière de « vie privée » évoluent ou disparaissent, peut provoquer, selon la perspective que nous avons adoptée, un sentiment d'intrusion auquel il devient de plus en plus difficile de réagir étant donné les évolutions des contraintes du milieu technique. Ces évolutions normatives, par exemple au sujet du droit *à la* vie privée, ne découlent toutefois pas automatiquement de l'évolution technique, mais de la rencontre entre cette dernière et des perceptions, des valeurs, des imaginaires qui provoquent des réactions sociales à leur encontre.

7 Traduction de l'auteur. Texte original : « Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". ».

Traces numérique et surveillance

La surveillance est une relation dans laquelle une personne en observe une autre, qui peut ou non se savoir observée. Pour Roger Clarke, la surveillance se définit comme « la fouille ou l'observation systématiques des communications et actions d'une ou plusieurs personnes » (Clarke, 1988).

La surveillance n’est pas née avec l’informatique (Mattelart, 2007 ; Rios-Bordes, 2018 ; Vitalis et Mattelart, 2014). Elle s’est toutefois révélée être un important domaine d’application des technologies numériques. Elles en ont profondément transformé les modalités (Agre, 1994) mais aussi l’ampleur, si bien que nous vivons aujourd’hui dans une « société de la surveillance » (Lyon, 2015). Cette surveillance informatisée repose sur l’exploitation de « traces numériques » inscrites sur les supports numériques.

Nous assistons à la démultiplication des points de capture de ces « traces numériques ». Chaque passage d'une carte de transport contenant une puce RFID, chaque visite sur un site web, chaque transaction par carte bancaire, laissent des traces enregistrées sur un support informatisé. Même le simple fait de marcher dans la rue entraîne de plus en plus souvent l'inscription d'une trace visuelle numérique dans des dispositifs de vidéosurveillance.

Les « traces numériques » sont « ces inscriptions qui doublent toujours les activités ayant lieu dans des environnements informatisés parce que ces activités sont des interactions avec des machines computationnelles » (Collomb, 2016, p. 16). Elles sont chargées de fortes attentes de la part d'acteurs économiques mais aussi dans le domaine de la recherche en sciences humaines et sociales. Comme le rappelle Cléo Collomb dans sa thèse : « les traces numériques portent […] les promesses d’un accès supposément direct au social voire au réel […] comme le laissent entendre certains discours qui accompagnent le développement des digital humanities ou du big data » (Collomb, 2016, p. 14). Grâce à la quantité de données disponibles, il deviendrait possible de renverser l'*apriorisme* méthodologique déductif (Mill, 1882) et de répondre au problème de Hume qui démontre l'impossibilité d'un raisonnement inductif (Hume, 2000 [1748]). En effet, la quantité massive de données disponibles sur le monde social, grâce à la capture de ces traces numériques, permettrait pour la première fois dans l'histoire de l'humanité d'induire des corrélations vraies tout en se passant d'hypothèses préalables. Il deviendrait possible de faire de la science sans modèle, sur un corpus tendant à l'exhaustivité des interactions sociales (Anderson, 2008). Ces projets épistémologiques font l’objet de nombreuses critiques, qui portent notamment sur le fait que l’indiciarité et l’exhaustivité supposées des traces numériques est un leurre, mais aussi sur la confusion que ces projets opèrent entre corrélation et causalité (voir notamment : Bigot, 2018 ; Bottini et Julliard, 2017 ; Bourdeloie, 2014 ; Boyadjian, 2014, 2016 ; Dijck, 2014 ;

Jeanneret, 2011 ; Schmitt, 2015). Ces critiques n'empêchent pas la naissance de projets fondés sur ce « paradigme dataïste » (van Dijck, 2014), qui rendent les traces numériques particulièrement intéressantes pour des applications en matière de surveillance.

Sur le plan matériel, toute trace est une « donnée » en informatique, c'est-à-dire une série de signes discrets binaires qui se manifestent par des variations de courant électrique entre 0V (pour figurer le 0) et 5V (pour figurer le 1). Par souci de simplicité, étant donné que la présente étude n'a pas pour objet les notions de « trace » et de « donnée », et parce que la notion de trace est finalement une catégorie non-spécifique, floue et difficilement opérationnelle (Jeanneret, 2011), nous considérerons sauf indication ponctuelle du contraire que les deux mots sont synonymes en tous points, à la nuance près que la « trace » peut connoter une intention ou une possibilité de traçage et de surveillance absente du terme de « donnée ».

Les traces numériques peuvent être des inscriptions intentionnelles comme non-intentionnelles, et ces dernières peuvent former ou enrichir des « profils » réalisés sur les individus. Deleuze définissait sa notion de « dividu » comme la substitution des corps par une matière « dividuelle » numérique à contrôler, témoin du passage d'une société de discipline à une société de contrôle (Deleuze, 1990). Ce dividu est l'individu éclaté à travers les traces qu'il laisse. Mais ces traces permettent également de reconstituer le portrait d'une personne, d'un « Homme-Trace », pour utiliser la terminologie de Béatrice Galinon-Mélénec (2011).

Les techniques numériques de l'information et de la communication se caractérisent entre autres par l'augmentation considérable de la capacité de stockage d'informations par rapport à tout autre support, leur relative durabilité, un coût de duplication de l'information très inférieur à son coût de production (Rochelandet, 2010), l'efficacité de l'indexation et de la recherche automatisée d'informations indexées, la facilité avec laquelle il est possible de croiser des fichiers, et la possibilité de communiquer rapidement, à faible coût, sur de grandes distances. Cela a rendu possible l'émergence de nouveaux modèles économiques autour de l'exploitation de ces données, notamment à partir des années 2000 et l'avènement du modèle économique du « Web 2.0 » (Fuchs, 2012 ; O'Reilly, 2007).

Le « *Big Data* », défini comme le traitement véloce de volumes massifs et variés (hétérogènes) de données numériques (Laney, 2001), est souvent présenté comme « la prochaine frontière de l'innovation, de la compétition et de la productivité[8] » (Manyika et al., 2011). En 2011, le cabinet McKinsey publiait un rapport estimant qu'il serait possible d'augmenter les marges du commerce de détail de 60 % grâce au Big Data et que la « le système de santé des États-Unis pourrait utiliser le Big Data de façon créative et efficace pour améliorer l'efficience et

8 Traduction de l'auteur. Texte original : « The next frontier for innovation, competition and productivity ».

la qualité des services. Nous estimons que la valeur potentielle des données produites par le secteur pourrait dépasser les 300 milliards de dollars US par an[9] » (Manyika et al., 2011, p. 2).

Des entreprises, comme Google ou Facebook, ont choisi de monétiser les données sur leurs visiteurs ou utilisateurs à travers la constitution de profils publicitaires vendus aux annonceurs (Cecere, Guel et Rochelandet, 2015). Certaines entreprises, comme Google ou Facebook, collectent directement ces données. D'autres, comme de nombreux journaux en ligne, insèrent sur les pages web des éléments permettant à des sociétés tierces qui les rémunèrent de tracer leurs visiteurs et de leur proposer de la publicité ciblée. Une étude publiée en 2013 sur les 197 sites les plus visités en France a montré qu'il y avait une corrélation positive entre le niveau d'intrusion des sites et leur performance économique (Cecere et Rochelandet, 2013).

Le programme PRISM de la NSA, révélé par Edward Snowden en 2013, a montré que les données auxquelles contribuent les internautes dans les bases de données privées d'entreprises comme Facebook ou Apple alimentent celles d'agences de renseignement étatiques comme la NSA (Lyon, 2015, p. 71). La surveillance n'est ni l'apanage de l'État ni celui de grandes entreprises. Elle est, ainsi que Didier Bigo la qualifie, diagonale, c'est-à-dire mêlant à de la surveillance verticale des éléments de surveillance, horizontale, entre pairs (Bigo, 2014). Penser une barrière absolue entre surveillance par des acteurs publics ou privés est donc illusoire dans le contexte du « capitalisme de la surveillance » (Zuboff, 2018) contemporain.

Roger Clarke, définit la « *dataveillance* », ou surveillance par les données, comme « l'usage systématique de données à caractère personnel dans l'enquête sur les actions de communication d'une ou plusieurs personnelles ou leur surveillance[10] » (Clarke, 1988). À partir de la collecte de données de masse, des algorithmes sont utilisés pour cibler des profils « à risque » qui font dès lors l'objet d'une surveillance renforcée. Une telle action peut être automatisée (en tout ou partie) à partir d'un profil calculé sur la base de traces éparses recombinées. Il est également possible de reconstituer des informations manquantes par traitement automatique de données. Par exemple, des chercheurs britanniques ont développé une méthode qu'ils présentent comme fiable pour identifier l'âge des utilisateurs de Twitter (Sloan et al., 2015). Enfin, l'intérêt du croisement de données à des fins de surveillance réside dans la possibilité de ré-identifier des individus à partir de « quasi-identifiants » tels que l'âge ou le code postal de résidence (Ohm, 2010 ; Sweeney, 2000), les données de paiement même sans le nom du détenteur du moyen de paiement (de Montjoye et al., 2015) ou encore un jeu de requêtes sur un moteur de recherche appartenant à une même personne dont le nom est inconnu (Barbaro et

9 Traduction de l'auteur. Texte original : « if US health care could use big data creatively and effectively to drive efficiency and quality, we estimate that the potential value from data in the sector could be more than $300 billion in value every year ».

10 Traduction de l'auteur. Texte original : « the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons ».

Zeller, 2006). Les similarités statistiques dans l'usage de la langue entre deux corpus de textes écrits par la même personne sous deux pseudonymes différents est également une technique mise en œuvre dans le cadre d'enquêtes de police (Ránki, 2011).

La *dataveillance* permet que « l'humain [soit] abstraitement « démembré » en flux de données disparates qui s'amalgament pour créer un hybride fonctionnel inscrit dans des processus globaux de surveillance » (Mondoux, 2011, p. 49). Comme le rappelle David Lyon, elle est aussi « un moyen de tri social[11] » (Lyon, 2015, p. 113), la surveillance servant à opérer des discriminations au sein du corps social, par exemple en séparant les personnes jugées dignes de confiance à qui une banque peut octroyer un crédit des autres, ou les personnes à qui une société souhaite adresser une publicité ciblée en particulier, des autres.

Droit *à la* vie privée, droit *à la* protection des données à caractère personnel

De nombreuses revendications ont émergé face au sentiment d'intrusion généré par le capitalisme de la surveillance (Zuboff, 2018) et par le phénomène de *dataveillance* que nous venons de décrire. Nous verrons comment ces revendications liant informatique, surveillance et intrusion dans la sphère privée ont été problématisées, d'abord aux États-Unis puis en Europe, à partir des années 1960[12], et ce à partir d'une lecture inspirée essentiellement par des conceptions de philosophie morale libérales utilitaristes[13].

Les controverses médiatiques sur la vie privée et l'informatique ont repris de l'ampleur au cours des années 2000, avec l'adoption de lois augmentant les pouvoirs des services de renseignement après les attentats du 11 septembre, les révélations d'Edward Snowden, puis les nombreux scandales autour de la façon dont des entreprises privées dans le domaine du numérique exploitent les données personnelles de ses utilisateurs. C'est dans ce contexte que circulent des discours médiatiques et politiques sur la revendication d'un « droit à l'oubli » comme solution à la situation d'« effondrement des contextes » d'énonciation des messages et informations à caractère privé (Walczak, 2014, p. 71-72). Ces discours fournissent des outils rhétoriques dans le cadre d'une forme de négociation collective de fait entre des entreprises comme Facebook et Google et leurs utilisateurs (Casilli, 2013 ; Walczak, 2014). Peuvent également se développer des pratiques de « résistance » ou de « résilience » (Raab, Jones et Székely, 2015) face aux pratiques de *dataveillance* de masse, comme la destruction de téléphones portables par des réfugiés au passage de frontières (Jones, Raab et Székely, 2018, p. 15) ou

11 Traduction de l'auteur. Texte original : « a means of social sorting ».
12 Cf. chapitre 5
13 Cf. chapitre 2

encore l'emploi de logiciels de chiffrement des communications par les internautes russes en réaction à la surveillance accrue de l'Internet par le gouvernement (Ermoshina et Musiani, 2017).

Pour répondre aux préoccupations que ces controverses et pratiques manifestent, le Parlement européen et le Conseil de l'Union européen ont adopté en 2016 un règlement et une directive visant à « protéger les données à caractère personnel » : il s'agit d'une Règlement général de protection des données[14] (RGPD) et d'une directive applicable au secteur spécifique de la justice et des enquêtes pénales[15]. Nous nous concentrerons sur le premier, car il fournit le cadre général du droit *de la* protection des données, là où le second texte est une adaptation du premier texte à un domaine spécifique.

Le RGPD a été conçu comme une réaction politique et collective à ce qui était perçu comme un phénomène d'intrusion dans la vie privée de la part à la fois d'entreprises et de services de renseignement étatiques. Ainsi, pour Jan Philipp Albrecht, rapporteur au Parlement européen du projet de Règlement général de protection des données (dossier 2012-011 (COD)) :

> « Pendant des années, les principales sociétés d'Internet dans la Silicon Valley ont contourné leurs obligations de protection des données et généré ainsi de substantiels profits […]. Une activité de lobbying à grande échelle permet aux géants de l'Internet de bloquer toute forme de réglementation aux États-Unis et dans l'Union européenne. […] Au regard des révélations sur la surveillance à grande échelle par les services de renseignement des États-Unis, la question de la mise en œuvre de la protection des données, de l'auto-détermination informationnelle et de la vie privée à l'âge numérique se pose à nouveau. La seule réponse qui peut y être donnée prend la forme de l'adoption par l'Union européenne d'un Règlement général de protection des données robuste[16] » (Albrecht, 2015a, p. 184-186)

14 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

15 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

16 Traduction de l'auteur. Texte original : « […] for years now, the major Internet companies in Silicon Valley have been circumventing data protection obligations and are generating substantial profilts as a result […]. As a result of large-scale lobbying activity, the internet giants are able to block any form of regulation in the USA or the EU. […] In view of the revelations of large-scale surveillance by the US secret service, the question once again arises regarding the implementation of data protection, informational self-determination and privacy in the digital era. The answer to this can only take the form of a strong Data Protection Regulation issued by the EU. »

Selon ce discours, le RGPD devait garantir le droit *à la* « vie privée ». D'autres instruments ont un but identique. C'est le cas des *Privacy Enhancing Technologies* (PET's) (Bennett et Raab, 2003, p. 139-159), au rang desquels certains projets du *World Wide Web Consortium* (W3C), comme le *Do Not Track* (DNT), sur lequel nous reviendrons.

Aujourd'hui, il devient difficile de repérer des discours s'opposant ouvertement à la protection de la « vie privée ». Même le discours institutionnel de Facebook et de Google s'affiche, avec des exceptions médiatisées déjà évoquées, favorable à « la vie privée ». Dans sa lettre du 25 avril 2012, Facebook affirme : « la vie privée est le cœur de tout ce que nous faisons chez Facebook et il y a trois principes directeurs guidant notre programme de vie privée : la transparence, le contrôle et l'imputabilité (« *accountability* »)[17] » (Corpus Lobbyplag, FACEBOOK1, 2012, p. 1).

La « vie privée » (« *privacy* ») évoquée dans cette courte citation d'un document de lobbying de Facebook est-elle celle dont parle Jan Philipp Albrecht, rapporteur du Règlement général de protection des données et eurodéputé écologiste de *Die Grünen* ? Lorsqu'ils parlent de « vie privée », Mark Zuckerberg (Clifford, 2018), patron de Facebook, et, par exemple, Isabelle Falque-Pierrotin (Falque-Pierrotin, 2009), présidente de la CNIL jusqu'en 2019, parlent-ils de la même chose ? En parlent-ils pour les mêmes raisons, leur accordent-ils la même valeur ? Quelles sont les conséquences des systèmes de conviction des acteurs impliqués dans l'élaboration de textes comme le RGPD dans les dispositions concrètes qui y sont rédigées ?

Comme le rappelle la critique féministe de la vie privée (Allen, 1988 ; Decew, 2015 ; MacKinnon, 1989), le droit *à la* « vie privée » était un argument juridique recevable pour acquitter les auteurs de violences domestiques comme le viol conjugal. En France, cet argument était jugé recevable jusqu'à un arrêt de la Cour de Cassation de 1992[18]. En Russie, la Douma a adopté une loi pour dépénaliser les violences conjugales au nom du respect de la « vie privée ».

17 Traduction de l'auteur. Texte original : « Privacy is at the core of everything that we do on Facebook and there are three main principles guiding our privacy programme: transparency, control and accountability ».

18 Cour de cassation, Ch. Crim. du 11 juin 1992.
Dans l'affaire ayant conduit à ce revirement de jurisprudence, une femme avait porté plainte pour viol contre son mari. Le juge d'instruction refusa d'instruire le dossier en avançant l'argument que les actes sexuels commis contre le gré de l'épouse « entraient dans le cadre du mariage tel qu'il est traditionnellement admis » (C. Cass. 11 juin 1992). La chambre d'accusation avait suivi cet avis en énonçant « qu'à juste titre, le juge d'instruction a estimé que le mariage a pour effet de légitimer les rapports sexuels et que l'épouse ne peut invoquer son absence de consentement ou l'agressivité qui a accompagné des actes sexuels normaux pour soutenir avoir été victime de viols » (C. Cass. 11 juin 1992). La victime dut se pourvoir en cassation pour que la Cour de cassation rappelle que « en confirmant par ces motifs l'ordonnance de refus d'informer du juge d'instruction, alors que la présomption de consentement des époux aux actes sexuels accomplis dans l'intimité de la vie conjugale ne vaut que jusqu'à preuve contraire, la chambre d'accusation a méconnu le sens et la portée de l'article 332 du Code pénal » (C. Cass. 11 juin 1992).
En 1984 (C. Cass. Ch. Crim. 17 juillet 1984), la Cour de Cassation avait déjà ouvert la possibilité de porter plainte pour viol contre son conjoint ou sa conjointe uniquement à des époux en instance de divorce.

Promulguée le 7 février 2017 par le président Vladimir Poutine (AFP, 2017), cette mesure était défendue par le député Andreï Issaïev avec l'argument que « «c'est un vote historique car, dans certains pays, le rôle de l'Etat dans la vie familiale dépasse toutes les bornes » (Mandraud, 2017). Est-ce cette « vie privée » que défendent d'une même voix la CNIL, le rapporteur du RGPD, et la communication actuelle de la société Facebook ? Il serait absurde de le supposer, et de fait, ce n'est pas le cas. Mais ce raisonnement par l'absurde doit nous convaincre qu'il existe bel et bien plusieurs conceptions, parfois opposées, de la « vie privée », qu'un consensus pour celle-ci peut en réalité masquer.

Alors, de quelle vie privée, et de quel droit *à la «* vie privée », parle-t-on ? Est-il même possible de donner une définition de la « vie privée » commune à toutes ses acceptions ?

De nombreuses tentatives ont été réalisées pour parvenir à une définition théorique et une description du contenu de la notion de « vie privée », dans l'espoir qu'elles puissent faire consensus (voir par exemple : Westin, 1970, Allen, 2000, 1988, p. 1177 ; Clarke, 2006 ; Finn, Wright et Friedewald, 2013). Pour Bert-Jaap Koops *et al.* (Koops et al., 2016, p. 503) ces tentatives sont confuses car elles confondent l'objet de ce que le droit *à la* vie privée protège, et le droit *à la* vie privée lui-même. Bert-Jaap Koops *et al.* établissent donc comme nous une différence entre le termes « *privacy* » et « *right to privacy* », c'est-à-dire entre « vie privée » et « droit *à la* vie privée ». Sur cette base, leur projet a consisté à étudier ce que le droit constitutionnel de neuf pays protégeait : les États-Unis, le Royaume-Uni, le Canada, les Pays-Bas, l'Allemagne, l'Italie, la République tchèque et la Slovénie. Le résultat de leurs travaux a été résumé dans le schéma suivant :

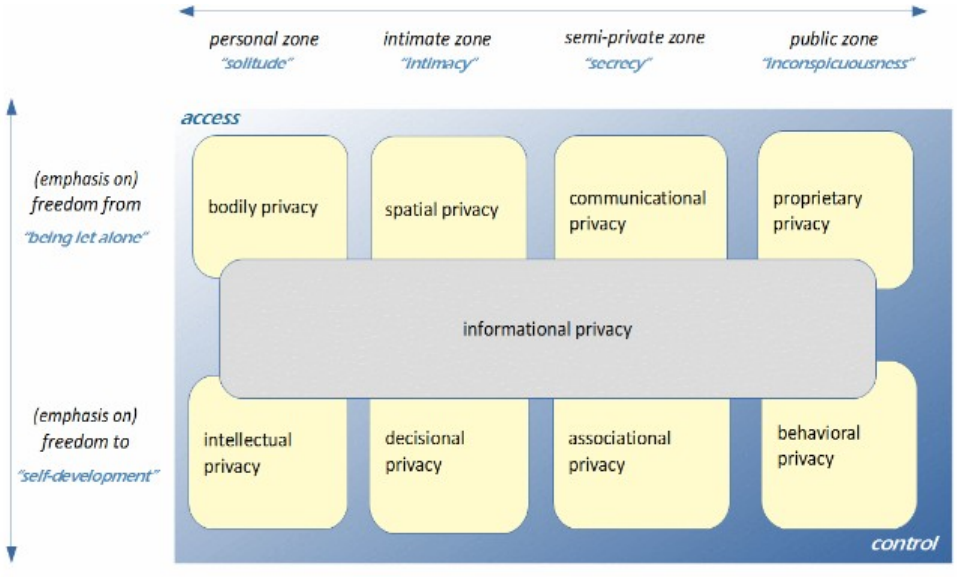


Figure 1 : *Définition de la « vie privée » sous forme de schéma. Schéma extrait de Koops et al., 2016, p. 484*

Ce schéma identifie plusieurs sphères imbriquées où s'exerce la protection juridique de la vie privée : la sphère de la personne, de l'intime, du semi-privé, et de l'espace public. Certaines lois insistent sur des éléments, pour reprendre la terminologie d'Isaiah Berlin (1969), de liberté négative : le droit à être laissé tranquille, tant par l'État que par des personnes privées physiques ou morales. D'autres dispositions juridiques insistent sur le droit à l'autonomie et au développement de soi, dans une optique de liberté positive : il s'agit de la liberté d'affirmer ses propres choix, et si besoin, d'y être aidé par la puissance publique. L'infraction au droit *à la* vie privée vient qualifier dans certains cas un accès non-souhaité à la personne (y compris un accès physique), et dans d'autres cas, un contrôle exercé de façon illégitime sur le comportement de cette personne. La vie privée informationnelle, qui recouvre peu ou prou ce que désigne la protection des données, traverse l'ensemble de ces dimensions.

Ces travaux, pour utiles et pertinents qu'ils soient, n'ont pour objet que de constater quel est, en l'état actuel du droit, l'objet de la protection du droit *de la* vie privée. Ils n'ont pas cherché à étudier s'il existait des visions politiques concurrentes de cet objet, ou de la valeur, de la justification morale, de ce droit. Étant une synthèse d'une étude comparée de l'état du droit dans quelques pays à une date donnée, ils ne prennent en compte ni les évolutions socio-historiques de cet objet, ni la façon dont ce dernier interagit avec un milieu technique en mutation.

Or, le droit à la vie privée est l'objet de discussions, de débats, de controverses entre des représentations sociales et discours politiques concurrents. Le schéma reproduit un peu plus haut

de Bert-Jaap Koops *et al*. (2016), ou l'étude par Bénédicte Rey de la « privacy » à l'ère du numérique (Rey, 2009), admettent une continuité conceptuelle entre le droit à la vie privée tel qu'il avait pensé par la doctrine de *Common Law* à la fin du XIX^{e} siècle aux États-Unis (Warren et Brandeis, 1890), sans interroger cette hypothèse.

La controverse médiatique en France de 2018 sur la création de droits de propriété cessibles sur les données personnelles, défendue par Grégoire Koenig et le think-tank Génération Libre (Schmitt et Madelaine, 2018), mais combattue par Isabelle Falque-Pierrotin, présidente de la CNIL (Cherif, 2018), illustre là encore l'absence de consensus, y compris entre des personnes qui prennent publiquement position en faveur du « droit à la vie privée ». Il existe de fait des systèmes de conviction concurrents qui s'affrontent pour influencer la production des normes de droit positif et des standards techniques rédigés dans l'optique de protéger la vie privée en contexte numérique.

Gardons également à l'esprit que les efforts de définition que nous venons d'évoquer s'intéressent à la « vie privée » et au droit *à la* vie privée, mais pas au droit *à la* protection des données à caractère personnel. Or, nous observons que, juridiquement, ces deux droits sont pourtant distincts, du moins dans le droit de l'Union européenne, et dans les conceptions d'un grand nombre d'acteurs des terrains que nous avons étudiés.

Il existe deux articles différents fondant deux libertés fondamentales distinctes dans la Charte des droits fondamentaux de l'Union européenne. Selon l'article 7 de celle-ci :

> « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications »

Et selon l'article 8 de la même Charte :

> « 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
>
> 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
>
> 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

Cette différence est-elle une différence lexicale ou implique-t-elle une vraie différence sémantique ? La Convention européenne des droits de l'Homme (Convention EDH), elle, ne connaît que le droit à la vie privée, auquel la Cour européenne des droits de l'Homme (CEDH) rattache le droit *de la* protection des données à caractère personnel[19].

Dans l'affaire « Tele2 Sverige », la Cour d'Appel (*Court of Appeals*) d'Angleterre et du Pays-de-Galles avait demandé à la Cour de justice de l'Union européenne (CJUE) de dire si une décision précédente étendait « la portée des articles 7 et/ou 8 de la Charte au-delà de celle de l'article 8 de la Convention EDH, telle qu'établie par la jurisprudence de la Cour européenne des droits de l'homme ? » (CJUE 21 décembre 2016 « Tele2 Sverige », pt. 59). En répondant à la question posée, la CJUE aurait pu clarifier la relation entre les articles 7 et 8 de la Charte, et entre ces deux articles et l'article 8 de la Convention EDH. Mais elle évite de répondre à cette question difficile en se déclarant incompétente (en droit) pour le faire :

> « La seconde question posée par la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile), Royaume-Uni] est irrecevable » (CJUE 21 décembre 2016 « Tele2 Sverige », dispositif)

Le droit *de la* protection des données à caractère personnel procède juridiquement à la fois du droit à la vie privée (art. 7 de la Charte) et du droit *à la* protection des données à caractère personnel (art. 8 de la Charte). Mais il n'existe pas, à l'heure actuelle, de réponse ayant autorité de la chose jugée à la question sur la relation entre droit *à la* protection des données et droit *à la* vie privée.

La distinction entre ces deux catégories juridiques est particulièrement importante pour Roger Clarke, qui dénonce la confusion entre « droit *à la* vie privée » et « droit *à la* protection des données à caractère personnel » qui régnerait selon lui aux États-Unis et en Australie : « Le terme de « vie privée » a été sérieusement corrompu dans les lois états-uniennes et australiennes qui l'ont confondu avec la notion très restrictive de « protection des données » »[20] (Clarke, 2006 [non paginé]).

Gloria González Fuster souligne elle aussi la différence entre ces deux droits, et critique l'ambiguïté de la délimitation entre eux dans la jurisprudence de la CJUE :

> « La lecture attentive de la jurisprudence de la CJUE sur les droits à la protection des données et à la vie privée révèle non seulement des incohérences et des faiblesses, mais

19 Voir notamment : CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pt. 103

20 Traduction de l'auteur. Texte original : « A serious debasement of the term 'privacy' has occurred in the case of U.S. and Australian statutes that have equated it with the highly restrictive idea of 'data protection'. »

de façon plus générale un manque de rigueur dans la délimitation exacte des contours de chacun de ces droits, de leurs substances, et de la relation (qui fluctue de façon apparemment aléatoire) entre eux[21] » (González Fuster, 2014b, p. 277-278)

Pour Mélanie Clément-Fontaine, au contraire, tant la jurisprudence de la CJUE que celle des tribunaux français consacrent de façon constante un « lient étroit » entre les droits *à la* vie privée et *à la* protection des données à caractère personnel. Cela n'empêche pas ce dernier d'avoir acquis une forme d'autonomie vis-à-vis du premier, qui invite à les distinguer. Toutefois, le droit *de la* protection des données à caractère personnel, qui est la catégorie dont fait partie par exemple le RGPD ou la directive 95/46/CE qui l'a précédé, doit être compris comme appliquant tant le droit *à la* protection des données que le droit *à la* vie privée (Clément-Fontaine, 2017).

Une interrogation se présente à ce stade de la réflexion : **qu'est-ce que le « droit *à la* protection des données à caractère personnel » ? Quel est son rapport avec le « droit *à la* vie privée » ? Quelle est l'origine de cette nouvelle catégorie de droit ? Quel est son objet ?**

Cette interrogation se rajoute aux interrogations que nous avons déjà formulées sur l'objet précis de la protection de ces droits (comme définissant la « vie privée ») et sur les systèmes de conviction qui ont motivé et expliquent les choix rédactionnels des auteurs des textes normatifs visant à garantir ces droits. Notre intuition, à ce stade, est que la compréhension fine de l'objet de la protection de textes comme le RGPD nous permettra de mieux comprendre la relation concrète qui lie (ou distingue) droit *à la* vie privée et *à la* protection des données à caractère personnel. Nous nous interrogerons notamment sur le rapport que peut entretenir cette distinction avec l'évolution du milieu technique qui découle de l'informatisation, et de réactions politico-juridiques cadrées par sa perception.

Le droit saisi par une approche communicationnelle

Chercher à répondre aux interrogations que nous venons de formuler nous incite à adopter une approche communicationnelle du droit. Cette approche rappelle que le droit est un instrument parmi d'autres des politiques publiques (Lascoumes, 2004 ; Lascoumes et Le Galès, 2005). Au même titre qu'un objet ou une infrastructure technique (Akrich, 1993 ; Lavelle, 2009 ; Rossi, 2017a ; Winner, 1980) il participe à l'exercice d'un pouvoir politique. Une disposition juridique

21 Traduction de l'auteur. Texte original : « The careful review of the case law of the EU Court of Justice on the rights to personal data protection and to privacy reveals not only inconsistencies and weaknesses, but more generally a lack of rigour in delimiting clearly the contours of each right, their substance, and the (seemingly randomly fluctuating) relations between them. »

et un artefact – objet technique (Simondon, 1958) ou infrastructure (Epstein, Katzenbach et Musiani, 2016 ; Massit-Folléa, 2014 ; Musiani et al., 2016) – ne sont pas identiques sur le plan matériel, ni sur le plan de leurs mécanismes d'action et d'interaction sur la société, mais ils produisent tous deux des effets de pouvoir et de régulation des comportements humains.

Matériellement, les textes juridiques sont faits d'énoncés performatifs (Austin, 1970 [1962] ; Laugier, 2004 ; Reinach, 2004 [1913]). Ils ne cherchent pas à décrire le réel mais à agir dessus, à le transformer. Ces énoncés ont pour dimension matérielle un contenu (au sens de : Bachimont, 2010) fait d'inscriptions scripturales faisant l'objet d'une circulation médiatique. Le contrôle sur les supports légitimes de communication du droit, comme les journaux officiels, est l'objet de luttes de pouvoir. Un législateur qui ne contrôle pas la publication du droit se retrouve dominé par l'institution détenant ce contrôle (voir : Gougeon, 1995). Enfin, comme tout contenu médiatique, le droit fait l'objet d'opérations de codage et de décodage (Hall, 1994 [1973]).

À l'étape de « codage », c'est-à-dire au moment de la production, les rédacteurs sont motivés par des systèmes de conviction et de représentations sociales rivales (Müller, 2000), par des intérêts qu'ils perçoivent et construisent à travers ces premiers, et finissent par adopter des compromis permettant de réunir les conditions d'adoption formelle (majorité, unanimité, consensus …) conférant à un texte sa légitimité et le faisant entrer dans le droit positif[22]. Par sa publication, ses auteurs produisent une forme de communication institutionnelle qui s'insère dans des logiques de communication publique (Ollivier-Yaniv, 2018). Ses mots ont, comme tout objet linguistique, une fonction référentielle (Jakobson, 1963). Ils font référence à la fois à un ensemble de connaissances juridiques, mais aussi à ces systèmes de conviction et de représentation de leurs auteurs. Or ces derniers ne sont pas forcément partagés par le public des politiques publiques dont un texte juridique est l'instrument. Les individus qui les lisent interprètent les signifiants qu'ils trouvent et « décodent », s'approprient les textes en fonction de leurs propres connaissances, valeurs et convictions (Ollivier-Yaniv, 2018 ; Revillard, 2018). Enfin, une partie du public d'un texte de Loi se réfère à des interprétations de tiers – journalistes, avocats, consultants, connaissances perçues comme plus « expertes » – qui jouent dans le processus de réception des politiques publiques un rôle analogue aux « leaders d'opinion » décrits par (Katz et Lazarsfeld, 2008 [1955]).

Une définition classique du droit considère qu'il s'agit de toute norme écrite assortie d'une sanction qu'une autorité investie du monopole de la violence légitime est capable de faire appliquer. Mais, sans même aborder la question du droit non-écrit, qu'en est-il par exemple des lois qui ne s'accompagnent pas de sanctions ? Aucun mécanisme international de sanction n'existe pour sanctionner les infractions des États à la Déclaration universelle des droits de l'Homme. Est-ce à dire que ce n'est pas du droit ?

22 L'étude de la rivalité de discours et systèmes de convictions dans la production de politiques publiques, dont le droit est un instrument, sera présentée dans la section sur la méthodologie.

Notre position est qu'il existe en dehors du droit « dur », de nombreux textes de droit appelés « souple » ou « flexible » (Carbonnier, 2001 ; Cazala, 2011) (« *hard law* / *soft law* » en anglais). Ces textes prétendent produire des effets normatifs et réguler les comportements humains. Ils ont eux aussi une vocation performative. Mais, qu'ils soient ou non de source publique, ils ne font pas nécessairement partie du corpus de textes sur lesquels un juge peut se fonder pour appliquer une sanction.

Dans le domaine de la gouvernance d'Internet – que nous définirons dans le chapitre 5 – nous pouvons distinguer d'une part la régulation par le code informatique (Lessig, 1999 et 2000) et d'autre part, la régulation par des conventions sociales écrites sur la façon dont les matériels et logiciels informatiques doivent être conçus et paramétrés pour communiquer entre eux et être interopérables sur Internet, participant à ce que Joël Reidenberg appelle la *Lex Informatica* (Reidenberg, 1997). Par exemple, le fonctionnement des adresses IP est décrit dans un document « RFC 791 » de l'*Internet Engineering Task Force* (IETF). D'autres documents, comme la RFC 1087 intitulé « Éthique et Internet » (« *Ethics and Internet* »), décrivent la façon dont les autres standards doivent être rédigés pour prendre en compte des valeurs de nature politique. Les conditions de réussite de la vocation performative de ces textes ne sont pas les mêmes que les textes de loi auxquels nous les comparons. Mais comme les textes de droit « dur », ces documents ne décrivent pas ce qui est, mais ce qui devrait être. Ils partagent avec le droit à la fois le fait d'être des énoncés performatifs et d'avoir une vocation normative.

Les choix techniques qui sont fixés dans des standards d'Internet ont des conséquences sur l'environnement technique des utilisateurs. Des questions politiques sur la liberté d'expression et le droit à la propriété intellectuelle sont soulevées par l'intégration de mesures techniques de protection (« *Digital Rights Management* » ou DRM) dans le corpus de standards du Web (Sire, 2017). Des choix dans le degré de précision d'un mécanisme permettant à un serveur web de connaître l'état de charge de batterie du terminal de l'internaute, pouvait augmenter les risques d'identification précise de l'utilisateur de l'appareil par un adversaire malveillant (Olejnik, Englehardt et Narayanan, 2017).

Il existe des tentatives de résoudre des problèmes politiques par la rédaction et l'adoption de standards techniques. Ces standards sont désignés par Nick Doty et Deirdre Mulligan par le terme de « standard techno-politique » (Doty et Mulligan, 2013). Parmi ceux-ci, plusieurs visent à protéger la « vie privée » (Bennett et Raab, 2003 ; DeNardis, 2014, p. 77). Les documents *Tracking Preference Expression* et *Tracking Compliance and Scope* rédigés au sein du *Tracking Protection Working Group* du *World Wide Web Consortium* (W3C) ont pour but d'intégrer dans les navigateurs web un mécanisme permettant à leurs utilisateurs de transmettre aux serveurs des

sites qu'ils visitent des préférences en matière de vie privée, et à ces serveurs de fournir une réponse standardisée quant à leur respect de ces préférences. Nous aurons l'occasion de revenir sur ces documents dans le chapitre trois et de nous demander si, en tant que texte visant à protéger la « vie privée », ils visent le même objet que les textes du Conseil de l'Europe, de l'OCDE, et de l'Union européenne que nous aurons étudié dans les deux chapitres précédents.

Notons que pour éviter toute confusion terminologique, bien que nous assimilons les standards techniques à des formes de droit souple, nous parlerons du « droit » produit par le Conseil de l'Europe, l'OCDE et l'Union européenne, et des « standards techniques » de l'IETF et du W3C. Les Lignes directrices de l'OCDE de 1980 régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel ne sont en effet pas du droit « dur ». Il ne s'agit que de recommandations du Conseil de l'OCDE, regroupant les représentants de ses États membres. Aucune sanction n'existe en cas d'infraction, et personne ne contrôle leur application. Pourtant, ce texte a bien vocation à promouvoir l'adoption de règles de droit national conformes à ses dispositions ; il a bien été rédigé par des juristes et discuté dans des arènes dont les acteurs, insérés dans des structures étatiques, ont l'habitude de la rédaction de règles de droit positif.

Il est important à ce stade de préciser ce que nous entendons par « arène ».

Une arène est un terme assez générique utilisé en anthropologie politique, en relations internationales mais aussi en analyse de controverses pour désigner tout lieu « où des groupes stratégiques hétérogènes s'affrontent, mus par des intérêts (matériels ou symboliques) plus ou moins compatibles » (Olivier de Sardan, 1993, p. 3). C'est aussi un « lieu matériel ou immatériel de confrontation […] [caractérisé] par des contraintes formelles et communicationnelles spécifiques, par une visibilité sociale variable, par une temporalité propre ainsi que par des inégalités d'accès pour les individus » (Ollivier-Yaniv, à paraître, p. 3 du pre-print). Cette dernière définition, qui s'inspire de celle de Joseph Gusfield (Gusfield, 1994), nous invite à porter attention au rôle des conditions matérielles et sociales de participation à chaque arène (Badouard, Mabi et Monnoyer-Smith, 2016 ; Bonaccorsi et Julliard, 2010 ; Mabi, 2013).

Or, le fonctionnement des arènes de standardisation techno-politiques est très différent des arènes de l'OCDE, de l'UE ou du Conseil de l'Europe que nous avons étudiées. Elles sont composées essentiellement d'ingénieurs n'ayant pas été formés au droit. Historiquement, elles se sont construites par défiance de ces acteurs vis-à-vis de l'intervention étatique dans la gouvernance d'Internet[23]. La production normative de ces arènes n'est pas non plus tout à fait de même nature que celle, par exemple, des arènes institutionnelles de l'UE, qui produisent du droit positif. Une compréhension des dimensions communicationnelle et performative du droit permet toutefois d'observer de nombreux points communs entre ces deux types de productions, que relient notamment la textualité et la normativité, et d'en produire une analyse comparée.

23 Cf. sections 5.1. et 5.2. sur la gouvernance d'Internet.

Construction de l’objet de recherche

La rédaction des textes de droit et des standards techno-politiques visant à protéger la « vie privée » ne s’est pas faite sans controverse, ni sans être précédée d’un processus de politisation et de mise à l’agenda politique structuré autour d’une formule nouvelle : en l’espèce, celle de « protection des données ». Cette notion de formule, que nous empruntons à Alice Krieg-Planque, désigne :

> « un ensemble de formulations qui, du fait de leurs emplois à un moment donné et dans un espace public donné, cristallisent des enjeux politiques et sociaux que ces formulations contribuent dans le même temps à construire » (Krieg-Planque, 2009, p. 7)

Un autre exemple de formule, dans un autre domaine de l’action publique, est celui de « développement durable » (Krieg-Planque, 2010).

Il a ensuite fallu que cette problématisation politique donne lieu à des revendications de mesures concrètes. Ces revendications ont rencontré des oppositions, soutenues par des arguments, auxquels les acteurs porteurs de ces revendications ont dû répondre par d’autres arguments, pour légitimer les leurs et discréditer celles de leurs adversaires. Ces discours peuvent avoir une dimension instrumentale voire n’avoir été produits que pour servir des intérêts matériels, sans que leurs auteurs ne soient convaincus par leurs propres arguments. Mais d’une part, nous n’avons pas accès aux intentions des acteurs, et, d’autre part, un discours produit sans sincérité pour défendre des intérêts autres que ceux qu’il prétend défendre est parfaitement capable de convaincre des personnes qui le reprendront alors avec sincérité. Enfin, la compréhension même de nos intérêts matériels est conditionnée par la perception que nous en avons, qui elle-même est forgée par nos imaginaires sociaux (Castoriadis, 2006 [1975] ; Gramsci, 2018 [1948] ; Mannheim, 2006 [1929] ; Ricœur, 1984). C’est pourquoi nous avons opté pour une approche par l’analyse de discours et de leurs confrontations dans des controverses, plutôt qu’une approche cherchant à dévoiler les intérêts économiques que cacheraient ces discours. Dans d’autres cas, certains discours peuvent être formulés sans intention stratégique particulière (Huet et Sarrouy, 2015), tout en étant perçus comme stratégiques par les personnes qui reçoivent ces discours, instaurant ainsi une situation, même sans le vouloir.

Notre intuition était que l’étude des controverses autour de la rédaction des normes de protection des données à caractère personnel permettrait de repérer de tels arguments et discours, faisant référence à des systèmes de conviction et à des imaginaires qui proposent leurs propres façons de concevoir la « vie privée », le « droit *à la* vie privée » et le « droit *à la* protection des données à caractère personnel ». Dans ce cadre-ci, les débats sur la définition de la notion de

« donnée à caractère personnel » nous ont apparu revêtir un intérêt tout particulier, parce que les « données à caractère personnel » sont aussi l'objet du droit *de la* protection des données à caractère personnel (Clément-Fontaine, 2017). En règle général[24], c'est la présence de telles données qui active l'application du droit *de la* protection des données, lié à la fois au droit fondamental *à la* protection des données à caractère personnel comme à celui *à la* vie privée. L'étude de l'objet de la controverse « donnée à caractère personnel » devait alors, toujours selon nos intuitions, avoir une valeur heuristique pour la compréhension de ce qu'est la « vie privée ».

Cette définition a été un élément central des débats pendant l'élaboration de normes juridiques ou techno-politiques de protection des données à caractère personnel, puisque de cette définition part le raisonnement permettant de déterminer le champ d'application matériel de ces normes. Cela n'est pas l'apanage de cette controverse définitionnelle en particulier.

Les controverses dans l'espace public peuvent se focaliser autour d'idées, ou de symboles. Edward Snowden a ainsi pu être qualifié « d'homme-controverse », permettant aux acteurs de la controverse sur le rôle et l'étendue des pouvoirs des services de renseignement dans des démocraties libérales de se positionner sur un axe clair (Musiani, 2015). Dans la sociologie des sciences et des techniques, une controverse peut porter sur des objets en particulier. Edward Lenert a ainsi montré comment la controverse autour du premier service de télévision en ligne, iCraveTV, a eu des effets sur la configuration technique de l'infrastructure de communication qu'est Internet (Lenert, 2004).

Les controverses portant sur des définitions de mots produisent aussi des effets politiques. Les mots contribuent à la construction de catégories permettant de penser le monde et l'action dans ce monde. Leurs définitions socialement répandues peuvent figer des stéréotypes, des représentations sociales et porter des idéologies (Barthes, 2014 [1957], 2015 [1985]), et, en amont de la mise à l'agenda d'un problème politique, influencer la production de politiques publiques dans un sens conforme au référentiel qui a gouverné l'adoption de la définition des termes dans lesquels ce problème politique est décrit (Butler, 1997 ; Cefaï, 1996). C'est dans cette perspective que Réjane Sénac-Slawinski a étudié les controverses définitionnelles autour des mots « *gender mainstreaming* » et « paritarisme » en France (Sénac-Slawinski, 2008).

24 Il existe des exceptions. Par exemple, le RGPD, en vertu de son article 2, ne s'applique pas aux traitements de données à caractère personnel effectués « par une personne physique dans le cadre d'une activité strictement personnelle ou domestique ». Mais cette exception n'agit qu'à une quatrième étape du raisonnement, qui consiste à vérifier tout d'abord si l'on est bien en présence de « données à caractère personnel » (1) faisant l'objet d'un « traitement » (2) « automatisé en tout ou partie » (art. 2 par. 1 du RGPD) ou ayant vocation à figurer dans un fichier (3), avant de voir si des exceptions s'appliquent (4). Toute réflexion pour déterminer si une situation est soumise aux règles du RGPD commence par s'interroger sur la présence de « données à caractère personnel » au sens de sa définition juridique.

Une controverse définitionnelle *juridique* ne porte pas seulement sur la signification d'un mot ou d'une expression comme « donnée à caractère personnel ». En effet, elle porte sur la définition d'un concept juridique. Pour qu'un tel concept s'applique à la description d'un phénomène concret, il faut qu'il soit possible de l'utiliser pour *qualifier* celui-ci en droit. Cette *qualification juridique* est un mécanisme qui transforme une situation de fait pouvant être exprimée dans un vocabulaire courant en une description en un vocabulaire juridique qui fait référence à des définitions précises de catégories juridiques auxquelles des règles de droit s'appliquent. Lors d'un procès, la qualification juridique retenue a des conséquences déterminantes sur son issue ; définir un événement comme une « contravention » ou un « délit » n'a pas la même conséquence. Un « homicide volontaire » n'a pas la même conséquence qu'un « homicide involontaire ». Or, les professionnels du droit justifient leurs choix de qualifications juridiques par un processus exégétique prenant appui sur chacun des mots de la définition du terme qu'ils utilisent pour décrire une situation.

Le cas, par exemple, des discussions sur la définition juridique du « réfugié[25] » – et son incidence très concrète sur la vie des demandeurs d'asile – rappelle l'importance politique des débats sur la formulation concrète de l'énoncé performatif qui constituent la matière des dispositions juridiques servant d'outils à un domaine de l'action publique. Ces dispositions juridiques sont des outils, dont l'écriture inscrite sur un support médiatique constitue la matérialité, sans nier les spécificités de l'instrument de politiques publiques qu'est le droit, il est possible d'étudier des controverses sur la configuration (l'écriture) de cet objet d'une façon analogue aux controverses sur la configuration des objets techniques.

Les directives et règlements européens contiennent habituellement des dispositions juridiques explicites qui définissent les notions qui revêtent une importance particulière eu égard à leur objet. Par exemple, la directive 2011/95/UE[26], à son article 2 sous d), reprend presque mot pour mot la définition de l'article 1A (2) de la Convention de Genève[27] de la notion de « réfugié ». La directive 2015/1535/UE[28], qui a abrogé la directive 98/34/CE[29], définit un

25 Voir les nombreuses discussions à ce sujet dans la littérature juridique, entre aux : Chemillier-Gendreau, 2006 ; Cournil, 2010 ; Créac'h, 2002 ; Ferracioli, 2014 ; Hyndman, 1987

26 Directive 2011/95/UE du Parlement européen et du Conseil du 13 décembre 2011 concernant les normes relatives aux conditions que doivent remplir les ressortissants des pays tiers ou les apatrides pour pouvoir bénéficier d'une protection internationale, à un statut uniforme pour les réfugiés ou les personnes pouvant bénéficier de la protection subsidiaire, et au contenu de cette protection

27 L'article 1A (1) de la Convention de Genève se borne à disposer que les personnes s'étant vues accorder le statut de réfugié sur la base de textes plus anciens peuvent continuer à se prévaloir de cette qualification juridique et peuvent bénéficier du nouveau régime adopté en 1951

28 Directive 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information

29 Directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques

« service »[30] au sens de cette directive comme « tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services » (art. 2 sous b) de la directive 2015/1535/UE).

La Convention 108 du Conseil de l'Europe, le RGPD, tout comme la RFC 6973, et bien d'autres textes normatifs sur la protection des données à caractère personnel contiennent quant à eux une définition bien précise de la notion de « donnée à caractère personnel » (ou d'un synonyme). Ce qui y est écrit est déterminant pour savoir à quelles situations le droit *de la* protection des données à caractère personnel doit s'appliquer. En d'autres termes, les « données à caractère personnel » sont l'*objet* du droit *de la* protection des données à caractère personnel dont nous avons vu qu'il procède de deux catégories de droit fondamentaux autonomes mais aujourd'hui impossibles à démêler : le droit *à la* vie privée et le droit *à la* protection des données à caractère personnel. Notre intuition est que l'étude de cette définition permette de mieux comprendre à la fois l'objet de ces droits et les éventuels dissensus à son égard. Si différents textes contiennent des définitions différentes, cela peut être le signe de désaccords conceptuels sur la nature de ce que recouvre cette notion de « vie privée » à protéger.

Cela nous amène à formuler la problématique suivante, qui constitue le fil directeur de cette thèse :

> **À quelle(s) conception(s) de la « vie privée », comme objet d'une protection par des textes normatifs, les définitions controversées de la notion de « donnée à caractère personnel » font-elles chacune référence ?**

Hypothèses

Notre première hypothèse de travail, qui était présentée dès le projet de recherche initial, est qu'il existe une différence d'ordre épistémique – voire une confrontation – entre des conceptions juridiques d'un côté et des conceptions informaticiennes de l'autre, du sens des termes « protection des données », « vie privée » et surtout « donnée à caractère personnel », notamment en raison de la formation différenciée des juristes d'une part, et des informaticiens de l'autre. L'existence d'une séparation disciplinaire ferait que les travaux en droit et en informatique, communiquant peu, n'auraient que peu d'occasion de converger autour d'une compréhension commune. Cette hypothèse est en partie une hypothèse de sens commun. Le droit

30 Cette définition succède à la définition du « service de la société de l'information »

serait sempiternellement « en retard » sur la « réalité technique », et cette idée, comme nous le verrons, a souvent été évoquée par les groupes d'intérêt industriels dans les négociations sur le RGPD et sur la définition de la notion de « donnée à caractère personnel » à y inclure.

Un sondage auprès des autorités européennes de protection des données dont les résultats ont été publiés en 2017 par Iván Székely et Charles Raab (2017) montre que la plupart d'entre elles jugent insatisfaisantes leurs connaissances en informatique. L'article rappelle aussi la perception de sens commun d'un décalage entre le droit et l'évolution rapide de l'informatique. Une étude sur les délégués à la protection des données menée en France par le Ministère du travail montrait qu'informaticiens et juristes n'étaient pas d'accord sur les compétences les plus utiles à l'exercice de leur métier (AFPA, 2019). D'autres travaux distinguent la protection des données « en théorie » (« *in the books* ») et « sur le terrain » (« *on the ground* ») (Bamberger et Mulligan, 2015), la capacité des autorités de contrôle à comprendre ce qui se passe « sur le terrain » étant notamment fonction de leur capacité à comprendre les procédés informatiques des traitements de données effectués (Rossi, 2017b).

Au-delà de ces différences, qui sont des différences de connaissance et d'expérience dans des domaines d'expertise distincts, certains articles suggèrent des conflits d'intérêts voire des différences conceptuelles effectives. Selon Martin Meints, il existerait par exemple une tension entre certains principes du droit *de la* protection des données et ceux de la sécurité des systèmes d'information (Meints, 2009). Selon Paul Ohm (2010), les définitions juridiques des notions équivalentes en droit états-unien à celle – plutôt d'origine européenne – de « donnée à caractère personnel », reposeraient sur un mythe : celui qu'il existe une distinction nette entre données personnelles d'une part, et données anonymes de l'autre, alors que de nombreux travaux en informatique ont prouvé qu'il existe un continuum de données plus ou moins facilement ré-identifiables (Barbaro et Zeller, 2006 ; de Montjoye et al., 2015 ; Olejnik et al., 2015 ; Sweeney, 2000). Sergio Mascetti, Anna Monreale, Annarita Ricci et Andrea Gerino, dont les travaux se sont fondés sur les définitions en droit de l'Union européenne et en droit italien de la notion de « donnée à caractère personnel », identifient également des différences entre celles-ci et les concepts qu'ils identifient dans les quelques publications en informatique sur la protection de la vie privée et des données à caractère personnel. Contrairement à Paul Ohm, ils trouvent que les publications en informatique qu'ils analysent tendent à exclure du champ de la définition de la notion de « donnée à caractère personnel » (ou ses synonymes) les quasi-identifiants, c'est-à-dire les données qui, sans être directement identifiantes (comme un nom), peuvent aider à retrouver l'identité de la personne (par exemple, la combinaison d'une date de naissance avec une adresse). Ils affirment également que la notion d'« attribut non-privé », c'est-à-dire d'information sur une personne qui n'est pas à protéger au titre de la « vie privée », n'existe pas en droit mais est employée en informatique (Mascetti et al., 2013, p. 106-112). Leur étude porte sur un corpus assez restreint, qui ne permet pas de tirer de conclusions définitives sur l'existence d'une différence d'approche de nature épistémique entre droit et informatique sur la « vie privée » à l'échelle de ces disciplines. Ils n'ont pas non plus interrogé de juristes ou d'informaticiens sur leurs représentations, ni étudié le rôle de leurs conceptions respectives de la « vie privée » dans

l'élaboration du droit *de la* protection des données à caractère personnel, ou dans sa réception et mise en œuvre dans des solutions informatiques.

Si cette hypothèse se vérifiait, alors juristes et informaticiens ne se figureraient en effet pas le même objet lorsqu'ils parlent de « protection des données à caractère personnel », laquelle est distincte, mais aussi liée, à celle de « protection de la vie privée », puisqu'ils ne partageraient pas la même compréhension de ce qu'est une « donnée à caractère personnel » à protéger. Nous avons donc cherché à tester cette hypothèse en commençant par une phase exploratoire d'entretiens avec des juristes et des informaticiens[31]. Nous avons ensuite étudié la façon dont se sont forgées les définitions de la notion de « donnée à caractère personnel » en droit, à travers des terrains comme les groupes d'experts du Conseil de l'Europe et de l'OCDE où s'est constituée une communauté transnationale ayant diffusé et mis à l'agenda la formule de « protection des données »[32], et le processus d'adoption du RGPD et les débats sur la définition à y inclure de la notion de « donnée à caractère personnel »[33]. Nous avons enfin comparé ces observations avec celle des débats de deux groupes d'ingénieurs œuvrant au sein du W3C à l'élaboration de standards techniques visant à protéger la « vie privée » : le *Tracking Protection Working Group* et le *Privacy Internet Group*[34].

Les résultats de l'enquête exploratoire nous ont très vite amené à nuancer cette première hypothèse, les différences observées dans le petit échantillon d'entretiens exploratoires effectués ne permettant pas de nous mettre sur la piste des différences observées par Mascetti *et al.* (2013) ou Paul Ohm (2010) qui, d'ailleurs, se contredisent sur certains points. Tout en restant une hypothèse de travail et un fil directeur du travail de recherche que nous présentons ici pour sa valeur heuristique, cette première hypothèse a rapidement été rejointe par d'autres hypothèses qui ont émergé au fur et à mesure des années de thèse.

Notre seconde hypothèse est que les formules de « protection des données », « droit à la protection des données à caractère personnel », et la définition de la notion juridique de « donnée à caractère personnel » n'ont pas émergé comme conséquence mécanique des évolutions de l'infrastructure technique de la société, mais en conséquence de *perceptions* de l'informatique, des ordinateurs qui s'insèrent dans cette infrastructure, comme étant des dangers pour un droit à la « vie privée » pré-existant. Cette hypothèse n'a rien d'une évidence, dans la mesure où ni la surveillance, ni le fichage, ni même les bases de données qui ont succédé aux registres, ne sont apparus avec l'informatique (Vitalis et Mattelart, 2014). Toutefois, l'usage de l'application Google Ngram[35] montre que les termes « data protection » et « datenschutz », qui signifient

31 Cf. sections 1.2.2. et 6.6.

32 Voir à ce sujet les ouvrages de Frits Hondius (1975), David Flaherty (1989), Colin Bennett (Bennett, 1992), Charles Raab et Colin Bennett (Bennett et Raab, 2003), James Rule et Graham Greenleaf (Rule et Greenleaf, 2010), Abraham Newman (2008) et Gloria González Fuster (González Fuster, 2014a). Cf. chapitre 3, en particulier sections 3.3. et 3.5.

33 Cf. chapitre 4, en particulier section 4.3.4., mais aussi la section 6.4.

34 Cf. chapitre 5.

35 Cette application permet d'interroger la base de données des livres numérisés par le projet Google Books, et de montrer l'évolution de la fréquence d'une ou plusieurs chaînes de caractères dans ce corpus de textes au cours du

« protection des données » en anglais et en allemand[36] apparaissent et connaissent rapidement une croissance forte de leur fréquence d'emploi environ deux décennies après la naissance de l'informatique électronique, ce qui peut laisser supposer une causalité chronologique :

Évolution de l'emploi du terme « data protection »	
Évolution de l'emploi du terme « datenschutz »	

Tableau 1 : *Évolution des fréquences d'emploi des termes «* data protection *» et «* datenschutz *» dans le corpus de livres numérisés par Google Books, visualisées avec l'outil* Google Ngram Viewer

Le travail d'enquête généalogique sur l'émergence et la mise à l'agenda de la « protection des données », et sur l'origine des premières définitions de la notion juridique de « donnée à caractère personnel[37] » nous a permis d'évaluer cette hypothèse[38].

La troisième hypothèse est que le droit *à la* et *de la* protection des données à caractère personnel ont été imaginés pour conserver l'efficacité de la protection du même objet qu'un droit pré-existant : le droit *à la* vie privée. Si cette hypothèse se vérifie, le droit *à la* protection des

temps. Cet outil est régulièrement utilisé dans les phases exploratoires de travaux en histoire linguistique (voir pour des exemples : Godin, 2016 ; Ophir, 2016 ; Steuckardt, 2015).

36 La recherche du terme « protection des données » sur Google Ngrams renvoie à un message d'erreur.

37 Cf. chapitre 6.

38 Cf. chapitre 3.

données à caractère personnel est une partie du droit *à la* vie privée, ce dernier couvrant un nombre plus vaste de situations, comme celles qui relèvent de l'inviolabilité du domicile, qui n'impliquent pas nécessairement une collecte de données. Si les conclusions de l'étude de Sergio Mascetti *et al.* (2013), intégrées à la première hypothèse, se vérifient, il est possible que les approches juridiques opèrent une distinction entre droit *à la* protection des données (de toute donnée) et droit *à la* vie privée (qui concerne seulement la « vie privée »), que les approches informaticiennes ne feraient pas car leur définition des données à protéger correspondraient uniquement ou en priorité à celles qui sont jugées « sensibles » car « privées » (ou « privées » car « sensibles »). Toutefois, il serait faux de considérer que le droit, ou en tout cas le droit en Europe que nous avons étudié, ignore toute distinction entre les « données à caractère personnel » en général et des données particulièrement « sensibles », puisque l'article 9 du RGPD prévoit des règles particulièrement strictes pour certaines catégories de données[39]. Il peut être par ailleurs fait exception à ces mêmes règles lorsque ces données « particulières » sont « manifestement rendues publiques par la personne concernée » (art. 9 paragraphe 2 sous e du RGPD), ce qui suggère une prise en compte du caractère public ou non de ces « données à caractère personnel ». Enfin, l'article 35 du RGPD prévoit encore d'autres règles à respecter lorsque « un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques » (art. 35 paragraphe 1 du RGPD). Il n'est donc à ce stade absolument pas évident que droit et informatique appréhendent différemment la question du risque ou de la sensibilité d'une donnée au regard de la « vie privée » d'une personne dans la détermination des règles à respecter en matière de « protection des données ». Cette troisième hypothèse, qui postule une continuité dans l'objet de la protection du droit *de la* et *à la* protection des données avec celui du droit *à la* vie privée, sera discutée principalement dans le chapitre étudiant les différentes définitions de la notion de « donnée à caractère personnel », son évolution et les débats les entourant à travers l'ensemble des terrains qui ont été choisis[40].

Enfin, si droits *de la* et *à la* protection des données ont été conçus pour protéger la même « vie privée » que le droit *à la* vie privée, nous pouvons supposer l'existence d'une continuité dans les idées, idéologies, systèmes de convictions, imaginaires sociaux et arguments qui en motivent la défense, ou au moins celle du partage d'une même généalogie intellectuelle et politique. Cette continuité d'ensembles d'idées, convictions et arguments, au-delà des différences sémantiques entre droit *à la* protection des données et droit *à la* vie privée, devraient avoir eu pour effet d'inciter à l'adoption d'une définition de la notion de « donnée à caractère personnel » qui désigne des données relevant de la vie privée d'une personne. Pourtant, la jurisprudence de la CJUE établit une différence nette entre « donnée à caractère personnel » et « donnée relative à la

39 Il s'agit des données qui révèlent « l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique » (art. 9 paragraphe 1 du RGPD)

40 Cf. chapitre 6

vie privée » (CJUE 16 juillet 2015 « ClientEarth », aff. C-615/13P). Si cette différence n'est pas purement lexicale, est-ce la conséquence d'une rupture entre deux conceptions de la « vie privée », l'une protégée par le droit *à la* protection des données, l'autre par le droit *à la* vie privée ?

Pour vérifier la validité de cette quatrième et dernière hypothèse, nous intégrerons à notre étude les imaginaires auxquels les acteurs impliqués dans les débats sur la rédaction de ces définitions font référence, les arguments qu'ils mobilisent, et nous les interrogerons sur leurs systèmes de convictions. En reliant ces résultats à une typologie de différentes conceptions théoriques produisant des discours sur la « vie privée » ou les « données personnelles »[41], nous verrons s'il existe des différences dans l'axiologie des acteurs impliqués dans les différentes arènes dans le temps (entre les premiers travaux du Conseil de l'Europe et de l'OCDE dans les années 1970 et l'adoption du RGPD dans les années 2010) et entre disciplines (en comparant ces deux terrains avec les discussions qui se déroulent au W3C). À l'issue de ce travail d'analyse, nous verrons quel sens est donné sur le terrain entre droit *à la* vie privée et droit *à la* protection des données, et si la défense deux deux relève d'un même système de convictions ou non.

Notons à l'issue de cette présentation du système d'hypothèses ayant guidé le travail de thèse qu'elle pourrait laisser croire qu'il s'est agi d'un travail strictement hypothético-déductif. Toutefois, seule l'hypothèse de travail d'une différence épistémique entre droit et informatique sur la façon de concevoir la « vie privée » et la « protection des données » était présente dès la première version du projet de recherche. Les autres hypothèses ont émergé de façon inductive au fur et à fur de lectures, de la fréquentation du terrain, ou encore de l'analyse des corpus, d'abord sous la forme d'intuitions. Elles ont ensuite été rédigées sous la forme d'hypothèses de travail à laquelle la méthodologie et le cadre théorique furent peu à peu adaptés pour aboutir aux résultats présentés dans ce mémoire de thèse.

Annonce du plan

Le premier chapitre présentera la méthodologie et les terrains qui ont alimenté la thèse. Après une présentation du cadre méthodologique général, nous verrons comment celui-ci a été décliné sur chacun des terrains étudiés, parfois avec des apports théoriques et des éléments de méthode spécifiques.

Le second chapitre présentera un panorama de différentes conceptions de la « vie privée » et de la « protection des données » dans la littérature académique ou dans les médias. Cette typologie idéal-typique nous permettra ensuite de retrouver ce à quoi les discours d'acteurs de nos différents terrains font référence.

41 Cf. chapitre 2.

Le chapitre suivant se concentrera sur la genèse et la mise à l'agenda politique du droit *de la* protection des données en Europe, dans une période centrée sur les années 1970. Nous verrons comment s'est alors structuré un réseau transnational de défenseurs de la vie privée, autour duquel s'est ensuite construit l'une des coalitions d'acteurs présente pendant les négociations du RGPD. La formation de cette coalition a été grandement facilitée par le Conseil de l'Europe et l'OCDE, qui furent des lieux d'élaborations des principes et définitions encore aujourd'hui contenues dans le RGPD. Ce chapitre sera l'occasion de vérifier notre hypothèse selon laquelle la perception de l'informatique comme danger pour la « vie privée » a servi de catalyseur à la mise à l'agenda politique de la « protection des données » comme problème public désigné par cette nouvelle formule.

Les négociations sur le RGPD seront présentées dans un quatrième chapitre, qui étudiera les discours produits par les différentes coalitions de cause ayant cherché à influencer leur issue. Nous verrons que, comme dans les années 1970, la coalition des défenseurs de la vie privée s'est alors principalement inspirée d'une conception libérale de la vie privée, devenue le référentiel sectoriel dans le sous-système de politiques publiques de l'UE. Face à une coalition industrielle très mobilisée, notamment autour de la volonté de modifier la définition juridique de la notion de « donnée à caractère personnel », au nom d'arguments économiques néolibéraux, les défenseurs de la vie privée parvinrent à consolider leurs demandes en les rattachant au référentiel global des politiques publiques de l'UE grâce à un argument : celui de la confiance. Selon cet argument, un haut niveau de protection des données serait nécessaire à la confiance des consommateurs en un marché du numérique, et cet objectif entrerait donc dans les priorités du projet de marché unique numérique de la Commission européenne. Ce même argument avait été utilisé avec succès par la coalition, libérale, des défenseurs de la vie privée, dans les années 1970, face à un référentiel global qui n'était pas encore néolibéral, mais qui n'en était pas moins favorable à une exploitation massive de données informatisées portant sur des individus.

Le cinquième chapitre sera l'occasion de voir que cet argument de la confiance a également été mobilisé par un groupe de défenseurs de la vie privée agissant au sein des deux groupes du W3C que nous avons étudiés : le PING et le TPWG. Contrairement à ce que laissait supposer notre première hypothèse, les discours sur la « vie privée » au W3C partagent avec ceux repérés dans les autres terrains l'idée selon laquelle le droit *à la* vie privée est un droit individuel. De surcroît, si les juristes, ont adopté une formule consacrée par le Tribunal constitutionnel fédéral d'Allemagne de l'Ouest, celle de « droit à l'auto-détermination informationnelle », et que les ingénieurs du W3C préfèrent parler de « contrôle par l'utilisateur » (« *user control* »), les deux expressions expriment toutes deux l'idée selon laquelle dans l'idéal, c'est à l'individu de déterminer les informations qu'il souhaite partager ou bien garder pour lui.

D'ailleurs, le sixième chapitre sera l'occasion de revenir sur le fait que la définition de la notion de « donnée à caractère personnel » figurant dans les documents du W3C PING et TPWG est identique à celle figurant dans le RGPD, qui elle-même remonte pour l'essentiel à des décisions prises au sein des groupes d'experts du Conseil de l'Europe et de l'OCDE dans les années 1970. Outre la démonstration de l'invalidité de notre première hypothèse, cette définition,

centrée sur l'individu, qui inclut toutes les données qu'elles relèvent ou non du « privé » et de « l'intime », lui laissant le soin de déterminer pour lui-même le contenu de ces catégories, correspond bien aux idées des conceptions libérales de la vie privée décrites dans le premier chapitre. De ce fait, le droit *de la* protection des données protège une conception de la « vie privée », fondée sur le contrôle individuel, qui s'oppose à une conception fondée sur la protection d'une barrière à protéger entre espace public et espace privé. « Donnée personnelle » et « donnée relative à la vie privée » sont donc bel et bien deux concepts juridiques distincts, la première ayant été inventée, comme discuté dans le second chapitre, durant les années 1970.

La conclusion sera d'abord l'occasion de répondre à notre problématique initiale et de faire le point sur nos quatre hypothèses. Nous verrons dans cette réponse que l'invention d'un droit *à la* et *de la* protection des données à caractère personnel en réaction à la diffusion de l'informatique perçue par un groupe de libéraux comme une menace, correspond à une évolution du droit *à la* vie privée qui n'est pas sans rappeler ce que Benjamin Constant désignait comme le passage de la Liberté des Anciens à celle des Modernes (Constant, 2010 [1819]). Avec la protection des données, la « vie privée » n'est plus un espace protégé par une frontière autour d'un espace privé pouvant être celui d'un collectif, mais est devenu un droit au contrôle individuel sur les « données à caractère personnel ». Toutefois, si la définition de cette dernière doit être lue comme une mesure concrète mettant en œuvre une conception libérale de la « vie privée » que nous qualifierons d'après Benjamin Constant de « moderne », cela ne nous dit rien sur la réception de ce droit, dont nous avons décrit en introduction le caractère communicationnel, ni sur ses effets sur les conceptions de la « vie privée » circulant plus largement dans la société. Nous prendrons donc le temps en fin de conclusion d'évoquer des pistes de recherche pour approfondir les résultats présentés dans cette thèse.

Chapitre 1 : Méthode et terrains

1.1. Le cadre méthodologique

Les problèmes publics ne sont pas donnés objectivement par la réalité. Si l'alcool au volant est une cause objective de décès sur les routes, ce n'est pas pour autant qu'il a toujours été considéré comme un problème public (Gusfield, 1994). De la même façon, même en admettant que l'hypothèse que l'ordinateur met en péril la « vie privée » est absolument et entièrement vraie, ce n'est pas pour autant que des débats parlementaires aboutissent nécessairement à l'adoption de lois qui deviennent l'instrument d'une politique publique de protection ou de restauration de cette « vie privée » en péril ou perdue. Les problèmes publics sont donc le fruit d'un processus de construction sociale, et ce constat, en nous détachant des approches matérialistes des effets de la technique sur la société, nous a conduit à choisir une méthode qui permette d'étudier les représentations des acteurs qui ont produit les instruments du droit *de la* protection des données.

La construction d'un problème public passe par la confrontation entre une expérience et des cadres d'interprétation de cette expérience (Benford, Snow et Plouchard, 2012 ; Goffman, 1974), ou encore des imaginaires sociaux (Castoriadis, 2006 [1975] ; Ricœur, 1984) qui sont eux aussi un produit d'interactions sociales. Daniel Cefaï (1996) rappelle que pour qu'un phénomène se transforme en problème public, puis qu'il soit mis à l'agenda médiatique ou politique, il faut qu'un passage soit opéré d'un sentiment de malaise ou d'injustice individuel et privé initialement identifié, à celui d'une expérience partagée prenant l'ampleur d'un problème collectif. Des récits et formules émergent alors pour désigner le nouveau problème public et lui donner un sens.

Certains problèmes publics peuvent donner naissance à de nouvelles catégories de l'action publique. Les sociétés modernes montrent en effet des tendances à la spécialisation (Bauman, 2000 ; Durkheim, 1893 ; Weber, 2003 [1921]). Cette tendance à la spécialisation s'observe également par la spécialisation d'acteurs et d'institutions sur des catégories spécifiques de l'action publique. C'est le cas de la « politique culturelle » à la fin des années 1950 (Dubois, 1999) ou encore de la « politique de la ville » entre la fin des années 1970 et le début des années 1990 (Tissot, 2013 [2007]). La politique « culturelle du numérique » est née, en France, au sein du ministère de la Culture au milieu des années 1990, et est très liée à la mobilisation d'une communauté composée « d'agents convaincus des potentialités d'Internet, notamment au sein de la direction de la recherche et de la direction des services informatiques, [qui] favorise la connexion précoce des postes de travail, l'introduction du courrier électronique et la mise en place de l'un des premiers sites web du gouvernement français, culture.fr […] » (Bellon, 2019, p. 170). Ces catégories n'existaient pas avant d'être construites comme des domaines

d'interventions désirables de l'État, vers lequel l'action d'institutions publiques spécialisées – créées ou aux missions modifiées – doit s'orienter. Se créent ainsi autour de certains problèmes publics émergents de nouvelles catégories d'intervention qui structurent autour d'elles des « champs de l'action publique » (Dubois, 2010, 2014), des « secteurs de l'action publique » (Jobert et Müller, 1987) ou encore des « sous-systèmes de politiques publiques » (Sabatier et Jenkins-Smith, 1993), ces trois termes décrivant peu ou prou le même objet[1].

Précisons à ce stade que nous entendons par « action publique » toute action visant à produire des effets politiques sur la société, quel qu'en soit l'auteur. Des associations, des églises, ou des entreprises, ou même des individus, peuvent participer à l'action publique, par exemple en faveur de l'environnement. Les politiques publiques, quant à elles, peuvent être définies succinctement comme l'action publique de l'État. Une politique publique a un contenu, c'est-à-dire des instruments mobilisés pour produire des effets auprès d'une certaine population selon des modalités qui (particularité idéal-typique de l'État) peuvent être coercitifs[2]. Elle déploie également un programme répondant à une orientation normative (Jobert et Müller, 1987, p. 51 ; Mény et Thoenig, 1989, p. 131).

L'approche séquentielle des politiques publiques, dont il existe plusieurs variantes, découpe leur production en plusieurs étapes. Le premier schéma séquentiel a été élaboré par Charles Jones (1970). Il y développe l'idée selon laquelle une politique publique se déroule en cinq temps : identification (et construction, mise à l'agenda) du problème public, prise de décision formelle, mise en œuvre de la décision formelle, évaluation et, éventuellement, terminaison du programme. Cette grille d'analyse idéal-typique est souvent plus normative qu'une description fidèle de la réalité. Elle a toutefois le mérite de souligner l'importance de la phase de mise à l'agenda et de construction d'un problème public dans la détermination des choix publics et ainsi dans la production de l'action publique (qu'il s'agisse d'ailleurs de celle de l'État ou de l'action publique en général).

Sans nier l'existence du cadre institutionnel et matériel dans lequel se déploie l'action de l'État, ni les logiques d'intérêts (socialement construits) qui entrent en jeu, les approches dites cognitives des politiques publiques sont une branche de l'étude des politiques publiques qui s'intéresse au rôle de ces représentations sociales dans la formulation et la mise en œuvre des

1 Le terme de « champ de l'action publique », bien que correspondant, pour prendre un exemple, à celui de « secteur » selon Vincent Dubois (Dubois, 2010), est en réalité moins stato-centré, puisque Pierre Müller envisage les politiques publiques à partir du rôle de l'État, et que la notion bourdieusienne de « champ » permet d'inclure plus facilement les autres acteurs de l'action publique, comme les associations ou les entreprises. À des fins de lisibilité, nous considérons toutefois ces termes, pour l'instant, comme synonymes, et n'entrerons dans le détail de leurs définitions que si et lorsque cela sera utile pour le déroulement de notre propos.

2 Pour la définition de la notion de politique publique, voir : Mény et Thoenig, 1989, p. 131.
Pour la définition de la notion d'instrument des politiques publiques, voir : Lascoumes, 2004.

politiques publiques, qui sont des processus à forte dimension communicationnelle. Ces approches se fondent sur le constat suivant :

> « Élaborer une politique publique consiste […] d'abord à construire une représentation, une image de la réalité sur laquelle on veut intervenir. C'est en référence à cette image cognitive que les acteurs organisent leur perception du problème, confrontent leurs solutions et définissent leurs propositions d'action : cette vision du monde est le référentiel d'une politique. » (Müller, 2011, p. 57)

Ces approches se sont beaucoup développées à l'époque du tournant néolibéral des années 1980, où les changements programmatiques dans la conduite de l'action de l'État ne pouvaient plus être expliqués par l'alternance électorale ou par l'existence de contraintes objectives pesant sur les institutions (Müller, 2000, p. 190), mais par un changement paradigmatique dans les systèmes de convictions des décideurs publics de l'époque[3] (Hall, 1986, 1993 ; Jobert, 1994).

Les approches cognitives des politiques publiques ont fourni une part centrale de l'armature théorique et méthodologique des travaux que nous présentons dans cette thèse. Elles se sont révélées particulièrement utiles pour l'étude de controverses entourant la production des définitions de la notion de « donnée à caractère personnel », et plus généralement, des controverses autour de la « vie privée » et de la « protection des données » dans les arènes produisant les textes normatifs auxquels nous nous sommes intéressés.

Le modèle des coalitions de cause (« *Advocacy Coalition Framework* », abrévié ACF) développé par Paul Sabatier et Hank Jenkins-Smith (Sabatier et Jenkins-Smith, 1993) s'intéresse au rôle des systèmes de conviction dans la conduite des politiques publiques, et aux conditions d'apprentissage et de changement de la part des acteurs qui les mènent. Son modèle cherche à concilier les approches *top-down* qui étudient la façon dont, entre la décision et la mise en œuvre, les décisions de politiques publiques sont mises en œuvre, et les approches *bottom-up*, pour lesquelles le rôle de l'État s'efface derrière la multiplicité d'acteurs se saisissant de problèmes publics sur le terrain (Bergeron, Surel et Valluy, 1998, p. 198). L'ACF prend donc en compte le rôle des institutions étatiques dans la conduite de politiques publiques, tout en permettant de décrire le rôle d'autres acteurs dans la formulation et la conduite des politiques publiques. D'après ce modèle, « une politique [sectorielle] peut être définie comme le produit d'un système de croyances spécifique, issu de la confrontation continue et des compromis successifs passés

3 Pierre Müller ne considère pas que l'approche de Peter Hall par les paradigmes de l'action publique fasse partie des approches cognitives des politiques publiques (Müller, 2000, p. 193). Cette exclusion ne nous paraît toutefois pas justifiée, car quelles que soient au demeurant les différences entre les deux théories, elles ont, de l'aveu même de Pierre Müller, un nombre conséquent de points communs dans leur approche de l'étude des politiques publiques par les cadres d'interprétation de leurs acteurs.

entre les systèmes de croyances propres à chaque coalition en présence dans un sous-système donné » (Bergeron, Surel et Valluy, 1998, p. 202-203).

Le modèle de l'ACF distingue plusieurs éléments dans les systèmes de conviction des acteurs engagés dans un sous-système de politiques publiques (Sabatier, 1998, p. 103) :

- Le noyau fondamental[4] (« *deep normative core* ») :

  Cette expression correspond à la couche centrale, composée d'axiomes normatifs. Il s'agit du noyau de convictions morales et philosophiques propre à chaque individu, comme par exemple les questions sur la nature anthropologique de l'être humain, ou les questions sur le Bien et le Mal. Un exemple donné par Paul Sabatier et cité par Henri Bergeron, Yves Surel et Jérôme Valluy (1998, p. 203) est l'opposition entre la croyance fondamentale en le progrès technique et en l'économie des coalitions industrielles, et les croyances fondamentales de la coalition environnementale, dans les politiques publiques industrielles ou environnementales.
- Le noyau superficiel, ou programmatique (« *near policy core* ») :

  Celui-ci correspond aux hypothèses sur les relations de causalité, aux choix programmatiques et stratégiques des acteurs. Ces choix visent à réaliser les objectifs normatifs au sein du sous-système étudié. Par exemple, l'idée de doter le livre d'un statut particulier le protégeant des lois du marché correspond à un élément du noyau programmatique (Bergeron, Surel et Valluy, 1998, p. 203). Nous préférons l'expression de « noyau programmatique » à celle de « noyau superficiel » car selon la théorie de l'ACF, c'est autour de ce noyau que sont soudées les alliances entre acteurs cherchant à influencer la production d'un sous-système de politiques publiques. Le terme « superficiel » reflète mal la centralité de cette notion de *near policy core*.

- Les aspects secondaires, ou mesures concrètes (« *secondary aspects* ») :

  Il s'agit de mesures concrètes servant à mettre en œuvre les objectifs stratégiques de la seconde couche, c'est-à-dire du noyau programmatique. Pour poursuivre avec l'exemple des politiques de l'édition en France, la concrétisation de l'idée de doter le livre d'un statut particulier se trouve dans la loi n° 81-766 dite Lang du 10 août 1981 relative au prix du livre qui introduit le prix unique du livre. Une formulation particulière de la définition de la notion de « donnée à caractère personnel » proposée pour l'article 4 du RGPD est un autre exemple d' « aspect secondaire ».

  Nous préférons toutefois parler de « mesures concrètes » traduisant les objectifs d'un système de convictions, plutôt que d'« aspects secondaires ». Différents travaux sur les mouvements sociaux ont montré que les modes d'action et les mesures concrètes

4 Les premières traductions vers le français des termes anglais « deep normative core », « near policy core » et « secondary aspects » sont tirées d'un article de Daniel Kübler (2002).

proposées ont un rôle dans la structuration de ce que le modèle de l'ACF nomme des coalitions de cause (cet aspect est évoqué dans : Benford, Snow et Plouchard, 2012).

La confrontation entre coalitions de cause est de nature communicationnelle, et peut s'observer dans certaines arènes, que nous avons déjà définies[5] comme les lieux de confrontation entre des acteurs aux convictions opposées. Cette confrontation peut s'observer en public, mais aussi se poursuivre dans des coulisses plus difficilement accessibles aux chercheurs. L'ACF propose une façon de repérer des clivages qui structurent ces coalitions rivales à travers cet ensemble d'espaces plus ou moins faciles d'accès pour la recherche.

Pour Paul Sabatier, une coalition de cause (« *advocacy coalition* ») est un ensemble d'acteurs (publics ou privés) qui « cherchent à traduire leurs croyances dans des politiques publiques[6] » (Sabatier, 1993, p. 28). Ces coalitions disposent de ressources qui leur permettent d'agir, mais leurs objectifs dépendent d'un système de convictions qui cimente l'alliance, généralement au niveau du *policy core* ou noyau programmatique (Sabatier, 1993, p. 32-33, 1998). Cartographier les coalitions de cause se fait donc en repérant les systèmes de conviction auxquels adhèrent les acteurs d'un sous-système de politiques publiques, et les points de clivages entre systèmes de convictions concurrents. Cette approche fournit le cadre de base de notre méthode pour étudier les controverses sur la protection des données et la définition de la notion de « donnée à caractère personnel », dont l'analyse doit nous permettre de mieux comprendre l'objet de la protection du droit *de la* et *à la* protection des données à caractère personnel.

Pierre Müller – un autre théoricien des approches cognitives des politiques publiques – s'est lui d'abord intéressé à la question de « l'État en action » (Jobert et Müller, 1987), et du paradoxe qu'il y a entre l'unité de l'action de l'État et l'existence de sous-systèmes spécialisés, ou plutôt, pour utiliser son propre vocabulaire au lieu de celui de Paul Sabatier et Hank Jenkins-Smith, l'existence de politiques publiques sectorielles souvent en concurrences non seulement pour des ressources, mais également pour les objectifs à poursuivre. Cette interrogation sur le rapport entre les niveaux global (qui exerce une force centripète) et le sectoriel (centrifuge) de la politique de l'État l'a amené avec Bruno Jobert à s'intéresser à la façon dont les discours de légitimation d'une politique publique sectorielle s'articule à l'action globale de l'État (Jobert et Müller, 1987).

Pour Pierre Müller, chaque politique publique sectorielle s'organise autour d'un référentiel, qu'il définit de la façon suivante :

5 Cf. paragraphe intitulé « Le droit saisi par une approche communicationnelle », dans l'introduction générale.
6 Traduction de l'auteur. Texte original : « Coalitions seek to translate their beliefs into public policies ».

> « Le référentiel correspond avant tout à une certaine vision de la place et du rôle du secteur concerné dans la société. Par exemple, les propositions que l'on pourra faire en matière de politique de la santé dépendront du statut de la maladie dans la société moderne et du statut des personnels chargés de mettre en œuvre les systèmes de soin. De même, l'exemple de l'interruption volontaire de grossesse montre que l'émergence d'une politique comme celle mise en place par Simone Veil supposait que se soient modifiées les représentations dominantes concernant la sexualité et la place des femmes. Plus récemment, la réforme des systèmes de retraite renvoie clairement à un débat sur le rapport entre vieillissement et vie active » (Müller, 2011, p. 57)

Pierre Müller décrit deux niveaux de référentiels : un référentiel global, et des référentiels sectoriels. Le référentiel global « est une image sociale de toute la société, c'est-à-dire une représentation globale autour de laquelle vont s'ordonner, se hiérarchiser les différentes représentations sectorielles » (Jobert et Müller, 1987, p. 65). Cette image n'est pas nécessairement un ensemble cohérent, mais elle hiérarchise les différents référentiels sectoriels. Elle est constituée « d'un ensemble de valeurs fondamentales qui constituent les croyances de base d'une société, ainsi que de normes définissant le rôle de l'État et des politiques publiques » (Müller, 2011, p. 59). Un référentiel sectoriel, à l'inverse, est propre à une politique sectorielle spécifique. Pour reprendre les mots de Bruno Jobert et Pierre Müller : « c'est l'image dominante du secteur, de la discipline, de la profession » (Jobert et Müller, 1987, p. 68).

Les référentiels ont une fonction hégémonique au sens gramscien (Gramsci, 2018 [1937]), car ils sont des mécanismes de légitimation de l'ordre social (Jobert et Müller, 1987, p. 62). En d'autres termes, un référentiel de politique publique joue un rôle idéologique, l'idéologie qui légitime un ordre social étant selon Károly Mannheim (Mannheim, 2006 [1929]) le contraire de l'utopie qui le remet en cause. Un désajustement entre le référentiel d'une politique publique sectorielle et le référentiel global entraîne la déstabilisation du premier. Ainsi, en France, après la Libération, la domination d'un référentiel global de modernisation entraîna la remise en cause des politiques sectorielles de l'agriculture, qui reposaient sur un référentiel de maintien des traditions et de la société rurale paysanne qui n'a pas su se légitimer dans les termes du nouveau référentiel global (c'est-à-dire s'articuler avec) (Müller, 1984). Une politique sectorielle fondée sur un référentiel incompatible avec le référentiel global ne survivra selon ce modèle théorique pas longtemps. En nous inspirant du concept d'articulation global-sectoriel de Pierre Müller, nous parlerons d'articulation pour décrire les stratégies argumentatives par lesquelles un discours correspondant à un référentiel sectoriel (ou même minoritaire au sein d'un secteur) prouve, ou fait semblant de prouver, qu'il est compatible avec une idéologie dominante ou hégémonique, comme par exemple un référentiel global, au niveau de l'État.

Pour Pierre Müller, le référentiel sectoriel est un « construit social » (Jobert et Müller, 1987, p. 69). Sa théorie n'aborde cependant que très superficiellement la façon dont se construit un référentiel sectoriel. Là où son modèle du référentiel global-sectoriel décrit des situations dans lesquelles des référentiels hégémoniques sont déjà établis, tant au niveau global qu'au niveau sectoriel, le modèle de l'ACF de Paul Sabatier et Hank Jenkins-Smith permet d'étudier les rivalités entre différents systèmes de convictions cherchant à devenir sinon hégémoniques, du moins paradigmatiques, au sein d'un secteur (ou sous-système) de politiques publiques. Là où l'hégémonie ne laisse place à aucune concurrence idéologique en dehors d'espaces marginaux, un référentiel sectoriel paradigmatique n'est qu'une référence incontournable pour tous les acteurs au sein d'un secteur. Nous verrons que le paradigme libéral de la vie privée[7] s'est imposé comme paradigme incontournable, mais il n'est pas absolument incontesté, et ne saurait être qualifié d'hégémonique.

Nous ajouterons donc à notre outillage lexical et conceptuel un troisième type de référentiel. Nous proposons de désigner simplement par « référentiel », ou référentiel « tout court », tout système de convictions reposant sur des valeurs, un imaginaire, une lecture particulière des relations de cause à effet dans la société, et des normes décrivant un écart entre l'état perçu de la société et la société idéale voulue[8], et décomposable en *deep core*, *near-policy core* et *secundary aspects* (ou mesures concrètes).

Ces référentiels sont en concurrence au sein d'un sous-système pour devenir *le* référentiel sectoriel de ce secteur. Conformément à la lecture qu'en propose Pierre Müller, un référentiel qui parvient le mieux à s'articuler au référentiel global aura les meilleures chances de légitimer les mesures concrètes défendues par ses partisans, et de devenir le référentiel sectoriel. De plus, les acteurs réagissent aux arguments de la coalition rivale en répondant par de nouveaux arguments, qui eux-mêmes reçoivent des contre-arguments. Ce jeu d'argumentation et de contre-argumentation contribue à structurer les oppositions entre systèmes de convictions, et donc entre coalitions de cause. Nous parlerons pour le désigner de *structure argumentative* de la rivalité.

Nous avons appliqué ces modèles théoriques à notre terrain sur l'adoption du RGPD. En l'adaptant au cadre institutionnel de la gouvernance d'Internet, dont les modalités de l'action publique diffèrent en de nombreux points de celle des États, nous l'avons également appliqué à l'étude des controverses au sein du W3C sur la protection de la vie privée et des données à caractère personnel. Ces modèles étaient toutefois inadaptés à l'étude de la genèse du droit *à la* protection des données à caractère personnel et de cette nouvelle catégorie d'intervention publique qui a donné lieu à l'émergence de sous-systèmes de politique publique nationaux et européen structurés autour du réseau des autorités de protection des données.

7 Cf. la description de ce courant de pensée en section 2.2.

8 Pour Pierre Müller, un référentiel se décompose en « valeurs », « images », « algorithmes » et « normes » (Müller, 2011, p. 57-58).

L'ACF permet mal d'étudier la genèse de sous-systèmes de politiques publiques (Bergeron, Surel et Valluy, 1998, p. 128). Paul Sabatier précise d'ailleurs bien que son modèle n'est valable que pour les sous-systèmes établis depuis au moins une dizaine d'années (Sabatier, 1993). Pour l'étude de la sociogenèse de la formule de « protection des données », de la constitution de ce à quoi elle fait référence comme problème public auquel répondre, et de sa mise à l'agenda politique, nous avons complété – mais pas remplacé – notre méthodologie fondée sur les approches cognitives des politiques publiques par des emprunts à la méthode généalogique (Foucault, 2008 [1969] ; Koopman, 2013). Cette méthode consiste à retrouver les moments de rupture dans l'histoire des connaissances, des moments où des catégories de savoirs sont apparues ou ont disparu, pour problématiser des savoirs ou des pratiques. Elle est une histoire du présent ; en étudiant l'Histoire, son but est d'éclairer le présent.

Nous avons mené une enquête qui a consisté, sur la base d'un travail d'archives, à retrouver les premières occurrences historiques de la formule « protection des données » pour, une fois ces moments repérés, retrouver le contexte et les auteurs de ces premières occurrences, retracer des évolutions de sens, et accéder aux débats qui, souvent dans des arènes confidentielles comme celles des groupes d'experts du Conseil de l'Europe, ont précédé la mise à l'agenda médiatique du problème public alors en gestation du traitement informatisé de « données personnelles ». Nous reviendrons plus en détail sur nos emprunts à la méthode généalogique en introduction du chapitre sur l'émergence de la protection des données comme problème public[9].

Nous verrons qu'une communauté de politique publique (*policy community*[10]), celle des « défenseurs de la vie privée » (« *privacy advocates* ») (Bennett, 2008), a joué dans la mise à l'agenda politique de la « protection des données », puis formé le noyau d'une coalition de cause

9 Cf. section 3.1.

10 Après hésitation, nous avons préféré ce concept à celui de communauté épistémique pour décrire le groupe de personnes qui, dans les années 1960 1970, ont porté à l'agenda la question de la protection de la vie privée vis-à-vis du développement de l'informatique en ayant une compréhension commune de ce problème public fondée sur une vision libérale de la « vie privée ». En effet, une communauté épistémique, telle que théorisée par Peter Haas, ne désigne pas que le partage de valeurs et de croyances, mais aussi le partage d'une épistémologie, c'est-à-dire d'axiomes scientifiques et méthodologiques sur comment produire des connaissances valides (Adler et Haas, 1992). Si cet aspect est utile pour comprendre les communautés d'économistes ayant mis à l'agenda politique les politiques économiques monétaristes au moment du tournant néolibéral des années 1980, ou pour comprendre la mise à l'agenda des questions climatiques vers la même période, ou encore la mise en place de politiques de protection de l'environnement en Méditerranée (Haas, 1989), il ne paraît pas pertinent pour décrire la *privacy community* des années 1960 et 1970. Le terme de *policy community*, employé par Colin Bennett (1991, 1992) nous paraît plus approprié, car il suggère le partage d'un intérêt pour un problème public émergent ou établi mais n'implique pas automatiquement que ses membres soient d'accord sur la façon de produire des connaissances scientifiques, ni même qu'ils aient besoin d'un tel accord pour travailler ensemble à un même objectif. Une *policy community* peut être nationale ou transnationale, et encourage la formation d'une perception commune d'un même problème public entre ses membres, par effet de socialisation (Bennett, 1991). Ce n'est toutefois pas la même chose qu'une coalition de cause, qui repose sur des convictions partagées, dans un contexte de rivalité pour la maîtrise d'un sous-système de politiques publiques établi. Comme dans le cas de la protection des données, une *policy community* peut précéder l'existence d'un tel sous-système sectoriel et en entreprendre la construction.

s'opposant à une coalition industrielle tant dans les débats sur l'adoption du RGPD, que dans les débats observés au sein du W3C sur la « vie privée ». Cette communauté transnationale (Bennett, 1991, 1992) a contribué à produire un référentiel libéral de la vie privée[11] qui est devenu paradigmatique. Il est le référentiel sectoriel des politiques publiques de protection des données à caractère personnel de l'UE, mais il est aussi le paradigme autour duquel s'articulent les discussions sur la « *privacy* » au sein des groupes du W3C que nous avons étudiés[12].

Pour repérer les systèmes de convictions des acteurs impliqués dans nos différents terrains, nous avons donc essayé[13] de cartographier des coalitions de cause. Les entretiens y ont grandement contribué. À l'exception d'un premier terrain exploratoire qui a précédé une ré-orientation de notre recherche[14] nous avons intégré à tous nos questionnaires d'entretiens des questions demandant à chaque enquêté d'identifier des alliés et des rivaux. D'autres questions visaient à identifier et comprendre :

- Le système de convictions des enquêtés (« *deep core* » et « *near-policy core* »), et notamment la conception de « la vie privée » à laquelle ils adhèrent ;
- Les mesures concrètes (« *secundary aspects* ») qu'ils défendent et qui traduisent en pratique leurs systèmes de convictions ;
- Les arguments mobilisés en défense de leurs convictions et des mesures concrètes revendiquées ;
- Quels ont été leurs alliés et leurs rivaux dans la controverse.

Pour identifier la structure argumentative des rivalités entre coalitions de cause, nous demandions à chaque personne de nous donner un exemple de mesure concrète qu'elle défend, de l'appuyer par des arguments, d'évoquer les contre-arguments de ses adversaires, et enfin la façon dont elle a l'habitude de répondre à ces contre-arguments. Ces questions étaient d'autant plus importantes qu'elles permettaient parfois de révéler des arguments circulant de façon orale entre acteurs de la controverse, sans qu'ils aient nécessairement laissé de traces écrites dans les documents compilés dans nos corpus. Il est aussi arrivé que les enquêtés évoquent d'eux-mêmes la façon dont ils percevaient la structuration des coalitions de cause rivales du sous-système où ils intervenaient. Nous avons cherché à susciter des discours d'acteurs sur notre objet d'étude, à les interroger sur leur axiologie, en leur demandant d'expliquer les causes de leur engagement.

11 Cf. section 2.2.

12 Cf. en particulier section 5.6.1.

13 Essayer car, dans les années 1960 et 1970, celles-ci ne s'étaient pas encore clairement structurées, et au W3C, il n'est pas possible de parler de coalitions de cause de la même façon que dans un sous-système de politiques publiques étatiques. Toutefois, le fait d'*essayer* d'en repérer a malgré tout permis de repérer des rivalités idéologiques entre acteurs, et aidé à observer la structure argumentative des controverses que nous avons étudiées. En ce qui concerne les négociations autour du RGPD entre 2009 et 2016, nous avons toutefois bel et bien *pu* cartographier des coalitions de cause, et pas seulement *essayé*.

14 Cf. 1.2.2.

La réalisation d'entretiens pose en général de nombreuses contraintes méthodologiques (Fontana et Frey, 2005). Certaines sont spécifiques à notre objet. La mémoire, par exemple, est faillible. Il peut y avoir des contradictions entre les entretiens, ou entre des entretiens et des documents d'archives, qui obligent à faire des choix ou bien à abandonner une partie du matériau pour cause d'incertitude sur sa fiabilité. Matériellement, il n'est pas toujours possible de confronter les enquêtés aux sources et de lever d'éventuelles contradictions ou difficultés d'interprétation.

De plus, plusieurs enquêtés avaient eu des carrières qui les avaient exposés médiatiquement et politiquement. Michael Kirby a été juge à la Cour Suprême de l'Australie, László Sólyom président de la République de Hongrie, Pieter Hustinx Contrôleur européen de la protection des données. Ce type de position peut habituer à l'expression de discours policés et construits à l'avance. Le fait que ces personnes aient été à la retraite au moment de l'entretien a cependant permis des échanges plus libres qu'avec des personnes en exercice de mandat.

D'autres enquêtés, encore en activité, peuvent être contraints par le fait d'être encore des participants actifs de controverses sur l'action publique en matière de protection des données. Leurs possibilités d'expression peuvent être contraintes par des logiques stratégiques, ou bien tout simplement par les clauses de confidentialité qu'ils peuvent avoir à respecter. L'anonymat a pu dans certains cas être une stratégie pour permettre une expression plus libre (voir : Beaud et Weber, 2017 ; Boumaza, 2001 ; Rossi et Bigot, 2018), mais souvent, l'intérêt d'un entretien résidait dans la position sociale occupée par l'enquêté dans la controverse. Dans ces cas, l'anonymat pouvait être difficile à garantir – obligeant à renoncer à citer des morceaux d'entretiens où la personne était reconnaissable – ou bien la décontextualisation des citations nécessaire à l'anonymisation risquait d'entraîner une perte de sens rendant la citation de l'entretien inutile. Les personnes interrogées ont donc signé un accord pour être enregistrées et pour que leurs entretiens soient utilisés pour la recherche, sur un formulaire, qui leur permettait d'indiquer une demande d'anonymat, sans que cette option ne soit présentée comme la solution par défaut. Elles avaient également la possibilité à tout moment de préciser que quelque chose qu'elles venaient de dire devaient rester « *off the record* », confidentiel. Finalement, peu d'enquêtés ont fait la demande de rester anonymes.

Nous nous sommes rendu sur place autant que possible afin de nous assurer de la qualité de l'entretien. Se rendre sur place, dans notre expérience, a souvent permis d'avoir une discussion à la fois plus libre et plus longue. Le fait d'être prêt à se déplacer crédibilisait aussi notre demande d'entretien auprès des enquêtés. Toutefois, cela n'a pas toujours été possible, pour des raisons budgétaires, et plusieurs entretiens se sont déroulés par visioconférence ou bien par téléphone.

Enfin, réaliser et retranscrire des entretiens est très coûteux en temps. Les personnes sollicitées peuvent elles-mêmes ne pas avoir le temps, ou bien l'envie, d'accepter l'entretien. Il était donc difficile d'avoir un nombre suffisant d'entretiens pour qu'ils fournissent à eux seuls une quantité de matériau empirique suffisante à notre travail de recherche.

Les entretiens ont donc été complétés par des documents d'archives, des retranscriptions de débats, des e-mails échangés sur des listes de discussion publiques, des rapports officiels, des textes de propositions d'amendements, ou encore des *policy papers* produits par des groupes d'intérêt.

Tous les documents produits dans le cadre des controverses que nous avons étudiées ne sont pas, normalement, accessibles au public. La question de l'accès aux coulisses, mais également à l'absence de trace des nombreuses interactions orales entre les acteurs de la controverse, a posé de nombreux défis méthodologiques. Notre objet d'analyse ne portait en effet pas sur une controverse se déployant uniquement dans des arènes publiques médiatiques, mais également dans des arènes aux travaux plus ou moins confidentiels – comme les groupes d'experts du Conseil de l'Union européenne – voire à travers des échanges interpersonnels informels ou privés entre acteurs de la controverse. Entretiens comme documents d'acteurs intégrés au corpus avaient donc une double fonction : ils étaient à la fois le support d'inscription de discours d'acteurs intégrés à notre corpus d'analyse, et de sources de renseignements factuels ou de contexte sur le déroulement de controverses échappant pour une large partie à l'œil du public.

L'analyse qualitative de documents est une méthode qui permet de fournir des éléments de contexte sur le milieu dans lequel des enquêtés évoluent. Elle permet de soulever des questions nouvelles, qui n'avaient pas été prévues à la phase de formulation des hypothèses. Elle fournit des données factuelles supplémentaires, en fournissant par exemple des dates précises d'événements que la mémoire humaine, sur laquelle les entretiens reposent, peut oublier ou confondre. Elle permet de documenter l'évolution des discours et des positions des différents acteurs. Elle peut corroborer d'autres sources d'information, comme les entretiens (Bowen, 2009). Enfin, ces documents contiennent des discours d'acteurs qui peuvent être analysés, et en comparant les prises de position sur les mesures concrètes, il est possible de compléter et d'affiner la cartographie des coalitions de cause.

L'analyse des discours d'acteurs a en effet joué un rôle important pour identifier le contenu des systèmes de conviction (ou référentiel « tout court ») de chaque coalition de cause. Un intérêt ici du terme de simple *référentiel* pour désigner un système de convictions est que ce mot fait référence, justement, à la fonction référentielle du langage décrite par le linguiste Roman Jakobson (Jakobson, 1963) : un message ne peut être décodé qu'en référence à un code partagé. La sémiotique ou la sémiologie diront qu'un signe se décompose en signifiant (forme) et signifié (sens) (Barthes, 2015 [1985]). Le discours d'un acteur cherchant à influencer la production de politiques publiques comportera des mots et des expressions qui font référence à des corpus

d'idées politiques, à des imaginaires, généralement implicites, qui pourront être décodés et compris à condition de connaître ces référentiels. Nous mobiliserons les outils de l'analyse de discours pour faire le lien entre les discours d'acteurs de nos corpus et les différentes théories politiques auxquelles ils font explicitement et implicitement référence, notamment en matière de « vie privée » et de « protection des données ».

Plutôt que de travailler sur des corpus constitués à partir de l'arène médiatique, nous avons ciblé des arènes d'experts semi-publiques voire confidentielles. En effet, bien que de nombreux discours et théories aient été publiés et circulent dans l'espace public, proposant des conceptions différentes de la « vie privée » ou de la « protection des données[15] », toutes, parmi celles-ci, ne sont pas forcément mobilisées dans les arènes où sont élaborées les normes de protection des données à caractère personnel contenant une définition de la notion de « donnée à caractère personnel ». Rien ne nous indique *a priori* que les débats dans ces arènes soient l'exact reflet des débats dans l'espace public médiatique.

De plus, travailler uniquement sur un corpus de documents médiatiques ne nous permettrait pas de saisir le travail de construction du problème public antérieur à la mise à l'agenda médiatique. La surveillance, la protection des données à caractère personnel, la « vie privée » et sa protection, font bien l'objet d'un traitement médiatique dans la sphère publique (Walczak, 2014), et les récits classiques sur l'origine de la protection des données font souvent remonter l'origine de ce problème public à la parution de certains articles dans la presse. En France, un article de Philippe Boucher de 1974 sur un projet du Ministère de l'Intérieur, le fichier SAFARI, est souvent cité comme ayant joué ce rôle (Boucher, 1974 ; Vitalis, 2010). Pourtant l'existence d'un rapport du Conseil d'État commandé par le gouvernement en 1969 et rendu (mais pas publié) en 1970 suggère – et les résultats que nous allons présenter l'ont confirmé – qu'en Europe, la mise à l'agenda politique du sujet a précédé sa médiatisation publique. Rajoutons à cela que les controverses publiques, même contemporaines, portent rarement sur des choses aussi précises que la rédaction de la définition juridique de la notion de « donnée à caractère personnel ». Enfin, rien ne nous permet de supposer que les discours qui circulent au sein des espaces publics nationaux soient identiques à ceux qui circulent dans des arènes transnationales composées d'un public de spécialistes, où les échanges peuvent être souvent oraux, informels ou confidentiels, et où cette définition est non seulement mise en discussion, mais également produite. Les travaux de recherche sur les controverses montrent plutôt que lorsqu'elle circule d'une arène à une autre, les modalités et les termes d'une controverse évoluent en fonction de la matérialité et du public de ces arènes (Dodier, 1999, Ollivier-Yaniv, à paraître).

Une des raisons pour lesquelles nous n'avons pas centré notre travail sur des corpus de textes médiatiques est liée à la question de l'*efficacité* des espaces publics. La controverse sur la protection des données à caractère personnel, et sur la « vie privée », se déploie à travers une

15 Cf. chapitre 2.

multiplicité d'arènes. Mais lesquelles sont *efficaces* ? Notre objet d'enquête porte sur les controverses dont le contenu a effectivement eu une influence sur le droit (dur ou souple) *de la* protection des données, et en particulier les différentes définitions de la notion de « donnée à caractère personnel ».

Nancy Fraser (Fraser, 2007) rappelle que la notion d'espace public, telle que théorisée et popularisée par Jürgen Habermas (Habermas, 1988 [1962]), est très liée à la question du pouvoir politique et de l'exercice d'un effet de l'opinion publique sur le gouvernement des démocraties libérales. L'espace public est censé faire de l'opinion publique qui s'y construit une « force politique » (« *political force* ») (Fraser, 2007, p. 7). Par conséquent, elle affirme que malgré l'existence avérée de mobilisations transnationales de l'opinion publique, faute d'entité politique transnationale, il ne peut y avoir d'espace public transnational. En d'autres termes, ce n'est pas parce qu'une controverse circule d'un espace public national à l'autre, que cette circulation, qui, en plus, va de paire avec des traductions, réappropriations, et reconfigurations du débat, est constitutive d'un espace public transnational. L'effritement du système international westphalien et la dilution de la souveraineté des États nations doit donc nous interroger sur les conditions dans lesquelles l'espace public peut demeurer *efficace*, c'est-à-dire capable de produire une force politique (l'opinion publique) qui agit sur la conduite des politiques publiques.

L'Union européenne est un cas à part, dans le sens où il s'agit d'une entité politique, dotée de responsables politiques identifiés, responsables soit devant des gouvernements nationaux (eux-mêmes issus d'élections) soit du Parlement européen, élu au suffrage universel direct. Mais pour de nombreuses raisons, que nous discuterons plus en détail dans le chapitre sur l'adoption du RGPD[16], il nous semble impossible de parler aujourd'hui d'espace public européen. Notons au passage qu'aucun espace public lié à l'action des organismes privés transnationaux – mais pas intergouvernementaux – de la gouvernance d'Internet n'a été à notre connaissance identifié ; et qu'un tel travail d'identification serait le sujet d'un travail de recherche à part entière.

En adoptant des cadres théoriques conçus pour l'analyse de production des politiques publiques, nous changeons légèrement le point de départ de notre regard sur les controverses étudiées par rapport à des approches qui prendraient l'espace public médiatique comme point d'entrée. Au lieu de partir d'un choix d'arènes publiques d'où constituer des corpus de documents et discours à analyser, nous partons des acteurs des politiques publiques, que nous devons d'abord identifier, pour identifier les discours qu'ils produisent et circulent ensuite dans des arènes que nous pouvons alors identifier. L'unité du corpus tient donc à la circulation des documents au sein d'un sous-système de politiques publiques, qui recouvre différentes arènes et dont nous devons, une fois qu'elles sont repérées, prendre également en compte les conditions matérielles et sociales d'accès que nous évoquions un peu plus tôt en introduction pour contribuer à guider le travail d'interprétation.

16 Cf. chapitre 3.

Notons enfin, comme cela a déjà pu se deviner à la lecture de ce qui précède, que lorsque cela s'est avéré nécessaire, des éléments de théorie ou de méthodologie ayant un rapport plus étroit avec l'un des terrains ou chapitres de la thèse en particulier ont été développés en introduction de ces chapitres. Ce choix de rédaction a été fait afin de faciliter la lecture.

1.2. Description des terrains

1.2.1. Présentation générale

Quatre terrains ont été mobilisés pour collecter le matériau empirique nécessaire au test de nos hypothèses. Une première phase de terrain exploratoire a été suivie par :

- Un terrain sur la socio-genèse de la « protection des données », entre la fin des années 1960 et l'adoption de la Convention 108 du Conseil de l'Europe en 1981, centré autour de groupes d'experts du Conseil de l'Europe et de l'OCDE ;
- Un terrain sur les controverses ayant entouré le processus d'adoption du RGPD, des premières réflexions institutionnelles de la Commission européenne en 2009 à l'adoption formelle de ce règlement en avril 2016, mais s'étendant également à la jurisprudence de la Cour de justice de l'Union européenne en matière de protection des données comme élément de contexte ;
- Un terrain sur les controverses qui se sont déroulées au sein du *Tracking Protection Working Group* et du *Privacy Internet Group* du W3C, qui sont des arènes où ont été produits des textes normatifs visant à protéger la « vie privée » dans et par la production des standards techniques du Web.

Le matériau récolté au cours de ces différents terrains est résumé dans le tableau ci-dessous :

	Entretiens	**Observation**	**Corpus de documents**
Terrain 1 : enquête exploratoire	- 10 entretiens qualitatifs semi-directifs, complétés par un questionnaire en ligne (96 réponses)		
Terrain 2 : Conseil de l'Europe et OCDE	- 9 entretiens qualitatifs semi-directifs		- Documents d'archives, principalement du Conseil de l'Europe et de l'OCDE. 79 fichiers récupérés

			depuis les archives de l'OCDE (films et microfiches numérisées). - Diverses publications d'époque. 16 fichiers récupérés depuis les archives en ligne du Conseil de l'Europe. - Sources juridiques (projets de loi, lois adoptées, jurisprudence…)
Terrain 3 : RGPD	- 10 entretiens qualitatifs semi-directifs	- Exploration ethnographique, parfois participante, principalement dans des conférences structurantes pour les acteurs du terrain.	- 534 *position papers* et documents officiels, récupérés depuis le site du collectif Lobbyplag ou le site de la Commission européenne. - Sources juridiques (projets de loi, lois adoptées, jurisprudence…).
Terrain 4 : W3C Privacy Interest Group	- 10 entretiens qualitatifs semi-directifs	- Journée d'observation au *Technical Plenary and Advisory Committee* du W3C en octobre 2018.	- 346 487 e-mails téléchargés depuis plusieurs listes de discussion publiques du W3C. - Standards de l'IETF et recommandations du W3C.

Tableau 2 : *Tableau de présentation synoptique des terrains.*

1.2.2. Les enquêtes exploratoires centrées sur la première hypothèse

Le projet de recherche initial était principalement axé sur la première hypothèse : celle d'une différence d'ordre épistémique entre l'appréhension de la protection des données et de la « vie privée » entre juristes et informaticiens. Partant de cette hypothèse, une première campagne d'entretiens exploratoires a été réalisée entre mai et octobre 2016. Son but était de mettre à l'épreuve un prototype de questionnaire pour entretiens semi-directifs administré à deux groupes d'enquêtés : un groupe d'informaticiens, et un groupe de juristes. Au total, dix entretiens ont été réalisés ; cinq avec des personnes s'identifiant comme juristes, et cinq comme informaticiennes :

Nom	Prénom	Date de l'entretien	Lieu	Âge	Droit / informatique
Colle	Pierre	30 mai 2016	Paris	29	Informatique
S.	Mathieu	6 juin 2016	Paris	35	Informatique
M	S	7 juillet 2016	Paris	31	Informatique
Ghaleb	Mathieu	7 juillet 2016	Paris	37	Informatique
V	E	12 septembre 2016	par Skype	Entre 20 et 25	Informatique
Q	E	13 septembre 2016	Paris	26	Droit
Robert	Mathilde	17 octobre 2016	Paris	24	Droit
S	H	17 octobre 2016	Paris	25	Droit
Bracq	Stéphane	18 octobre 2016	Lille	46	Droit
Delette	Grégoire	18 octobre 2016	Bruxelles	24	Droit

Tableau 3 : *Entretiens réalisés dans le cadre de la campagne d'entretiens exploratoires*

Les personnes recrutées pour cette campagne l'ont été par effet boule-de-neige. Aucun critère rigoureux de représentativité n'a été appliqué, en raison d'une part de l'absence d'études sociodémographiques permettant de faire émerger de tels critères pour la profession d'informaticien et d'autre part, parce qu'il ne s'agissait à ce stade que d'une phase exploratoire destinée à mettre à l'épreuve, et au point, un questionnaire.

L'analyse de ces entretiens a porté sur des retranscriptions intégrales, pour des entretiens qui ont durée de 30 à 120 minutes.

Après ces entretiens exploratoires, un questionnaire a été publié en ligne en anglais et en français aux adresses dataprotectionsurvey.eu et enqueteprotectiondesdonnees.eu[17]. Le formulaire a été construit à l'aide du logiciel libre Limesurvey. La mise en ligne a eu lieu en septembre 2017. Elle n'a toutefois recueilli qu'un nombre insuffisant de réponses pour être exploitable en l'état : 1221 visites, mais seulement 40 réponses complètes à toutes les questions, 81 personnes avaient renseigné leur date de naissance. Il n'était en effet pas obligatoire de répondre à toutes les questions. Les questions sur la définition de la notion de « donnée à caractère personnel » ont collecté autour d'une cinquantaine de réponses chacune. Enfin, seules 19 personnes ont indiqué avoir été formées au droit, et 10 à l'informatique. Cela ne permet pas de tirer des conclusions statistiquement significatives. Toutefois, les réponses aux champs à réponse libre, qui permettent

17 Cf. annexe 14.

d'alimenter une démarche plus qualitative, ont pu fournir des éclairages, discutés dans le dernier chapitre[18].

L'échantillon de cette enquête exploratoire (en ligne comme par entretiens) s'est donc finalement révélé beaucoup trop faible pour pouvoir tirer les moindres conclusions statistiquement significatives. L'absence de différences notables entre les réponses des juristes et celles des informaticiens, dont nous aurions pu approfondir l'étude à une plus large échelle pour observer des éléments de définition propre à chaque profession, a rendu difficilement justifiable de poursuivre des efforts de recherche dans cette direction malgré la faiblesse de l'échantillon.

De plus, massifier le nombre de réponses de non-experts à un questionnaire détaillé sur la notion de « donnée à caractère personnel » se révélait en pratique compliqué pour plusieurs raisons. Tout d'abord, un tel questionnaire est long à remplir, notamment car il nécessite de la réflexion pour en parvenir à bout. L'un des répondants a indiqué dans un champ de commentaire libre en fin de questionnaire y avoir passé une heure, soit quatre fois plus que les personnes ayant répondu en situation de test. Cela tend à indiquer que les répondants y ont perçu un enjeu, et ont pu prendre le questionnaire pour une forme d'évaluation, dans un contexte où, selon les retours que nous avons eu en sollicitant des non-experts pour la campagne d'entretiens qualitatifs préliminaires, la plupart des gens ne s'est pas sentie légitime pour répondre à nos questions et ont dû, pour nombre d'entre elles, être rassurées avant d'accepter l'entretien. Poursuivre dans cette direction aurait demandé un investissement en temps qui, eu égard à ces premiers résultats de l'enquête exploratoire, ne se justifiait pas.

Tout en gardant la même hypothèse de travail, nous avons donc pris la décision, fin 2017, d'abandonner la démarche qui avait été entamée dans cette enquête exploratoire, au profit d'une comparaison des discours en circulation dans des arènes dominées par des acteurs socialisés au droit d'un côté et des arènes dominées par des acteurs socialisés à l'informatique d'autre part. Cela a abouti respectivement au terrain sur les « discussions » qui ont entouré l'adoption du RGPD et d'autre part sur le terrain sur le W3C PING. En parallèle de ces deux enquêtes, le travail sur la généalogie des politiques publiques de protection des données à caractère personnel s'est imposé entre autres raisons pour voir quel avait pu être le rôle d'interactions entre juristes et informaticiens au moment de la mise à l'agenda politique initiale de la question.

18 Cf. section 6.6.

1.2.3. L’étude de la socio-genèse du droit *de la* protection des données au Conseil de l’Europe et à l’OCDE

1.2.3.1. Identification du terrain

Notre deuxième terrain s’est centré sur les groupes d’experts qui, au Conseil de l’Europe et à l’OCDE, ont travaillé à la rédaction respectivement de la Convention n° 108 pour la protection des données à caractère personnel de 1981 et des Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de 1980. Ces groupes avaient déjà été identifiés par plusieurs études comme ayant été le lieu d’élaboration de principes et définitions juridiques qui ont inspiré, dans les années 1970, les lois nationales de protection des données (Bennett, 1992 ; Bennett et Raab, 2003 ; Flaherty, 1989 ; Hondius, 1975). Ils ont également été des lieux de rencontre pour des acteurs qui se sont structurés en un réseau transgouvernemental qui milita activement, sur le plan national comme supranational, en faveur de l’adoption en droit positif des principes et définitions qu’ils inventèrent dans le but de protéger la « vie privée » et assurer la « protection des données » (Newman, 2008).

En 1980, Michael Kirby, qui présidait le groupe d’experts chargé auprès de l’OCDE de rédiger le projet de lignes directrices en matière de protection des données à caractère personnel, écrivait :

> « Au vu des différents langages, traditions juridiques, et valeurs culturelles et sociales, des désaccords fondamentaux auraient été attendus. Cependant, curieusement, dans tous les travaux internationaux majeurs effectués jusqu'ici sur la question, un large consensus a été trouvé quant aux « règles de base » fondant la législation de protection de la vie privée dans les droits nationaux[19]. » (Kirby, 1980, p. 29 cité par Bennett, 1992, p. 95)

La forte ressemblance dans les contenus des lois de protection des données à caractère personnel adoptées dans plusieurs pays du bloc de l’Ouest entre 1970 et 1980 n’est pas sans cause. Si dès 1989, David Flaherty (1989) a mené des études de cas sur l’émergence de la protection des données en Allemagne, Suède, France, au Canada et aux États-Unis, Colin Bennett (1992) s’est employé à entamer une généalogie des principes fondamentaux de la protection des données et à comprendre la cause de cette corrélation entre les différentes lois nationales. Il démontre que si chacune d’entre elles fut bien entendue le fruit d’un processus d’élaboration

19 Traduction. Texte original : « Given the different langages, legal traditions, and cultural and social values, fundamental disagreements might have been expected. Surprisingly, in all of the major international efforts that have so far addressed this problem, there has been a broad measure of agreement on the “basic rules” around which domestic privacy legislation. »

national, leur corrélation s'explique par le fait qu'elles sont avant tout le fruit d'un processus d'élaboration international, ou du moins à l'échelle des pays de l'OCDE. Il démontra aussi que l'orientation politique des majorités parlementaires à la date d'adoption de ces lois n'a pas eu d'incidence sur leur contenu, pas plus que d'autres facteurs nationaux qui auraient pu peser sur le processus d'adoption (Bennett, 1992, p. 147-148). Colin Bennett décrit enfin l'existence d'une *policy community* centrée sur les problématiques de protection de la vie privée, dont, selon lui, les principaux acteurs furent : Spiros Simitis en Allemagne, Jan Freese et Peter Seipel en Suède, Louis Joinet en France, Paul Sieghart au Royaume-Uni, Michael Kirby en Australie, Stefano Rodotà en Italie, mais aussi : Hans Peter Gassman de l'OCDE et Frits Hondius du Conseil de l'Europe (Bennett, 1992, p. 128). Cette communauté, que nous dénommerons « *privacy community*[20] », se constitua très tôt, dès les années 1970, en un réseau d'« entrepreneurs transgouvernementaux » (selon le terme d'Abraham Newman (2008)), structuré autour de deux groupes d'experts en relation étroite, l'un hébergé par le Conseil de l'Europe, et l'autre par l'OCDE. Comme Colin Bennett, Gloria González Fuster (2014) souligne dans ses travaux sur la diffusion des termes de « *privacy* » ou « vie privée » et de « *Datenschutz* » ou « protection des données » dans différents ordres juridiques nationaux à partir des années 1970, le rôle de ces deux arènes, dont nous préciserons la chronologie, la composition et le fonctionnement dans la section 3.4.

Le livre publié par Frits Hondius en 1975 sur l'émergence d'un droit nouveau, le droit *à la* protection des données à caractère personnel, a constitué un précieux témoignage d'époque d'un acteur au centre de ce réseau de hauts fonctionnaires qui ont rédigé les premières lois européennes de protection des données. Un article publié en 2017 par Michael Kirby a joué le même rôle en ce qui concerne le groupe d'experts de l'OCDE qui avait été en charge, entre 1978 et 1979, de rédiger un texte qui est devenu en 1980 les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.

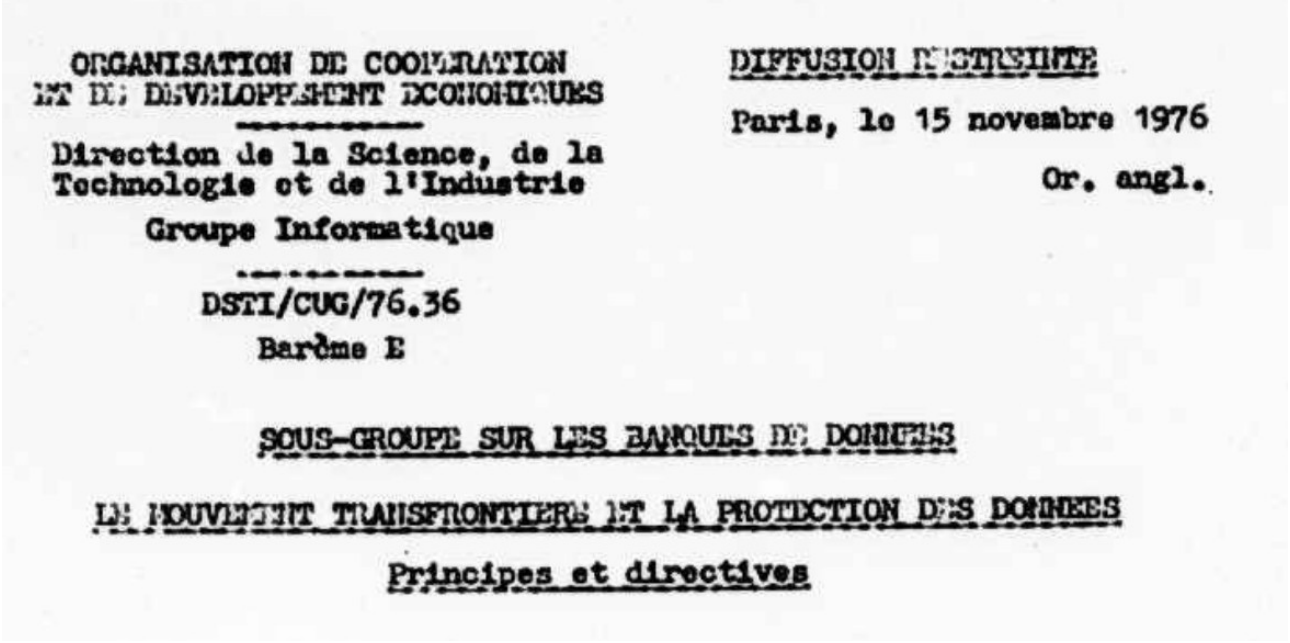
Notre enquête généalogique sur l'émergence de la protection des données s'est basée, en plus de la lecture de cette littérature académique, sur ces groupes d'experts qui, au Conseil de l'Europe et à l'OCDE furent chargés de réfléchir à la protection de la vie privée vis-à-vis de la menace que l'informatique faisait peser elle selon la perception qu'en avaient leurs membres.

Pour remonter aux premiers discours et aux premiers débats sur la protection des données et l'informatique, nous avons constitué un corpus composé de documents d'archives, et d'entretiens réalisés avec des témoins de l'histoire de la protection des données.

20 Cf. section 3.5.

1.2.3.2. Travail sur archives

Nous avons passé une semaine en avril 2016 dans les salles d'archives de l'OCDE pour y récupérer, sur clef USB, le plus possible de documents sur la protection de la vie privée et des données personnelles produits pendant la période étudiée. À l'exception de quelques cartons de courrier interne ne contenant pas de discussions sur la protection des données, mais seulement sur l'organisation du travail interne au secrétariat de l'OCDE, nous avons travaillé sur microfiches et microfilms. Les références des documents auxquels nous avons eu accès ont été trouvées sur le catalogue en ligne de l'OCDE. Puis, une fois sur place, nous avons identifié des cotes correspondant aux groupes qui nous intéressaient. Par exemple, la cote DSTI/CUG désigne tous les documents produits par ou pour le groupe informatique (en anglais : *Computer Utilization Group*, ou CUG) de la Direction de la science, de la technologie et de l'industrie (DSTI). La plupart des documents de l'OCDE étaient disponibles dans les deux langues officielles : l'anglais et le français. Chaque document précisait la langue d'origine du document, et le niveau de classification d'origine (en général : « diffusion restreinte »). Ci-dessous, nous voyons le haut de la première page du 36e document daté de 1976 et rédigé par ou pour le groupe informatique de l'OCDE :



ORGANISATION DE COOPERATION
ET DE DEVELOPPEMENT ECONOMIQUES

Direction de la Science, de la
Technologie et de l'Industrie

Groupe Informatique

DSTI/CUG/76.36
Barème E

DIFFUSION RESTREINTE

Paris, le 15 novembre 1976

Or. angl.

SOUS-GROUPE SUR LES BANQUES DE DONNEES

LE MOUVEMENT TRANSFRONTIERES ET LA PROTECTION DES DONNEES

Principes et directives

Figure 2 : *En-tête typique d'un document de l'OCDE récupéré sur microfiches, ici un rapport du sous-groupe sur les banques de données du groupe informatique de la Direction de la science, de la technologie et de l'industrie de l'OCDE, daté du 15 novembre 1976, traduit en français depuis l'anglais, et classé « diffusion restreinte ».*

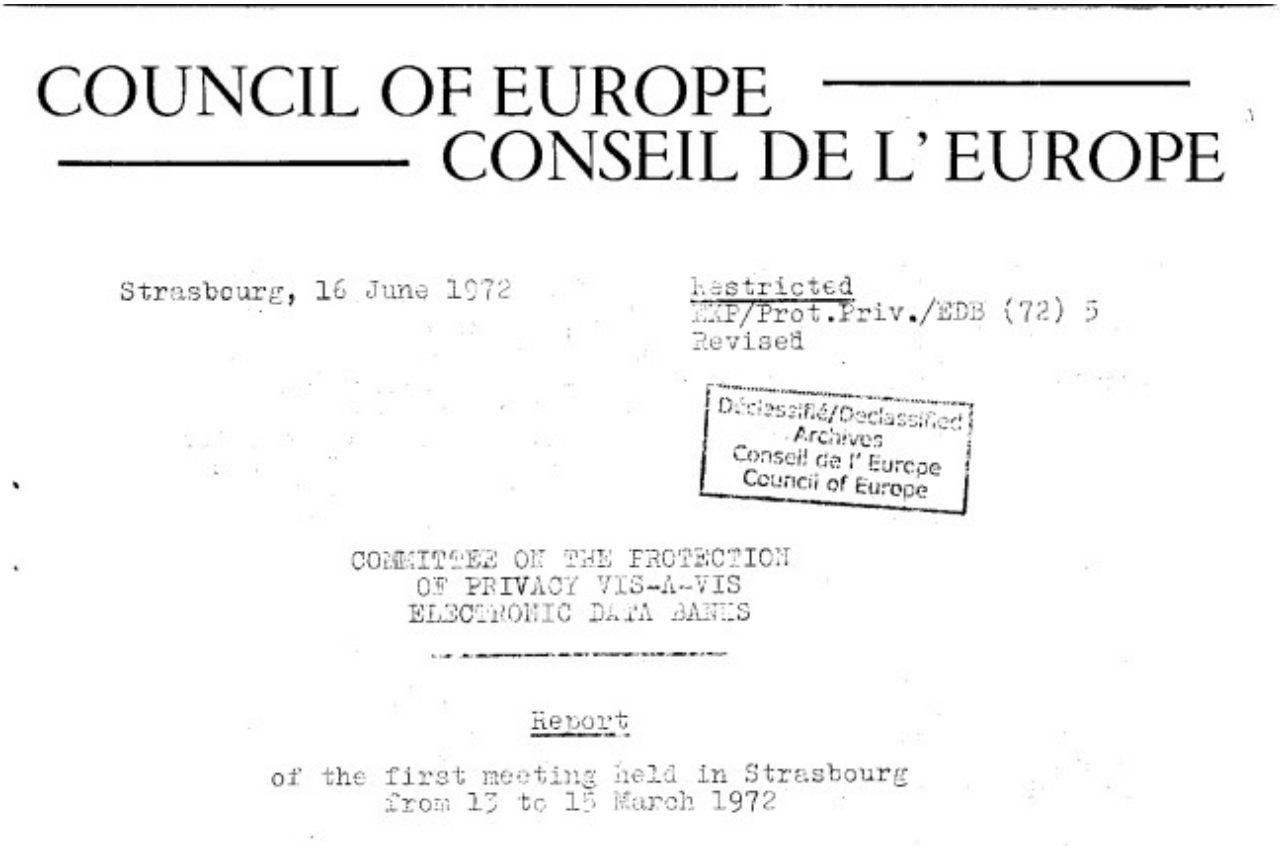
Il n’a pas été aussi simple d’accéder aux archives du Conseil de l’Europe, car elles sont généralement fermées au public, pour des raisons de restriction de moyens. Voici un extrait de la réponse que nous avons reçue à notre demande de rendez-vous de mars 2016 :

> « L’accueil des archives est ouvert de façon exceptionnelle seulement. La prochaine ouverture aura lieu du 23 au 27 mai 2016. Nous pouvons accueillir 4 ou 5 chercheurs à la fois. Vous êtes inscrit sur liste d’attente. Nous vous tiendrons informé si nous pouvons vous accueillir. » (e-mail de Archives@coe.int reçu le 30 mars 2016)

Au final, il n’a pas été possible d’accéder physiquement aux archives du Conseil de l’Europe. Nous avons dû nous contenter des documents numérisés et disponibles en ligne[21]. Or, très peu de documents sur la période entre 1975 et 1981 y ont été publiés, ce qui a limité la quantité de documents sur cette période que nous avons pu intégrer à notre corpus. Cela n’a fort heureusement pas été un obstacle majeur car, comme nous le verrons dans le chapitre 3, l’essentiel des débats s’est déroulé entre 1970 et 1973, soit la période abondamment documentée dans les archives numériques. Enfin, notons que ces documents ont généralement été mis en ligne dans leur version anglaise, ce qui explique que la plupart du temps, la traduction en français que nous fournissons n’est pas la traduction officielle.

Le système de classement des documents du Conseil de l’Europe est similaire à celui de l’OCDE. Par exemple, le document dont le haut de la première page est reproduit ci-dessous est un rapport du groupe d’experts sur la protection de la vie privée vis-à-vis des banques de données électroniques. Il s’agit d’une version révisée du cinquième document archivé, produit pour ou par ce groupe, en 1972 :

21 Ce site est accessible à l’URL suivante : http://normalsup.coe.int/uhtbin/cgisirsi.exe/?ps=zDXURmPdMy/ARCHIVES/X/60/79/X (page consultée le 22 février 2019)



COUNCIL OF EUROPE
CONSEIL DE L' EUROPE

Strasbourg, 16 June 1972

Restricted
MMP/Prot.Priv./EDB (72) 5
Revised

Déclassifié/Declassified
Archives
Conseil de l' Europe
Council of Europe

COMMITTEE ON THE PROTECTION
OF PRIVACY VIS-A-VIS
ELECTRONIC DATA BANKS

Report

of the first meeting held in Strasbourg
from 13 to 15 March 1972

Figure 3 : *Haut de la première page de la version révisée du 5e document attribué en 1972 au groupe d'experts sur la protection de la vie privée vis-à-vis des banques de données électroniques du Conseil de l'Europe, daté du 16 juin, classé « diffusion restreinte », et portant la marque d'un tampon indiquant son caractère déclassifié, sans précision de la date de déclassification.*

Ces documents du Conseil de l'Europe et de l'OCDE ont, sauf mention contraire indiquée dans le document, été rédigés par des personnes du secrétariat de ces organisations intergouvernementales. Ils portent la trace des contributions des différentes délégations nationales aux groupes d'experts étudiés, mais ne permettent généralement pas de retrouver l'auteur individuel d'un propos. Ce sont dans tous les cas des documents qui ont circulé entre les participants de ces groupes de travail, et qui ont servi de documents de travail et de références communes pendant les réunions.

1.2.3.3. Entretiens

Les livres, témoignages écrits et documents d'archives de notre corpus ont été complétés par neuf entretiens conduits entre juin 2016 et novembre 2018 avec des personnes qui avaient été

témoins du début de l'histoire de la protection des données à caractère personnel. Parmi ces témoins, certains sont d'anciens membres des groupes d'experts étudiés. D'autres ont connu ces personnes et travaillé avec elles.

Ces entretiens avaient plusieurs objectifs.

Tout d'abord, ils nous ont aidé à reconstituer la chronologie des événements, et à comprendre le lien entre les événements de cette chronologie. Les entretiens ont aussi aidé à hiérarchiser les événements selon leur importance dans le souvenir des personnes interrogées. Par exemple, ils nous ont conduit à réévaluer à la hausse l'influence des débats sur la « vie privée » qui avaient eu lieu dans les années 1960 aux États-Unis dans la façon dont les acteurs européens ont cadré la question, et à nuancer le rôle du contexte de Guerre froide et d'une éventuelle aversion pour le type de surveillance politique qui pesait sur les sociétés en Europe de l'Est.

Le but était ensuite de susciter des discours sur la « vie privée », la « protection des données », le rôle et la légitimité des droits à ces deux objets, et le lien entre les deux. Nous avons aussi posé des questions sur l'image que les enquêtés se faisaient de l'informatique et des ordinateurs, sur les arguments qu'ils ont utilisés, et sur ceux auxquels ils devaient répondre. Cela nous a été précieux pour comprendre l'axiologie de ces personnes, confirmer l'hypothèse empruntée à Colin Bennett et Charles Raab (2003) d'une inspiration libérale, mais aussi pour comprendre et mieux percevoir des lignes de débat qui ne ressortent pas de documents d'archives policés, écrits dans un souci de consensus, dans un contexte très institutionnel et administratif, généralement par des employés de secrétariats censés rester neutres dans les débats. C'est grâce à ces entretiens que nous avons pu percevoir le rôle de la différence de culture juridique entre juristes de *Common Law* et de droit continental dans la structuration des débats de l'époque[22].

Les entretiens ont aussi contribué à rendre plus vivants les documents d'archives en permettant de mieux comprendre le contexte dans lequel ils ont été rédigés. Quelle était l'ambiance ? Quel était le rythme de travail ? Quel était l'état des relations interpersonnelles entre les différents acteurs ? Quels avaient été leurs parcours personnels ?

Enfin, si les entretiens ont permis de relever ou de retrouver la trace de certains événements factuels, ils ont aussi fourni du matériau pour l'analyse des discours d'acteurs, aux côtés des témoignages écrits et documents d'archives de notre corpus.

Le tableau ci-dessous fait une liste des entretiens réalisés. L'annexe 15 précise pour chaque personne les raisons biographiques qui nous ont conduit à leur proposer de témoigner sur l'histoire de la protection des données, lorsque ces informations biographiques sont publiquement disponibles.

22 Cf. section 3.7.

	Nom	Prénom	Date	Lieu de l'entretien	Pays de résidence
HIST 1	Hustinx	Peter	15 juin 2016	Ville de taille moyenne aux Pays-Bas[23]	Pays-Bas
HIST 2	Simitis	Spiros	27 septembre 2016	Francfort sur le Main	Allemagne
HIST 3	Kirby	Michael	7 octobre 2017	Par téléphone	Australie
HIST 4	Frank	Alice	16 octobre 2017	Banlieue d'une ville de taille moyenne au Royaume-Uni	Royaume-Uni
HIST 5	Delahaie	Henri	13 novembre 2017	Paris	France
HIST 6	Sólyom	László	20 novembre 2017	Budapest	Hongrie
HIST 7	Corell	Hans	24 novembre 2017	Par visioconférence	Suède
HIST 8	Vitalis	André	20 avril 2018	Banlieue d'une grande ville française	France
HIST 9	Georges	Marie	29 novembre 2018	Paris	France

Tableau 4 : *Liste des entretiens réalisés dans le cadre du terrain sur la socio-genèse de la protection des données*

Le recrutement s'est fait au départ en repérant des personnes ayant encore une activité professionnelle, ou en contactant le dernier employeur connu d'une personne pour qu'il transmette notre demande d'entretien à l'intéressé. Cela n'a pas toujours fonctionné. Certains

23 Nous n'indiquons pas la ville précise lorsque cette précision donnerait des indications sur le lieu de résidence privée des enquêtés.

employeurs ont refusé de transmettre notre demande. L'une des personnes que nous souhaitions interroger est décédée alors que nous étions en train de rédiger le courrier de demande d'entretien. Dans d'autres cas, la personne contactée a décliné notre demande pour cause de problèmes de santé. Parfois, il a fallu d'abord convaincre la famille, qui, dans un cas, n'a pas accepté de transmettre notre demande. Il y a également quelques rares refus de principe à participer à une campagne d'entretiens.

À la fin de chaque entretien, nous avons demandé qui il serait encore intéressant de contacter. Souvent, les personnes interrogées avaient gardé les coordonnées d'anciens collègues ou amis, et étaient encore en contact plus ou moins régulier avec eux. Cela nous a permis d'entrer en contact avec certaines personnes dont nous n'avions pas réussi à trouver les coordonnées en ligne.

1.2.3.4. Autres documents

Nous nous sommes concentré dans notre enquête sur les groupes d'experts du Conseil de l'Europe[24] et de l'OCDE[25]. Mais les documents et réponses aux entretiens que nous avons collectés font souvent référence à d'autres événements, ou documents, ou idées, exogènes à ces groupes. Ces documents peuvent être des livres, des rapports rédigés à un niveau national et non intergouvernemental, ou encore des ouvrages de science-fiction : les références à *Big Brother* du roman *1984* de George Orwell, sont nombreuses dans notre corpus. Ainsi, une section entière sera dédiée[26] à la problématisation de la vie privée dans un contexte de développement de l'informatique aux États-Unis dans les années 1960, car elle a précédé et influencé les discussions au Conseil de l'Europe et à l'OCDE. Puisque la méthode que nous avons choisie est une méthode « archéologique » (Foucault, 2008 [1969]), il fallait exhumer strate après strate les discours et documents produits en partant de l'époque la plus récente pour remonter dans le temps en suivant la piste des références bibliographiques, des références littéraires et artistiques, et des sources d'inspiration décrites dans les verbatims d'entretiens. En procédant de la sorte, nous avons observé un lien fort entre les discussions en Europe et celles des années 1965 à 1970 aux États-Unis, d'où a été importée la controverse sur l'ordinateur et la « vie privée » à partir de la toute fin des années 1960, où elle a suivi son propre cours pour donner naissance à une formule nouvelle : la « protection des données », qui elle-même a donné son nom à la catégorie nouvelle de droit fondamental qu'est le droit *à la* protection des données à caractère personnel, autour duquel une nouvelle catégorie de l'action publique s'est structurée.

Le RGPD, sur l'élaboration duquel porte notre troisième terrain, est aujourd'hui un instrument central de ce secteur de l'action publique en Europe.

24 Cf. section 3.4.2.
25 Cf. section 3.4.3.
26 Cf. section 3.2.

1.2.4. L'adoption du Règlement général de protection des données

1.2.4.1. La jurisprudence de la Cour de justice de l'Union européenne

En 1995, l'Union européenne a adopté une directive sur la protection des données à caractère personnel[27], harmonisant différentes lois nationales, et transférant du Conseil de l'Europe aux institutions communautaires le lieu central de la production de droit *de la* protection des données en Europe[28]. La Cour de justice de l'Union européenne (CJUE) a rendu des arrêts, depuis le début des années 2000, précisant l'interprétation valable, ayant autorité de la chose jugée, des dispositions de cette directive. Ces affaires ont été l'occasion pour différents acteurs de tenter d'infléchir l'interprétation de la définition de « donnée à caractère personnel » inscrite dans la directive dans le sens de leurs intérêts[29], qui sont eux-même le fruit de cadres d'interprétation socialement construits.

Certaines de ces affaires datent de plusieurs années avant le moment où, en 2009, la Commission européenne a annoncé son intention de réformer le cadre juridique de la directive de 1995, puis se sont poursuivies en parallèle des « discussions[30] » sur le RGPD qui se prolongèrent jusqu'à l'adoption définitive du texte en 2016, et qu'elles ont influencé. Nous les avons donc toutes intégrées à notre terrain, même lorsqu'elles datent d'avant 2009. La liste des décisions de la CJUE lues et discutées dans le chapitre 6 est disponible en annexe 12.

À l'exception du corpus jurisprudentiel nous ayant permis de décrire et analyser les tentatives de modifications de l'interprétation de la notion juridique de la notion de « donnée à caractère personnel » du droit de l'Union européenne, notre terrain sur l'adoption du RGPD porte sur la période qui va de 2009 à 2016.

1.2.4.2. Identification du terrain

Les questions qui ont guidé notre étude de l'adoption du RGPD ont été les suivantes : quels ont été les points de controverse dans les débats ayant précédé l'adoption du RGPD, pour les acteurs impliqués dans le processus de décision ? Quels ont été les référentiels de ces acteurs,

27 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

28 Cf. section 4.1.2.

29 Cf. section 6.3.

30 Nous reviendrons sur le sens de ce mot en section 4.1.5.

et, afin de les repérer, quels ont été les discours et arguments produits par ces derniers ? Y répondre n'a pas été aisé, pour des raisons à la fois méthodologiques et pratiques.

Le premier obstacle à l'étude des controverses autour de la proposition de réforme du droit *de la* protection des données à caractère personnel proposée par la Commission européenne était l'absence déjà évoquée de véritable espace public européen, efficace au sens de Nancy Fraser (2007), à partir duquel constituer un corpus de sources médiatiques.

L'UE n'est pas seulement intergouvernentale, mais prétend être dotée d'institutions politiques et démocratiques supranationales. Il existe des élections européennes, qui ont lieu tous les cinq ans depuis 1979. La Commission européenne est responsable devant le Parlement, supranational, élu au suffrage universel direct. Depuis le traité de Maastricht, il existe même une citoyenneté de l'UE[31]. Le caractère post-westphalien et supranational de l'UE, et l'existence d'une citoyenneté européenne pourraient permettre d'envisager, comme le fait Jürgen Habermas (2000), l'existence d'un espace public européen en dehors du cadre national dans lequel a été pensé le concept d'espace public (voir : Fraser, 2007).

Sa défense d'un espace public européen nous semble toutefois plus relever d'une intention normative que descriptive et empirique. Il n'existe pas d'équivalent à l'échelle européenne d'un espace public national, mais seulement, au mieux des espaces publics sectoriels, étroits et « dépendants des institutions où des acteurs politiques mènent des débats européens sur des questions européennes » (Dacheux, 2008). Il existe bien quelques organes de presse, comme *Euronews* pour la télévision, *European Voice* (devenu *Politico Europe* en 2014) pour la presse hebdomadaire écrite, ou encore *Euractiv* pour la presse en ligne. Leur diffusion demeure toutefois confidentielle, centrée sur les personnes exerçant une profession en lien avec l'activité des institutions de l'Union européenne. C'est d'ailleurs le public que cible *Politico Europe*, qui indique sur sa page web dédiée à la vente d'espace publicitaire qu'une publication dans leurs colonnes « est la meilleure façon de s'adresser aux décideurs publics, régulateurs et leaders intellectuels européens[32] ». Enfin, il existe des médias sectoriels propres au champ de la protection des données à caractère personnel, comme le mensuel *Privacy Laws & Business*, mais sa diffusion est d'autant plus restreinte que son prix est élevé (105£ par numéro en mai 2019).

Quel espace public observer pour réaliser une analyse des controverses sur le RGPD ? D'un espace public européen pratiquement inexistant, en tout cas au sens où l'entend Jürgen Habermas ? Des vingt-huit espaces publics nationaux – si tant est qu'il soit toujours possible de

31 Voir l'art. 9 TUE, 20 TFUE et la directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) n° 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE

32 Traduction de l'auteur. Texte original : « Advertising with POLITICO is the best way to reach European policymakers, regulators and thought leaders. » Voir : https://www.politico.eu/advertising/ (page consultée le 31 mai 2019).

parler d’espaces publics nationaux, notamment dans les États fédéraux – composant l’UE ? De publications liées à des espaces publics sectoriels, comme *Privacy Laws & Business* pour les professionnels de la protection des données ? Ou bien des journaux en ligne spécialisés dans l’actualité de l’informatique et du « numérique », comme *ZDNet* ?

Une première piste aurait pu être d’aller étudier les controverses dans les espaces publics nationaux, ou dans un ensemble d’arènes dispersées. Une telle approche a par exemple été développée par Caroline Ollivier-Yaniv (à paraître) pour l’étude des controverses vaccinales en France, où la controverse traverse des arènes dispersées et fonctionnant selon des règles et des contraintes différentes, comme les arènes scientifiques, institutionnelles et des « médias institutionnels ». Une autre approche pourrait être d’étudier la réception dans les médias d’espaces publics nationaux et fragmentés des discours et production normative de l’UE en matière de politiques publiques de protection des données. Dans une telle approche, les journalistes des médias nationaux pourraient être décrits comme un public institutionnel des institutions de l’Union. Étudier la réception médiatique des publics institutionnels (Ollivier-Yaniv, 2019) nous paraît adapté avant tout à l’étude de la réception des politiques publiques (Revillard, 2018). Or, cela n’est pas l’objet de notre terrain qui porte ici sur le processus d’adoption du RGPD, en amont de la phase qui, à partir de 2016, visait par la communication institutionnelle à faire connaître, et à légitimer, les règles du RGPD, pour préparer son entrée en application à partir du 25 mai 2018.

Dans la construction de notre corpus, nous avons concentré nos efforts sur les documents produits ou circulant dans des arènes formelles et informelles, dispersées et hétérogènes qui ont pour point commun d’avoir une certaine « efficacité », c’est-à-dire que les discours qui y circulent et qui y sont construits peuvent effectivement produire des effets sur la production du domaine de l’action publique étudié (voir : Fraser, 2007). Sélectionner un corpus d’articles en commençant par sélectionner des espaces médiatiques *a priori* représentatifs des controverses auxquelles ont participé les acteurs qui ont rédigé le RGPD était impossible en raison de l’absence d’espace public européen au sens propre du terme, et de la dispersion des arènes pertinentes et efficaces, dont une grande partie était en tout ou partie confidentielles. Nous avons donc opté pour une autre démarche. Au lieu de partir des arènes publiques, nous sommes parti des acteurs impliqués dans le sous-système de politique publique de protection des données de l’UE pour voir où s’exprimaient ces derniers, comment ils ont échangé et débattu pendant le processus d’adoption du RGPD, de 2009 à 2016.

Un deuxième obstacle était l’éclatement linguistique de notre corpus. Si les documents produits par le Conseil de l’Europe ou l’OCDE sont dans l’une des langues officielles des organisations intergouvernementales (le français et l’anglais), l’Union européenne disposait en 2009 de 23 langues officielles, et de 24 en 2016, dont l’allemand, le français ou l’anglais mais aussi le finnois, l’irlandais et le maltais. Toutes ces langues peuvent être utilisées. Certaines le

sont moins que d'autres. L'anglais domine ainsi très largement. C'est la langue dans laquelle la majorité des documents de notre corpus était rédigée, et celle à partir de laquelle l'essentiel de nos analyses de discours a été effectué. Malgré tout, le corpus de documents que nous nous sommes procurés contenait de nombreux textes rédigés dans d'autres langues. Parmi ceux-ci, nous n'avons été capables de prendre en compte que ceux rédigés en français, néerlandais, hongrois, italien ou castillan et, dans une moindre mesure et en sollicitant, pour les documents importants, l'aide d'amis et de collègues germanophones : l'allemand.

L'étude des représentations des acteurs impliqués dans l'adoption du RGPD et des échanges d'arguments entre coalitions de cause rivales nous a conduit à adopter une démarche principalement qualitative et interprétative, où il s'est agi d'essayer de repérer les référentiels auxquels les discours faisaient référence. Pour y parvenir, une certaine forme d'immersion dans le milieu étudié était nécessaire, afin de maîtriser les codes des discours étudiés et de faciliter le travail d'interprétation. Nous avons ensuite opéré une sélection d'un corpus de documents, qui sont pour l'essentiel des *position papers* de groupes d'intérêt et des documents institutionnels du Parlement européen, de la Commission européenne et du Conseil de l'Union européenne. Nous avons complété ce corpus par des entretiens qualitatifs avec des acteurs du processus d'adoption du RGPD. Enfin, nous avons expérimenté des méthodes quali-quantitatives assistées par ordinateur pour essayer de cartographier les coalitions de cause rivales structurant la controverse[33].

Le croisement de ces différentes méthodes (exploration par immersion ethnographique, analyse de discours et de documents, expérimentation de méthodes quali-quantitatives de cartographie des controverses, entretiens semi-directifs) avait pour but de limiter les effets de la subjectivité de l'interprétant (Bowen, 2009), indispensable aux méthodes interprétatives, mais qui peut, s'ils ne sont pas pris en compte et en l'absence de réflexivité (Beaud et Weber, 2017 ; Le Guern, 2007 ; Paugam, 2012) ou de croisement de méthodes, aboutir à des conclusions totalement étrangères aux acteurs du terrain et ne faisant que renforcer les préjugés initiaux du chercheur. Il nous paraissait indispensable, pour éviter cet écueil, de nous confronter aux points de vue des acteurs du terrain par ces entretiens, mais aussi par une démarche d'exploration et de fréquentation du terrain inspirée des méthodes ethnographiques.

1.2.4.3. Exploration ethnographique

Deux stages, l'un à l'Autorité nationale pour la protection des données et la liberté de l'information (*Nemzeti Adatvédelmi és Információszabadság Hatóság* – NAIH) en Hongrie puis à la Commission nationale de l'informatique et des libertés (CNIL) en France en 2014 ont ainsi

33 Cf. section 4.2.

contribué à mon[34] immersion dans le champ social étudié. Je suis également adhérent depuis 2014 de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP), dont je participe régulièrement aux rencontres (« Université du correspondant informatique et libertés » en janvier, assemblée générale annuelle en mai ou juin). J'ai également participé à l'organisation d'un atelier européen sur la réparation du préjudice subi par les personnes concernées à cause d'une infraction à leur droit *à la* protection des données en avril 2018[35], avec des chercheurs, des avocats et des militants associatifs. En 2019, j'ai été invité par une personne travaillant à l'UNESCO à intervenir en tant que modérateur d'une session de l'*Internet Governance Forum* (IGF) à Berlin.

Ma fréquentation du terrain a été inspirée par des méthodes ethnographiques appliquées à la « fabrique du droit » (Latour, 2004). L'idée était à la fois de me familiariser avec celui-ci et avec l'univers symbolique des membres du terrain, mais aussi d'utiliser la méthodologie réflexive de l'ethnographie pour correctement intégrer à la réflexion ces expériences participantes dont certaines ont précédé le début de la thèse.

Dans son étude sur les défenseurs de la vie privée et sur la « *privacy community* », Colin Bennett (2008) insiste sur le rôle structurant que jouent les conférences (« *privacy conferences* ») dans leur socialisation, et sur l'importance de s'y rendre pour appréhender ce terrain :

> « […] les défenseurs de la vie privée vont à beaucoup de conférences. Les présentations formelles qui y sont données et le réseautage informel ont aussi beaucoup contribué à ma compréhension et à mes analyses[36] » (Bennett, 2009, p. xix)

Ces conférences sont également des lieux publics d'échange et de débat où s'expriment différents points de vue, arguments et discours. Elles sont également l'occasion de nombreux entretiens informels permettant de valider des hypothèses d'interprétation de discours et de prises de position d'acteurs, mais aussi d'apprendre et de se tenir informé d'événements n'ayant pas

34 Cette thèse est écrite à la première personne du pluriel. Cela est conforme aux usages académiques traditionnels, et permet aussi, d'une certaine façon, de rappeler que le travail d'un chercheur n'est jamais tout à fait solitaire. Nous nous reposons en réalité en permanence sur des savoirs et des réflexions produits par les gens qui nous entourent (Origgi, 2004). Dire « nous » est une façon de rappeler cette réalité.
Malgré tout, j'ai fait le choix de m'exprimer par moments à la première personne du singulier pour parler d'expériences personnelles ayant influencé ma démarche de recherche, lorsque leur narration à la première personne du pluriel aurait relevé plus d'un « nous » aristocratique et prétentieux que d'un « nous » académique.

35 Voir le compte-rendu sur le site de l'ISOC France : https://www.isoc.fr/cr-atelier-europeen-protection-donnees-personnelles-25-avril/ (page consultée le 31 mai 2019)

36 Traduction de l'auteur. Texte original : « « […] privacy advocates attend a lot of conferences. The formal presentations at these events, as well as informal networking also contributed to my understandings and insights »

nécessairement fait l'objet d'une communication au public. L'un des enquêtés a d'ailleurs évoqué l'importance de s'y déplacer et de s'y exprimer pour le travail de plaidoyer :

> « Donc quelques experts de CDT sont venus en Europe à ce moment-là, à plusieurs conférences, pour participer aux débats, et ainsi de suite[37]. » (Entretien avec Jens-Henrik Jeppesen)

Certaines de ces conférences, comme la conférence *Computers, Privacy and Data Protection* (CPDP) ou *Privacy Camp*, sont ouvertes au public. D'autres événements ne sont ouverts qu'aux membres, comme l'Assemblée générale et l'Université annuelle de l'AFCDP. Certaines conférences sont à huis clos, et ne peuvent y être présentes qu'une liste limitée de personnes invitées. C'est le cas par exemple de la Conférence de printemps des autorités européennes de protection des données. D'autres, enfin, comme l'*International Conference of Data Protection and Privacy Commissioners* (ICDPPC), est répartie entre des temps et des espaces ouverts au public, et d'autres à huis clos.

Ces conférences peuvent être organisées par différents types d'organisations. L'Université des CIL de l'AFCDP, ou le *Global Privacy Summit* de l'IAPP, sont par exemple l'œuvre d'organisations de professionnels de la protection des données. La *Privacy Law Scholars Conference* est quant à elle à dominante académique et juridique. L'*Information Ethics Roundtable* est une conférence universitaire interdisciplinaire. L'ICDPPC et la Conférence de printemps réunissent les autorités de protection des données. *Privacy Camp* est une conférence organisée sur une journée chaque année à Bruxelles, juste avant la CPDP, par des ONG. Enfin, certaines conférences réunissent une diversité d'acteurs, comme la CPDP, qui semble être la conférence la plus importante, celle à ne pas manquer, pour bon nombre des acteurs impliqués dans les politiques publiques de protection des données. Selon les chiffres des organisateurs, cette conférence a ainsi attiré, en 2018, 420 intervenants, et 1100 inscrits, venus de 55 pays différents[38]. D'autre conférences sont de taille plus modeste, avec un public plus ciblé.

Certaines conférences récurrentes, bien que n'ayant pas pour thème spécifique la protection des données ou le RGPD, portent sur des thèmes qui incluent ce sujet. C'est le cas notamment de l'*Internet Governance Forum* (IGF) organisé chaque année par l'UNESCO, et de ses déclinaisons nationales. C'est également le cas des conférences sur les données numériques et leurs usages, comme le Salon de la Data qui a lieu tous les ans à Nantes.

Généralement, ces conférences sont organisées en deux espaces : un espace de conférence formelle, avec des panels, et des espaces de réseautage organisés de sorte à favoriser les

37 Traduction de l'auteur. Texte original : « « So some CDT experts have come to Europe at the time, at various conferences, participating in debates, and so on. »

38 Voir : https://www.cpdpconferences.org/press (page consultée le 31 mai 2019).

rencontres et les échanges informels. Chaque personne est identifiée par un badge portant son nom et son affiliation professionnelle, afin de faciliter ces rencontres.

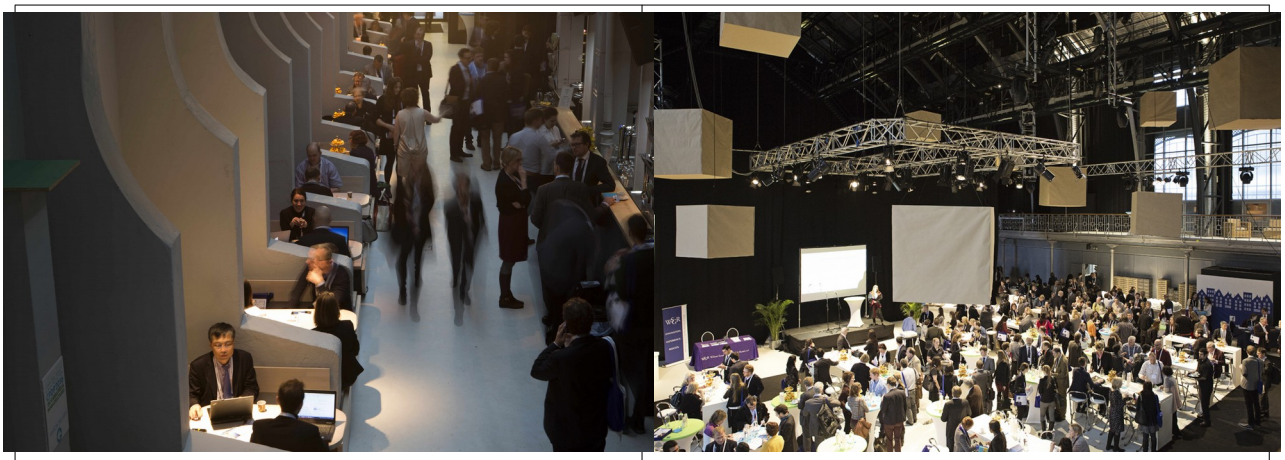


Figure 4 : *Espaces de socialisation informelle et de réseautage à la CPDP. Crédits photo : CPDP Conferences*[39]

Chaque déplacement a été l'occasion d'apprendre, de nouer des contacts formels et informels avec des acteurs du sous-système de politique publique étudié, de repérer et de démarcher des personnes susceptible de participer à la campagne d'entretiens, et de prendre des notes dans des carnets ou sur ordinateur sur les échanges observés. J'ai également participé en tant qu'intervenant à certaines de ces conférences, comme à l'édition 2015 de l'Université des CIL pour une présentation du G29, au Forum sur la gouvernance d'Internet français de 2018 et à l'édition 2019 de la CPDP et de l'IGF en tant que modérateur de panel[40].

Le nombre de déplacements à des conférences a été limité par plusieurs facteurs. L'investissement en temps est élevé, puisqu'il faut parfois bloquer plusieurs journées de conférences en plus de demi-journées voire de journées entière de trajet. Le coût d'inscription à une conférence peut s'élever à plusieurs centaines d'euros, sans compter les frais de déplacement et d'hébergement. Malgré les divers financements obtenus[41], il a ainsi fallu renoncer à me rendre à toutes les conférences qui auraient été pertinentes pour l'enquête.

39 Voir : https://cpdpconferences.net/CPDP2016-pictures.zip (ressource consultée le 31 mai 2019)

40 La vidéo de cette dernière intervention a été mise en ligne sur Youtube : https://www.youtube.com/watch?v=6XQjCntmJMY (page consultée le 31 mai 2019)

41 Le projet ANR ENEID-Éternités numériques, le groupe EPIN du laboratoire COSTECH de l'Université de technologie de Compiègne, le projet PROFILE du Cominlabs, et l'Internet Society France ont tous contribué financièrement à ces déplacements.

Les principales conférences auxquelles j'ai pu assister et/ou participer au cours de la thèse, dans le cadre de l'exploration du présent terrain, ont été les suivantes :

- Les éditions 2014, 2015 et 2019 de l'Université des CIL (renommée « Université des DPO » en 2019) de l'AFCDP à Paris et dans des villes de la banlieue parisienne[42] ;
- L'édition de 2016 de la Conférence de printemps des autorités européennes de protection des données, sur invitation de l'autorité hôte, à Budapest (*Budapest Spring Conference 2016*[43]) ;
- Les assemblées générales 2016, 2017, 2018 et 2019 de l'AFCDP à Issy-les-Moulineaux puis à Paris ;
- Les éditions 2016 à 2020 de la CPDP à Bruxelles[44] ;
- L'édition 2017 du Salon de la Data de Nantes[45] ;
- Les éditions 2017 à 2019 de *Privacy Camp* à Bruxelles[46] ;
- L'*Internet Ethics Roundtable* de 2018 à Copenhague[47] ;
- Les éditions 2018 et 2019 de l'*Internet Governance Forum* mondial, à Paris et à Berlin, et du Forum sur la gouvernance d'Internet français à Paris en 2018 et 2019[48].
- L'édition 2019 de l'ICDPPC à Tirana.

Cette démarche d'observation ethnographique exploratoire a aidé à connaître et à comprendre les codes du sous-système de politiques publiques de protection des données à caractère personnel, qu'il fallait apprendre pour se doter des clefs de compréhension des documents étudiés. Cette phase a commencé avant la phase d'entretiens et d'analyse de documents, et s'est poursuivie pendant l'ensemble de la thèse.

1.2.4.4. Analyse qualitative de documents

La liste des documents cités dans le cadre de l'analyse quantitative de documents en rapport avec l'adoption du RGPD est disponible dans la bibliographie. La liste exhaustive des documents récupérés est disponible en annexe 4. Elle comprend :

42 Voir : https://afcdp.net/ (page consultée le 31 mai 2019).
43 Voir : http://www.naih.hu/budapest-springconf/ (page consultée le 31 mai 2019).
44 Voir : https://www.cpdpconferences.org/ (page consultée le 31 mai 2019).
45 Voir : https://salondata.fr/ (page consultée le 31 mai 2019).
46 Voir : https://privacycamp.eu/ (page consultée le 31 mai 2019).
47 Voir : http://www.ier2018.info/ (page consultée le 31 mai 2019).
48 Voir : https://www.intgovforum.org/multilingual/content/igf-2018-0 et https://www.isoc.fr/ateliers/ (pages consultées le 31 mai 2019).

- Des documents officiels des institutions de l'Union européenne (Commission, Conseil et Parlement) :
  - Des communications, communiqués de presse et propositions législatives de la Commission européenne ;
  - Des listes d'amendements déposés par des parlementaires européens ;
  - Des documents produits par le secrétariat et par la présidence du Conseil de l'UE ;
  - Des notes envoyées par les délégations nationales au Conseil de l'UE.
- Des documents produits par les autorités de protection des données à caractère personnel, et en particulier par le Groupe de travail de l'Article 29 ;
- Des *position papers* produits par les groupes d'intérêt ayant cherché à influencer le résultat du processus d'adoption du RGPD et la rédaction du texte final (voir la liste en bibliographie et en annexe 4).

Le terme anglais « *position paper* » n'a pas de traduction en français. Il peut être traduit par « papier de positionnement », « exposé de position », « document d'orientations », « document de prise de position politique » ou d'autres périphrases cherchant à désigner un document écrit qui expose la position d'une organisation sur une question politique, et peut contenir des propositions de mesures concrètes, comme des textes de dispositions juridiques à adopter, ainsi que des arguments pour convaincre le lecteur. Ces documents sont souvent, mais pas nécessairement, produits par des professionnels du plaidoyer ou des militants bénévoles. Ils ont pour destinataire les décideurs publics qui ont la compétence et le pouvoir d'adopter les décisions politiques revendiquées par ses auteurs.

Un grand nombre de *position papers* ont été produits par les groupes d'intérêt qui ont cherché à influencer le processus d'adoption du RGPD. Certains ont été produits en réponse à des consultations organisées en 2009[49] et en 2010[50] par la Commission européenne. Ceux-ci ont été téléchargés depuis la page web de la Commission européenne où ils avaient été mis en ligne. D'autres ont été rédigés et envoyés à des destinataires spécifiques, notamment des parlementaires, sans qu'ils aient nécessairement été publiés, ou conçus pour être répertoriés. Le collectif de militants Lobbyplag a réuni 102 de ces documents en mars 2013 sur son dépôt Github[51], qui ont été téléchargés et intégrés à notre corpus d'analyse. Au total, nous avons récupéré 561 « *position papers* ».

49 Voir : https://ec.europa.eu/home-affairs/what-is-new/public-consultation/2009/consulting_0003_en (page consultée le 20 février. Depuis, le lien semble ne plus fonctionner)

50 Voir : https://web.archive.org/web/20101107205129/http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm (page consultée le 31 mai 2019)

51 Voir : https://github.com/lobbyplag/lobbyplag-data/tree/master/raw/lobby-documents (page consultée le 31 mai 2019)

Le grand nombre de documents recueillis a rendu nécessaire de faire des sélections dans le corpus au moment de l'analyse. Certains documents ont été choisis pour la centralité du rôle joué par le groupe d'intérêt les ayant produits selon l'avis des personnes interrogées en entretien. Cela concerne par exemple les documents de Digitals Rights Europe (EDRi) et de la Chambre de commerce des États-Unis en Europe (AmCham EU). Pour compléter cela, un script Python a été réalisé, pour repérer une liste de mots-clefs, comme « consent », « growth », « trust » ou encore « westin[52] ». Ce script a généré un tableau montrant, en face de chaque document PDF correspondant à un *position paper*, les pages où le terme était cité. Quelques autres documents, enfin, ont été choisis au hasard. Cela a permis de naviguer de façon praticable dans le corpus et de sélectionner des passages qui sont, sinon les plus pertinents, du moins plus pertinents que s'ils avaient été sélectionnés au cours d'une sélection totalement aléatoire.

Malgré tout, l'analyse qualitative de documents doit prendre en compte l'existence d'un effet de sélection qui, à l'inverse d'une exhaustivité au demeurant inatteignable, nous donne une vision certainement déformée de la réalité passée que nous tentons d'observer à partir de notre position située. Cet effet, généralement désigné comme étant un biais de sélection (Bowen, 2009), est renforcé dans notre cas par les caractéristiques d'un terrain en clair-obscur. En effet, rien ne garantit, et c'est même hautement improbable, que nous soyons parvenu à obtenir l'intégralité des *position papers* jamais écrits dans le cadre de la procédure d'adoption du RGPD. Il est même impossible de savoir ce que sont ceux dont nous ne disposons pas, ce qui veut dire que même si nous avons atteint cette exhaustivité – situation tout à fait exceptionnelle – alors nous n'avons aucun moyen de le savoir. Cela est également vrai pour les documents issus du Conseil de l'UE, dont seule une partie est immédiatement rendue publique, et dont le collectif Lobbyplag n'est parvenu à obtenir qu'une partie de ceux dont la diffusion devait être restreinte.

Il est indispensable de garder en mémoire dans un tel travail de terrain sur un processus législatif que les acteurs impliqués dans un sous-système de politique publique interagissent certes par écrit, et parfois par publications interposées, ou dans des débats publics, mais qu'ils échangent aussi très souvent entre eux, de façon informelle, soit via des canaux de communication privés (comme la messagerie électronique, les SMS et des applications de communication chiffrée comme Telegram, Whatsapp ou Signal) soit à l'oral, lors de réunions formelles ou de rencontres informelles. Ainsi, *Privacy Camp* et la CPDP sont chaque année l'occasion d'organiser de soirées à huis clos dans des bars de la capitale belge, où les participants font la fête, dansent, parfois s'enivrent, ensemble[53]. Ces échanges peuvent ne laisser aucune trace,

52 Les chaînes de caractères qui ont été recherchées par notre script (sans sensibilité à la casse) ont été : "big data", "consent", "children", "data mining", "research", "pseudonymous", "anonymous", "portability", "legitimate purpose", "processor", "right to be forgotten", "sovereignty", "legal certainty", "technical reality", "click fatigue", "surveillance", "fundamental right", "privacy", "digital single market", "single market", "westin", "orwell", "trust", "consumer demand", "growth", "jobs", "burdensome", "sme", "forum shopping", "innovation", "brandeis", "right to be let alone" et "control".

53 En 2019 et 2020, la fondation Mozilla a par exemple financé la soirée de la CPDP. Le titre de la soirée de 2019 était : « *Dance like no one is watching: the official CPDP party!* » (voir : https://www.cpdpconferences.org/events/dance-like-no-one-is-watching-the-official-cpdp-party ; page consultée le 31 mai 2019). En 2018, *Privacy Camp* organisait une soirée au Smouss Bar de Bruxelles :

autrement que dans la mémoire de ses protagonistes. Or, ils ont pu jouer un rôle tout aussi important que les communications écrites.

Ainsi, certains groupes d'intérêt très actifs n'ont laissé que très peu de traces écrites de leur activité de plaidoyer auprès des institutions européennes pendant le processus d'adoption du RGPD. De l'avis de plusieurs enquêtés, cela a notamment été le cas de Google :

> « Les principaux acteurs étaient globalement Microsoft et Google[54] » (entretien avec Razvan Antemir)

> « Google fait du lobby à l'échelle internationale contre la protection des données. Ils disent : "Regardez ces lois ridicules". Pour eux, c'est un outil de lobbying très efficace. Et c'est juste… […] très difficile à contrer. Ils n'ont presque rien écrit. Ils passent leur temps à appeler des journalistes. Ils font sortir le sujet dans la presse[55]. » (entretien avec Joe McNamee)

Effectivement, nous n'avons pu récupérer dans notre corpus aucun document signé directement par Google, alors que nous disposons de documents de Facebook, Yahoo, Microsoft ou encore eBay. Google a pourtant été très actif dans les discussions qui ont entouré l'adoption du RGPD. De fait, Rita Balogh, qui dirigeait l'équipe d'affaires publiques de Google à Bruxelles, est beaucoup intervenue à l'oral lors de multiples conférences qui, comme nous l'avons vu, jouent un rôle important dans la structuration de ce champ qu'est le sous-système de politiques publiques de la protection des données à caractère personnel[56].

1.2.4.5. Entretiens

Comme les documents, les entretiens ont servi à la fois de sources d'informations et, dans un second temps, de textes du corpus pour l'analyse de discours.

---

https://privacycamp.eu/?p=807 (page consultée le 31 mai 2019)

54 Traduit de l'anglais. Texte original : « The key players were basically Microsoft and Google ».

55 Traduit de l'anglais. Texte original : « Google lobbies against data protection globally. And if they can keep saying: well look at this ridiculous legislation, then it's a very effective lobbying tool for them. And it's just… […] it's very hard to account for. Because they've written virtually nothing down. They call journalists the whole time. They get the story out. »

56 Ses interventions sont pour partie disponibles en ligne, comme par exemple son intervention à un panel de 2017 de la conférence CPDP, intitulé « Data Protection and Data-Driven Innovation for Health Care and Biomedical Research », disponible sur Youtube : https://www.youtube.com/watch?v=7X-SxqophQA (page consultée le 9 mai 2019)

L'un des objectifs de ces entretiens était donc de pouvoir faire appel à la mémoire des acteurs de la controverse entourant l'adoption du RGPD pour saisir ce qui n'a pas été consigné par écrit ou qui n'est pas disponible publiquement. Les entretiens ont aussi été l'occasion de confronter une interprétation personnelle des documents analysés aux perceptions des acteurs du terrain. Ils ont servi à susciter des discours sur certains sujets spécifiques, comme sur la définition de ce qu'est le droit *à la* vie privée ou *à la* protection des données à caractère personnelles, et les raisons pour lesquelles ces droits doivent être défendus dans le cas des acteurs travaillant pour des associations militantes.

Les entretiens réalisés ont aussi aidé à identifier les coalitions de cause en demandant à chaque acteur interrogé qui étaient ses alliés et ses rivaux. Enfin, les enquêtés ont été invités à identifier une mesure concrète importante, ou une revendication phare de leur groupe d'intérêt. Puis, ils ont été interrogés sur leurs arguments pour soutenir cette mesure, les contre-arguments de leurs rivaux, et enfin leur façon de répondre à ces contre-arguments.

Les entretiens réalisés sont les suivants :

	Nom	**Prénom**	**Anonymat demandé**	**Date**	**Lieu**	**Organisation de rattachement**
Euro1[57]	M.	C.	INITIALES	19/10/16	Bruxelles	Groupe d'intérêt industriel européen
Euro2	Walkowiak	Anna	NON	08/12/16	Varsovie	Fundacja Panoptykon (ONG polonaise membre d'EDRi)
Euro3	Hötzendorfer	Walter	NON	05/05/17	Vienne	AT Research Institute (entreprise) et Epicenter Works (ONG)
Euro4	Antemir	Razvan	NON	06/11/17	Bruxelles	FEDMA puis Emota (groupe d'intérêt industriel européen)
Euro5			OUI	08/11/17	Bruxelles	Groupe d'intérêt industriel européen
Euro6		Jens-Henrik	NON	08/11/17	Bruxelles	CDT (ONG)

57 Dû au niveau de bruit dans la brasserie où l'entretien a été réalisé, cet entretien n'a malheureusement pas pu être pleinement exploité

	Jeppesen					
Euro7	Blanco	Laura	NON	08/11/17	Bruxelles	CDT (ONG)
Euro8	McNamee	Joe	OUI	09/11/17	Bruxelles	EDRi (ONG)
Euro9	Kallas	Kaja	NON	09/11/17	Bruxelles	Groupe ADLE (Parlement européen)
Euro10	Maurel	Lionel	NON	15/02/19	Paris	La Quadrature du Net (ONG)

Tableau 5 : *Liste des entretiens menés dans le cadre de l'enquête de terrain sur l'adoption du RGPD*

S'il a été plus facile qu'initialement prévu de prendre contact avec des salariés de groupes d'intérêt industriels, il a en revanche été plus difficile de solliciter des militants et employés d'ONG en raison des fortes sollicitations professionnelles qui pèsent sur eux. Les acteurs institutionnels, dans un contexte où le RGPD venait tout juste d'être adopté, étaient pour leur part trop sollicités pour répondre à nos demandes d'entretien. Seul un entretien a donc pu être réalisé avec une eurodéputée. C'est pourquoi, pour ces derniers, nous nous sommes finalement appuyés essentiellement sur les documents qu'ils ont produit, incluant, pour ce qui concerne le rapporteur du RGPD, un livre qu'il a publié sur le sujet (Albrecht, 2015a).

Une autre difficulté a été que l'essentiel des personnes sollicitées étaient basées à Bruxelles, alors que les périodes de séjour à Bruxelles ont été courtes et peu nombreuses pour des raisons financières. Les autres personnes interrogées n'étaient pas non plus nécessairement installées en France, car nous avons cherché à interroger des personnes de différentes nationalités et vivant dans différents pays pour refléter la dimension européenne du processus d'adoption du RGPD et éviter les biais du nationalisme méthodologique. Les visites pour motifs personnels à Vienne et à Varsovie ont été mises à profit pour y réaliser des entretiens avec des acteurs du terrain qui y habitaient. Les quelques demandes d'entretien par visioconférence n'ont pas abouti, peut-être en raison du fait qu'un chercheur ne se déplaçant pas pour réaliser l'entretien était perçu comme moins impliqué, moins motivé.

C'est en croisant ces différents types de documents provenant de différentes sources, et les différentes méthodes que nous venons d'exposer, que nous avons mené cette étude de terrain sur l'adoption du RGPD dans le sous-système de politique publique de l'UE de protection des données à caractère personnel. Cette étude sera présentée dans plus de détails dans le chapitre 4.

1.2.5. Le *Privacy Internet Group* et le *Tracking Protection Working Group* du W3C

1.2.5.1. Identification du terrain

Après avoir étudié deux terrains dominés sinon par des juristes, du moins par des personnes évoluant professionnellement dans un environnement juridique, nous avons étudié un terrain composé essentiellement d'ingénieurs informaticiens. L'idée était de comparer les discours qui y circulent avec ceux des deux terrains précédents, tout en tenant compte des spécificités de la façon dont s'y déroule la controverse sur le contenu à donner à la définition de la notion de « donnée à caractère personnel ».

Notre terrain devait se concentrer sur le *Privacy Interest Group* (PING) du W3C, qui est un groupe de travail ayant vocation à faire en sorte que les standards adoptés par le W3C soient compatibles avec l'objectif de protéger la « vie privée » des internautes. En raison de la proximité avec le PING, tant dans les missions, la composition, que dans la chronologie, du *Tracking Protection Working Group* (TPWG) du W3C, qui travaillait à l'élaboration d'un mécanisme permettant à des navigateurs de signaler aux serveurs Web la volonté de l'internaute de ne pas être pisté, il s'est avéré difficile d'opérer de réelle distinction entre les deux, et nous avons donc fait le choix d'étendre le champ de nos observations aux deux groupes.

Nous avons exploité quatre sources de matériau empirique : des entretiens qualitatifs, des courriers électroniques échangés par les acteurs sur des listes de discussion publiques, des documents produits par le PING et le TPWG, et une journée d'observation participante lors de la réunion annuelle du PING au *Technical Plenary and Advisory Committee* (TPAC) du W3C en octobre 2018 à Lyon.

1.2.5.2. Entretiens

Il existe une liste officielle des membres du W3C PING et du TPWG. Mais parmi ceux-ci, certains nous ont indiqué ne plus participer, ou ne pas vraiment avoir participé à l'un ou l'autre de ces groupes, lorsque nous les avons contactés pour un entretien :

> « Je ne savais pas que j'étais encore indiqué comme faisant partie de ce groupe. En fait je m'étais inscrit il y a quelques années parce que je pensais travailler sur le domaine […] et

diverses choses ont fait que cela ne s'est jamais fait » (Extrait d'un e-mail reçu le 24 mai 2017 avec quelqu'un contacté pour participer à la campagne d'entretiens)

Le critère qui a donc été choisi pour contacter des participants à ce groupe de travail ne fut pas celui d'être officiellement membre du W3C PING, mais de participer à la liste de discussion *public-privacy*, la liste de discussion utilisée par ses membres. Nombre d'entre eux participaient aussi à la liste *public-tracking* du TPWG, ce qui a contribué à la décision d'élargir le terrain du W3C PING *stricto sensu* au TPWG, et notamment à la controverse sur la définition du « *tracking* » qui s'y est déroulée[58].

Le flou concernant la barrière entre ces deux groupes est bien illustré par l'extrait d'entretien ci-dessous :

« Les gens que je connais de PING ça va être soit des personnes que je connais de Do Not Track, soit des gens que je connais autrement, lors de conférences ou de ce genre de choses. […] Comme de toutes façons sur ma boîte mail perso PING et Do Not Track vont dans le même répertoire, généralement, quand je browse […] je vois les deux en même temps. » (Entretien avec Vincent Toubiana)

Au total, nous avons contacté 18 personnes, sélectionnées pour leur activité (rôle de présidence, ancienneté, nombre d'e-mails échangés, employeur) ou parce que leur contact a été recommandé par un précédent enquêté. Cette approche a été préférée à un envoi massif à l'ensemble des personnes ayant participé pour plusieurs raisons :

- Tout d'abord, chaque prise de contact prend du temps, notamment en relances et en suivi des relances et des réponses, chaque e-mail devant être personnalisé pour parvenir à avoir une réponse positive, ce qui nécessitait à chaque fois d'étudier la biographie et les publications de la personne avant de prendre contact avec elle ;
- Ensuite, chaque questionnaire a été adapté à la marge à la personne interrogée. Comme un entretien durait entre 30 et 60 minutes, il fallait sélectionner pour chaque personne au moins un sujet sur lequel cette personne était particulièrement pertinente à interroger, en fonction d'éléments biographiques disponibles en ligne sur la personne ;
- Par ailleurs, nous avons voulu éviter l'effet de « spam » qui pourrait naître en envoyant à tous les participants un e-mail sur toutes leurs adresses e-mail ;
- Enfin, cela peut prendre du temps de retrouver les coordonnées d'une personne lorsqu'elle change d'employeur et devient moins active dans le cadre des activités du

58 Cf. section 5.5.

W3C, le W3C n'offrant pas d'annuaire public mis à jour des coordonnées des participants.

Sur ces 18 personnes contactées, 10 ont accepté l'entretien. Tous les entretiens sauf un ont été enregistrés et retranscrits. Il n'a été possible de réaliser en présentiel, pour des raisons de moyens limités et d'éloignement géographique des enquêtés, que deux des dix entretiens. Les entretiens ont duré entre 30 et 90 minutes selon les cas.

Les entretiens réalisés ne sont pas strictement représentatifs de la composition du W3C PING. Certaines discussions avec des participants salariés d'entreprises membres n'ont pas obtenu l'autorisation de leur hiérarchie pour participer à la campagne d'entretiens, comme l'illustre cet e-mail :

« Salut Julien,

J'ai vérifié avec notre équipe d'affaires publiques et, malheureusement, nous ne pouvons pas participer à ta recherche.

Je te souhaite bonne chance pour ton projet,

Cordialement,

[Signature][59] » (e-mail reçu le 25 mai 2017)

D'autres participants ont accepté de participer, à condition de rester anonymes, d'où l'omission de certains noms dans le tableau ci-dessous. Un des participants étant le seul du groupe à vivre dans un pays donné, nous avons remplacé l'indication de son pays de résidence avec la zone géographique dans laquelle il vit pour respecter sa demande d'anonymat :

	Nom	**Prénom**	**Anonymat**	**Date de l'entretien**	**Pays de résidence**	**Employeur**
W3C1			OUI	13/02/17	Europe de l'Ouest	
W3C2	Rice	Simon	NON	31/03/17	Royaume-Uni	ICO
W3C3	Hall	Joseph	NON	14/04/17	États-Unis	CDT

59 Traduction de l'auteur. Texte original : « « Hi Julien,
I checked with our policy team and, unfortunately, we are not able to participate in your research.
I wish you luck with your project.
Regards,
[Signature] »

W3C4	Toubiana	Vincent	NON	09/05/17	France	CNIL
W3C5			OUI	03/11/17	États-Unis	
W3C6	Stamm	Sid	NON	05/12/17	États-Unis	Mozilla Foundation
W3C7	Olejnik	Lukasz	NON	05/12/17	Royaume-Uni	INRIA
W3C8	Wenning	Rigo	OUI	14/12/17	France	ERCIM (W3C)
W3C9	Dawson	Frank	NON	20/12/17	États-Unis	Nokia
W3C10			OUI	20/12/17	États-Unis	

Tableau 6 : *Tableau des entretiens réalisés dans le cadre du terrain sur le W3C* Privacy Interest Group

Les femmes sont sous-représentées dans notre échantillon, puisque sur les 10 entretiens, seul un a été réalisé avec une femme. Or, sur 49 participants dont le nom était listé officiellement sur le site du W3C PING en juillet 2018, au moins 10 étaient des femmes, sachant que 4 personnes avaient des noms dont il n'a pas été possible de déduire s'il s'agissait d'un homme ou d'une femme. Les hommes sont donc surreprésentés dans notre échantillon. Cet effet involontaire est dû au fait que les hommes ont répondu plus favorablement que les femmes contactées à nos demandes d'entretien. Une des femmes contactées a répondu qu'un de ses collègues serait plus à même de répondre à nos questions. Quant à l'origine géographique, seuls des membres européens ou nord-américains ont répondu à nos sollicitations.

Malgré tout ces biais, nous avons eu dans notre échantillon des gens représentants chacun des types d'employeurs : des associations militantes (*Center for Democracy and Technology*, Mozilla), des universitaires (INRIA), des employés d'entreprises (Nokia), des employés du W3C et des personnes qui, bien que n'étant pas officiellement des représentants de leurs employeurs, travaillaient pour des autorités de protection des données. L'exploitation des données collectées à partir des listes de discussion publiques *public-privacy* et *public-tracking* a servi à compenser en partie cette représentativité approximative.

Nous avons également, surtout au cours des premiers entretiens, ajouté des questions sur le fonctionnement concret du W3C PING, sa relation avec d'autres arènes, et sa relation au droit.

1.2.5.3. Listes de discussion (mailing-lists)

Toutes les *mailing-lists* publiques de groupes actifs du W3C répertoriés en octobre 2017 sur leur page web de présentation ont été téléchargées. Certaines *mailing-lists* historiques, comme celle du groupe de travail *Platform for Privacy Preferences* (P3P), ont également été téléchargées en raison de leur importance ou de leur rapport direct avec le sujet de la protection de la vie privée. Les *mailing-lists* de *Community Groups*, qui sont des groupes de travail informels hébergés par le W3C mais ne travaillant pas sur des spécifications officielles, ont été ignorées.

La raison pour laquelle l'ensemble des e-mails n'a pas été téléchargé de façon exhaustive est le temps que cela prend. Ainsi, au 10 mai 2018, notre corpus comprenait un total de 346 487 e-mails téléchargés. Or, pour télécharger ces e-mails, il a fallu créer un script Python qui aille sur la page web des archives publiques de chaque liste de discussion, pour télécharger un à un chacun des e-mails, extraire le contenu et les métadonnées (expéditeur et date) de chaque e-mail, pour ensuite pouvoir en extraire des statistiques exportées dans des feuilles de calcul au format CSV. Pour éviter que les serveurs du W3C n'interprètent une série de 346 487 requêtes comme étant une attaque par déni de service, c'est-à-dire par mitraillage de requêtes visant à submerger la capacité d'un serveur à répondre, il a fallu introduire une instruction ordonnant à l'ordinateur de faire une pause aléatoire de 3 à 8 secondes entre deux requêtes, soit 5,5 secondes en moyenne. Si l'exécution de notre script a respecté la loi mathématique des grands nombres, ces 346 487 e-mails ont donc mis environ 1905678,5 secondes à être téléchargés, soit un peu plus de 22 jours non-stop. Ce temps ne prend pas en compte le temps de traitement des données qui, bien que nettement plus rapide, est lui aussi significatif.

Ceci explique qu'un choix ait dû être fait et que l'exhaustivité n'était pas matériellement à notre portée.

Des études similaires à ce que nous avons fait ont déjà été menées sur les *mailing-lists* de l'IETF pour générer des statistiques sur l'évolution de l'emploi des termes « *security* » et « *privacy* » (Doty, 2015). Il est ainsi possible de générer rapidement des statistiques sur un corpus large et de déterminer des pics d'activité, ou des corrélations entre l'emploi de certains termes. La représentation sur un même graphe de l'évolution dans le temps de l'emploi de certains termes, dans plusieurs listes de discussion représentées chacune par une ligne, permet de faire des hypothèses sur la circulation de certaines thématiques d'une arène à l'autre. Télécharger les e-mails publiquement disponibles sous un format qu'il est possible de traiter par des scripts, en Python ou dans un autre langage de programmation (comme R ou Ruby), permet donc de gagner du temps dans la constitution de corpus plus restreints sur lesquels il est ensuite possible de faire une étude qualitative.

Il est important de garder à l'esprit les limites de cette méthode.

Tout d'abord, les listes de discussion publiques ne couvrent pas tous les échanges. Il peut y avoir des échanges interpersonnels qui n'y sont pas adressés, entre participants aux groupes de travail du W3C.

Ensuite, il existe des *mailing-lists* non publiques. Leur nombre semble avoir eu tendance à décroître au fil des années. Cela veut dire que les échanges des premières années du W3C, et de projets comme P3P, sont sous-représentés dans les statistiques que nous pouvons générer à partir des e-mails publiquement diffusés. Comme le rappellent en effet Nick Doty et Deirdre Mulligan :

> « Une augmentation du niveau de transparence des discussions, des délibérations et des discussions entre P3P et DNT est évidente. Le processus P3P impliquait de nombreuses discussions réservées aux membres alors que le processus DNT est effectué intégralement avec des listes de diffusion publiques et des réunions ouvertes[60]. » (Doty et Mulligan, 2013, p. 159)

La difficulté de l'analyse des échanges lors des premiers temps du W3C est accrue par le fait qu'au début des années 1990, certaines des discussions avaient encore lieu sur des *newsgroups* USENET comme comp.infosystems.www.authority.stylesheets, où se tenait la discussion sur la standardisation des feuilles de style (qui a donné le CSS).

Les listes de discussion publiques ne couvrent pas non plus les échanges sur les canaux de messagerie instantanée reposant sur le protocole IRC, qui ne sont pas structurées de la même façon que les listes de discussion et nécessiteraient un traitement très différent, ni les discussions orales en téléconférence ou lors des (rares) rencontres *de visu*.

Ensuite, il est difficile d'établir des statistiques précises sur le nombre réel de participants. Une adresse e-mail ne correspond pas toujours à une personne. Elle peut correspondre parfois à un robot, et dans d'autres cas, une même personne peut utiliser plusieurs adresses de courrier électronique. Or, c'est par son adresse e-mail que le script est capable d'identifier une personne. En outre, une liste de discussion ne correspond pas forcément à un seul groupe, et un groupe peut avoir plusieurs listes de discussion publiques. Des listes de discussion sont crées avant la création officielle du groupe, et souvent, elles demeurent actives après sa clôture officielle. L'adéquation entre personne et adresse e-mail d'une part, groupe de travail et liste de discussion d'autre part, est donc tout à fait approximative, même s'il y a un lien entre les deux.

60 Traduit de l'anglais. Texte original : « An increase in the level of transparency about discussions, deliberations and decisions is evident from P3P to DNT. The P3P process involved many member-only discussions while DNT is being conducted completely on public mailing-lists and open meetings. »

Pour toutes ces raisons, la méthode de fouille automatisée de données textuelles ne peut être qu'une méthode exploratoire. Il s'agit cependant d'une méthode exploratoire puissante qui fait économiser beaucoup de temps dans la sélection d'un matériau plus restreint, pouvant être lu, interprété et analysé par un humain.

Voici la liste des *mailing-lists* qui ont été téléchargées pour une analyse par traitement automatique, sur une période d'août 1995 à octobre 2017 (voire jusqu'à mi-2018 pour certaines de ces listes) :

Nom de la mailing-list	**Groupe de travail ou d'intérêt ou autre groupe correspondant**	**Nom de la mailing-list**	**Groupe de travail ou d'intérêt ou autre groupe correspondant**
www-dom	À l'origine : Document Object Model Activity Statement. Désormais : W3C Web Applications Working Group	public-poe-wg	Permissions and Obligations Expression Working Group
public-svg-wg	SVG Working Group	public-device-apis	Device APIs and Policy Working Group
public-payments-wg	Web Payments Working Group	public-pling	Policy Language Interest Group
public-data-shapes-wg	RDF Data Shapes Working Group	public-audio	Audio Working Group
public-vc-wg	Verifiable Claims Working Group	public-webapps	Web Platform Working Group
public-browser-tools-testing	Browser Testing and Tools Working Group	public-tt	Timed Text Working Group
public-sdw-wg	Spatial Data on the Web Working Group	public-p3p-ws	Platform for Privacy Preferences Working Group
xsl-editors	XSLT Working Group	www-p3p-dev	Platform for Privacy Preferences Working Group
www-p3p-policy	Platform for Privacy Preferences Working Group	public-html	HTML Working Group, puis Web Platform WG
www-ql	XML Query Working Group	public-exi	Efficient Extensible Interchange Working Group

public-aria	Accessible Rich Internet Applications Working Group	public-dxwg-wg	Dataset Exchange Working Group
public-webassembly	WebAssembly Working Group	public-xsl-wg	XSLT Working Group
public-webfonts-wg	Web Fonts Working Group	w3c-wai-eo	Education & Outreach Working Group
www-style	Tous les groupes de travail travaillant sur des spécifications de feuilles de style (CSS, XSL)	public-apa	Accessible Platform Architectures Working Group
public-socialweb	Social Web Working Group	public-p3p	Platform for Privacy Preferences Working Group
public-geolocation	Geolocation Working Group	www-p3p-interop	Platform for Privacy Preferences Working Group
www-tag	W3C Technical Architecture Group	public-webrtc	Real-time Communication Between Browsers Working Group
www-privacy-evaluator	*	public-pointer-events	Pointer Events Working Group
public-html-media	HTML Media Extensions Working Group	w3c-wai-gl	Web Content Accessibility Guidelines Working Group
www-xsl-fo	XSL FO Subgroup	public-tracking	Tracking Protection Working Group
public-webappsec	Web Application Security Working Group	www-font	Web Fonts Working Group
public-privacy	Privacy Interest Group	www-international	Internationalization Working Group
public-publ-wg	Publishing Working Group	public-web-perf	Web Performance Working Group
public-webauthn	Web Authentication Working Group	www-svg	Scalable Vector Graphics Working Group
public-script-coord	liste de discussion de coordination	public-wot-wg	Web of Things Interest Group et Web of

			Things Working Group
public-p3p-spec	Platform for Privacy Preferences Working Group	public-automotive	Automotive Working Group
www-p3p-public-comments	Platform for Privacy Preferences Working Group	public-secondscreen	Second Screen Working Group

* : indique que le groupe de travail correspondant n’a pas pu être déterminé

Tableau 7 : *Liste des listes de discussion publiques du W3C téléchargées dans le cadre de l’étude de terrain sur le W3C PING*

Concrètement, des scripts Python ont été rédigés pour procéder à la fouille exploratoire de ces données, une fois celles-ci téléchargées par un premier script.

Deux types d'opérations ont été menées sur ces données.

Dans un premier temps, il s'est agi de cartographier, avec l'aide du logiciel Gephi, quelles adresses e-mail participent à quelles listes de discussion. L'idée était de voir quels étaient les liens personnels entres groupes du W3C.

Dans un deuxième temps, nous avons généré des tableaux qui montrent l'évolution mois par mois et par *mailing-list* du nombre de fois où certains termes, comme « *privacy* » ou « *gdpr* », ont été utilisés, avec la fréquence d'utilisation de ces mots. L'objectif était de voir quand ces mots, liés à la thématique de la vie privée et de la protection des données, sont apparus, et dans quelles listes de discussion, puis de sélectionner des corpus restreints d'e-mails à analyser de façon qualitative autour de pics d'occurrences. Ces tableaux et graphiques sont présentés dans le chapitre 5.

1.2.5.4. Observation participante lors de la réunion F2F annuel du Privacy Interest Group au Technical Plenary and Advisory Committee de Lyon en 2018

La réunion annuelle du W3C TPAC (*Technical Plenary and Advisory Committee*) de 2018 a eu lieu à Lyon, du lundi 22 au vendredi 26 octobre 2018. Il a donc été possible de profiter de la proximité géographique pour me rendre à la réunion « *Face to Face* » (F2F), c’est-à-dire en présentiel, du PING du vendredi 26 octobre 2018, sur invitation de Tara Whalen, *co-chair* du

PING. Le TPWG n'existait de fait plus depuis le début de ce mois[61], ce qui explique que je n'aie pas pu assister à une réunion F2F de ce groupe.

Cette réunion avait lieu au Centre des Congrès de Lyon, non loin du campus de la Doua.

À l'exception de la plénière du mercredi, à laquelle je n'ai pas pu assister en raison de contraintes d'emploi du temps, toutes les réunions se sont déroulées par *working groups* (ou *interest group* dans le cas du PING[62]) dans des salles de réunion. Chaque salle de réunion était équipé d'un vidéoprojecteur, et de tables en U y faisant face. Des chaises avaient été disposées le long des murs de la salle pour accueillir des participants supplémentaires en cas de besoin.

Les participants pouvaient entrer et sortir librement des salles à tout moment. Dans la salle affectée au PING, il y a eu entre six et quinze personnes selon le moment de la journée. Parmi les personnes présentes qui contribuent régulièrement au PING depuis plusieurs années, j'ai pu noter la présence de Tara Whalen, Samuel Weiler, Michael O'Neill, Michael West, David Singer, Wendy Seltzer et Jason Novak. Nick Doty et Christine Runnegar ont rejoint la discussion en fin de journée, à distance via le logiciel WebEX couplé à des micros et des hauts-parleurs présents dans la salle. Parmi les fabricants de navigateurs, étaient présents des ingénieurs d'Apple, de Google, de Brave et de Samsung, mais personne de Mozilla, Microsoft ou Opera ne nous a rejoint.

Cette observation de terrain est venue assez tardivement. Dès lors, elle n'a servi qu'à compléter, préciser, et mieux comprendre l'analyse qui avait déjà été faite des corpus précédemment décrits d'entretiens, d'e-mails échangés sur des listes de discussion publiques et de documents produits par des groupes de travail ou d'intérêt du W3C pertinents par rapport à l'objet d'étude.

1.2.5.5. Autres documents exploités dans l'analyse

En plus du corpus d'entretiens et d'e-mails, et de nos observations au TPAC, nous avons intégré un grand nombre de documents produits dans des arènes de standardisation technique d'Internet. Ceux-ci sont listés de façon exhaustive dans la bibliographie.

Enfin, pour l'étude de la controverse autour de la définition du terme « *tracking* », qui a eu lieu au sein du TPWG mais que nous avons intégrée en raison des références qui y ont été faites dans les entretiens, nous avons exploité les 471 messages échangés entre septembre 2011 et avril

61 La charte de ce groupe n'a été étendue que jusqu'au 30 septembre 2018. La fermeture officielle du groupe est intervenue le 17 janvier 2019. Voir : https://www.w3.org/2016/11/tracking-protection-wg.html (page consultée le 8 septembre 2019). Le TPWG ne s'est pas réuni lors du TPAC de 2018.

62 Nous reviendrons sur cette distinction en section 5.3.

2015 sur le fil de discussion « *ISSUE-5 : What is the definition of tracking ?* » de l'outil de *bug tracking* du TPWG[63]. Ces messages sont en fait des courriels de la liste de discussion *public-tracking*, qui ont été sélectionnés pour être intégrés à ce fil de discussion spécifique, comme nous pouvons le voir dans la capture d'écran ci-dessous :

Figure 5 : *Capture d'écran de la page* « ISSUE-5: What is the definition of tracking? » *du* Tracking Protection Working Group *du* W3C. *Page consultée à l'adresse https://www.w3.org/2011/tracking-protection/track/issues/5 le 20 avril 2020.*

1.3. Explorer les différentes conceptions de la notion de « vie privée »

Nous avons vu en introduction qu'il n'est pas simple de définir la « vie privée ». Les notions de droit *à la* vie privée et de droit *à la* protection des données soulèvent elles aussi, telles qu'elles sont employées sur le terrain, de nombreuses difficultés conceptuelles.

Cette thèse propose de contribuer à clarifier la relation entre ces différents concepts, et à étudier si l'arrivée de l'informatique, les transformations du milieu technique qu'elle induit et la perception qu'en ont les acteurs qui rédigent les normes de protection des données ont fait évoluer la « vie privée » en tant qu'objet du droit *à la* vie privée.

63 Voir la page : https://www.w3.org/2011/tracking-protection/track/issues/5 (page consultée le 26 août 2019)

L’analyse des discours des documents collectés et des entretiens a notamment servi à relier la controverse définitionnelle sur la notion de « donnée à caractère personnel », qui détermine ce à quoi s’applique ce droit *à la* protection des données, à des conceptions théoriques de la « vie privée » auxquels ils font référence, explicitement ou implicitement. Pour effectuer ce travail, il a fallu dans un premier temps repérer dans l’espace public, notamment dans des livres, des articles de presse, des publications académiques ou encore des discours publics d’acteurs institutionnels et de militants, des discours sur la « vie privée » pour établir une typologie de ces différentes conceptions.

Le résultat de ce travail va être présenté dans le prochain chapitre afin de pouvoir faire référence dans la suite de ce mémoire de thèse aux différentes conceptions repérées dans les discours de nos corpus.

Chapitre 2 : Penser le droit *à la* vie privée

2.1. Introduction : défaire l'illusion du consensus

Les discours des acteurs ayant participé à la rédaction ou à la controverse autour de la rédaction de textes normatifs de protection des données à caractère personnel, qu'il s'agisse de textes de droit dur ou de droit souple, font référence à des corpus d'idées et des façons de concevoir le droit *à la* vie privée ou le droit *à la* protection des données à caractère personnel. Ces conceptions portent à la fois sur le contenu de ce qui doit être protégé, et sur le « pourquoi », sur la valeur philosophique et morale de ce droit. Leurs expressions peuvent se retrouver dans l'espace public : dans des essais, des ouvrages scientifiques, des articles de presse ou de revues scientifiques, ou même dans des romans ou d'autres œuvres littéraires.

Ces questions ne sont toutefois que très rarement abordées de façon explicite dans les documents institutionnels ou les discours d'acteurs ayant pris part à l'élaboration des droits *de la* vie privée et *de la* protection des données personnelles. L'idée que le « droit à la vie privée », ou la « vie privée » en général soient désirables, normativement de « bonnes » choses, y est souvent présentée comme faisant consensus. Dans d'autres cas, comme au W3C, nous observons une volonté délibérée d'éviter de délibérer et de s'exprimer sur ces questions, pour ne pas risquer de perdre du temps à chercher un consensus perçu comme impossible[1]. La justification axiologique de l'engagement des acteurs en faveur de leur conception du droit *à la* vie privée – ou contre la conception des acteurs de la coalition rivale – est souvent renvoyée à un plan implicite.

Afin de répondre à la question de recherche sur l'objet de la protection des textes normatifs de protection des données à caractère personnel, l'une des étapes essentielles de l'analyse consiste à relier les discours d'acteurs aux conceptions théoriques servant de soubassement à leur action, auxquelles ils font référence, souvent implicitement, parfois explicitement, notamment en réponse à des questions en entretien semi-directif.

Les documents officiels ou de doctrine juridique discutant ou établissant le droit *à la* vie privée ne perdent en général pas beaucoup de temps en explications et justifications de ce droit. Par exemple, le deuxième considérant de la directive 95/46/CE[2] est la seule disposition dans ce texte qui mentionne des arguments généraux et philosophiques en faveur de la protection des données à caractère personnel, et même là, la protection de la vie privée y est un allant-de-soi auquel il est brièvement fait allusion :

1 Cf. section 5.5.3.

2 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

> « (2) considérant que les systèmes de traitement de données sont au service de l'homme; qu'ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus ; » (directive 95/46/CE, considérant 2)

Cela est vrai également dans les documents produits dans des arènes de production de standards techniques d'Internet s'intéressant à la protection de la vie privée. Ainsi, la description sur la page d'accueil du *Privacy Interest Group* du W3C[3] indique :

> « L'évolution des technologies du Web a augmenté la collecte, le traitement et la publication de données à caractère personnel. Des inquiétudes liées à la vie privée sont exprimées plus souvent, au fur et à mesure que les applications construites sur la plateforme du Web gagnent l'accès à plus de données sensibles – incluant la localisation, la santé et les informations de réseau social – et que l'activité des utilisateurs sur le Web est pistée de façon ubiquitaire. L'Activité Vie Privée du W3C coordonne les travaux de standardisation pour améliorer le support de la vie privée des utilisateurs dans le Web et développer une expertise générale dans le domaine de la Vie privée dès la conception pour les standards du Web[4] » [5]

Les citations ci-dessus illustrent une façon commune de poser le problème de la vie privée conjuguée à la problématique de la société informationnelle : le développement de nouvelles technologies y est lié à des risques accrus pour la vie privée, et la nécessité de protéger la vie privée comme un bien y est implicitement admise sans qu'il soit nécessaire de l'expliciter dans un texte. D'ailleurs, aucun des *position papers* de notre corpus, rédigés par des groupes d'intérêt pendant la phase d'adoption du RGPD, n'attaque frontalement ou fondamentalement le bien-fondé philosophique et moral du droit *à la* vie privée.

La société Google, sanctionnée et condamnée à de nombreuses reprises pour avoir enfreint le droit *de la* protection des données à caractère personnel[6], diffuse aujourd'hui un discours officiel en faveur de la vie privée :

---

3 Voir en-ligne (page consultée le 21 mars 2016) : https://www.w3.org/Privacy/

4 Traduction de l'auteur. Texte original : « The evolution of Web technologies has increased collection, processing and publication of personal data. Privacy concerns are raised more often as applications built on the Web platform have access to more sensitive data — including location, health and social network information — and users' activity on the Web is ubiquitously tracked. The W3C Privacy Activity coordinates standardization work to improve support for user privacy on the Web and develops general expertise in privacy-by-design for Web standards. »

5 Extrait de la page web « W3C Privacy Interest Group » du site web du W3C. Page consultée le 21 mars 2016 à l'URL : https://www.w3.org/Privacy/

6 Voir notamment : CNIL (France) Délibération n°2013-420 du 3 janvier 2014 prononçant une sanction pécuniaire à l'encontre de la société Google Inc., Garante Privacy (Italie) Provvedimento del 10 gennaio 2019 [9090292], Garante Privacy (Italie) Ordinanza di ingiunzione nei confronti di Google Inc. - 18 dicembre 2013, AEPD (Espagne) Resolución R/02892/2013 del 19 de Diciembre de 2013

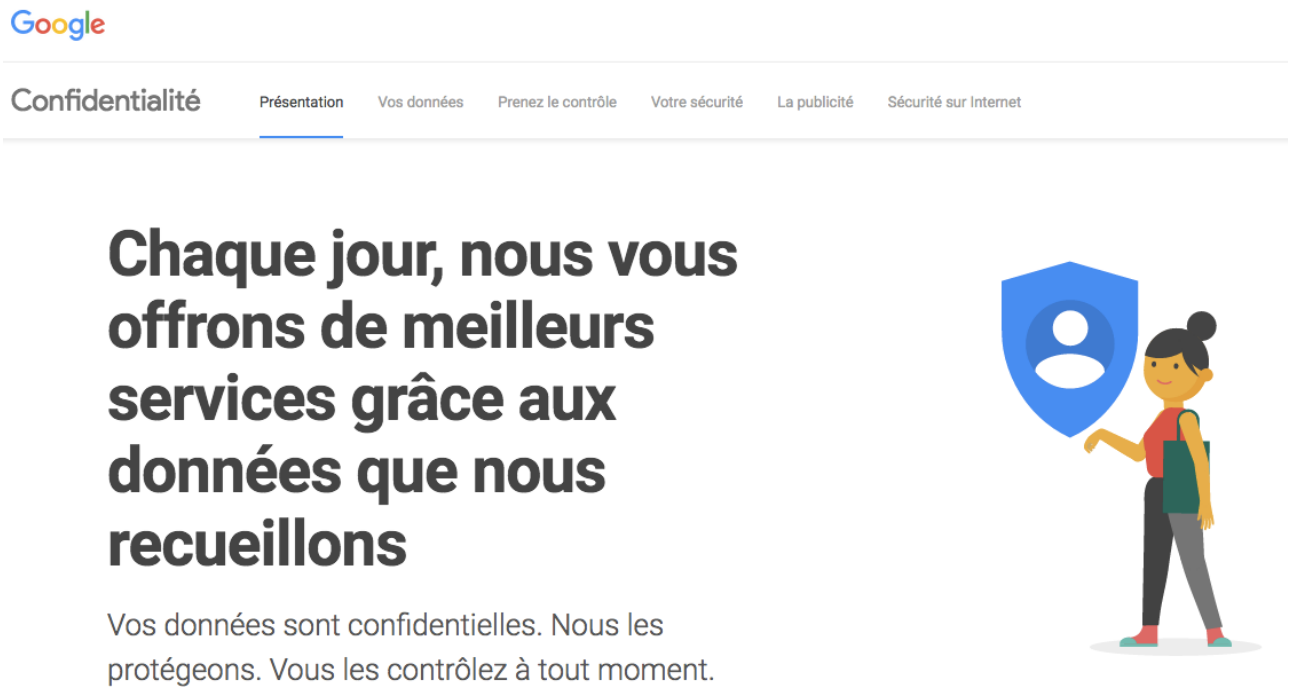


Figure 6 : *Capture d'écran du site Internet https://privacy.google.com en date du 18 juillet 2017. Le texte en police plus petite, en bas à gauche, suggère l'importance que l'entreprise Google dit accorder à la confidentialité des données de l'internaute qui consulte cette page.*

Même un site comme ResearchGate, qui impose l'installation de cookies traceurs sur le terminal de l'internaute, en flagrante infraction avec l'article 5 paragraphe 3 de la directive 2002/58/CE amendée en 2009, lu en conjonction avec le RGPD, prétend « accorder de la valeur à [notre] vie privée[7] » :

7 Pour une étude des interfaces web de recueil de consentement, voir : Utz et al., 2019

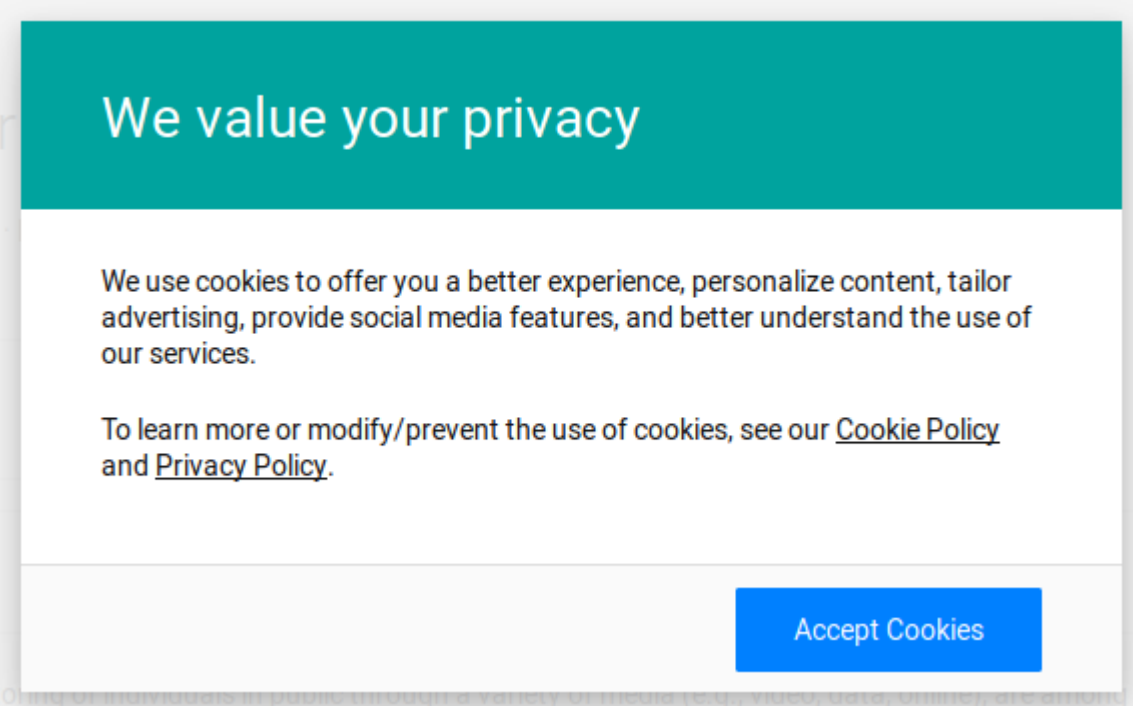


Figure 7 : *Extrait de capture d'écran de la page https://www.researchgate.net/publication/228198982_Privacy_As_Contextual_Integrity, du 19 juillet 2019*

L'illusion de consensus autour de la définition et du contenu du droit *à la* vie privée et *à la* protection des données à caractère personnel est également entretenue par une partie de la littérature académique. Différentes études sur le paradoxe de la vie privée ont elles aussi tendance à supposer que le sens du mot « vie privée » (ou « *privacy* » en anglais) est transparent, et que les enquêtés en partagent avec les enquêteurs une même compréhension. Ainsi, Alessandro Acquisti et Ralph Gross (2006), lorsqu'ils comparent les comportements d'utilisateurs de Facebook avec leurs niveaux déclarés de préoccupation pour la protection de leur « vie privée », ne leur posent aucune question sur le sens que ces derniers donnent à ces mots. Dans une autre étude, sur les liens entre réglementation sur la protection de la « vie privée », perception des risques, confiance et comportements d'utilisateurs, Caroline Miltgen et Jeff Smith (2015) entament leur propos en rappelant l'importance prise à partir des années 1970 par les questions de protection de la vie privée, sans pour autant chercher à définir cette notion, à en délimiter le contenu, ou même à expliquer ou justifier cette importance. Dans une étude publiée en 2018 par l'Institut d'économie de Zagreb au terme d'un projet de recherche sur la sensibilité à la « vie privée[8] », les auteurs ont bien pris le temps de préciser quelle était leur définition de la « vie privée », y compris en faisant référence à des travaux de théoriciens de la vie privée (Anić et al., 2018, p. 14-28). Ils précisent que toute mesure quantitative de sensibilité à la vie privée est difficile car « hautement

8 Il s'agit du projet PRICON, pour « *Extended Model of Online Privacy Concern* », financé par la Fondation croate pour la science. Voir : (Anić et al., 2018).

subjective »[9] (Anić et al., 2018, p. 34). Toutefois, malgré la sophistication et l'intérêt considérables du modèle proposé, cette étude n'a pas non plus cherché à faire émerger du terrain une ou des définitions de la « vie privée » et du « droit *à la* vie privée ». Enfin, bien que la critique communautariste de la vie privée[10] y soit évoquée, le chapitre de cette étude consacrée à la présentation de la définition adoptée par les auteurs de la « vie privée » est construit de telle sorte à aboutir à une forme de consensus sur ce « qu'est » la vie privée, pour en tirer une définition opérationnelle. Cela a pour effet de gommer les clivages entre approches antagonistes, et de renforcer l'impression qu'il existerait un consensus général sur l'idée même du bien-fondé du droit *à la* vie privée.

Plusieurs voix de dissensus se font pourtant parfois entendre dans le débat public. En 2010, Mark Zuckerberg, fondateur de Facebook, déclarait ainsi que « la vie privée n'est plus une norme sociale[11] » (Barnett, 2010). Vint Cerf, un des cadres dirigeants de Google, a affirmé en 2013 devant la Federal Trade Commission américaine que « la vie privée pourrait bien en fait être une anomalie[12] » (Cerf, 2013, p. 147).

Par ailleurs, nous trouvons y compris dans la littérature académique des voix prenant partie contre le droit *à la* vie privée. C'est le cas à la fois de Richard Posner (1977, 1981), George Stigler (1980) ou encore – pour des raisons différentes – Catherine MacKinnon (1989). D'autres critiquèrent l'existence ontologique d'une catégorie de droit qui serait un droit *à la* vie privée. Selon cette critique – connue sous le nom de critique « réductionniste » (DeCew, 2018) – le droit *à la* « vie privée » désignerait un ensemble incohérent de droits déjà protégés par ailleurs, par exemple par le droit à la propriété, ou à la sécurité (Thomson, 1975).

La valeur, la désirabilité même du droit *à la* vie privée ne fait donc pas tout à fait consensus, et même entre partisans d'un tel droit, il existe des débats sur sa justification philosophique et morale, sur ses limites, ou encore sur ses modalités.

Le but du présent chapitre n'est pas de faire un état de l'art sur les conceptions existantes du droit *à la* vie privée en poursuivant un idéal inatteignable d'exhaustivité, mais de présenter les grandes lignes des débats théoriques que nous avons repérés dans l'espace public pour essayer de distinguer plusieurs courants de pensée. Il n'est pas non plus de prendre position en faveur de l'une ou de l'autre, même si j'ai effectivement un avis sur le sujet. Cette présentation est fondée sur un travail de recherche et de lecture de nombreux textes théoriques sur la vie privée, qui a précédé la conduite des terrains présentés dans les trois prochains chapitres. Régulièrement, nous

9 Traduction de l'auteur. Texte original : « highly subjective ».
10 Cf. section 2.3.4.
11 Traduction de l'auteur. Texte original : « privacy is no longer a social norm ».
12 Traduction de l'auteur. Texte original : « privacy may actually be an anomaly ».

ferons des renvois vers ce chapitre, lorsque nous serons en présence d'un discours d'acteur qui nous paraît faire référence à l'une des conceptions du droit *à la* vie privée présentée ici, ou tout du moins la refléter, s'en approcher.

Notons que pour ne pas s'écarter du cadre de l'objet de recherche de la thèse, seuls seront présentés ici dans les grandes lignes des théories sur le droit *à la* vie privée ou sur le droit *à la* protection des données à caractère personnel. Tous les discours sur les données *en général* ne seront pas présentés. Ceci nous a par exemple amené à exclure de notre champ d'étude la présentation et l'analyse des discours sur le *Big Data*, dont la généalogie remonte aux travaux et projets anciens sur la statistique et la gestion des probabilités (Bernstein, 1998 ; Desrosières, 2014 ; Rouvroy et Berns, 2013), couplée à l'idée que les traces numériques sont des indices fiables du réel tendant à l'exhaustivité et capables de révolutionner par l'obsolescence de la recherche d'hypothèses explicatives les méthodes scientifiques et l'innovation industrielle (Bonenfant et al., 2015 ; Boullier, 2015 ; Bourdeloie, 2014 ; Jeanneret, 2011 ; Rouvroy et Berns, 2013 ; Schmitt, 2015) et à des imaginaires techno-libertaires ou néolibéraux (Ibekwe-Sanjuan et Paquienséguy, 2015).

À l'inverse, des discours partant d'une réflexion sur la technique ont eux été intégrés s'ils contenaient des éléments sur le droit *à la* vie privée ou *à la* protection des données à caractère personnel, mais ne seront pas présentés dans leur ensemble. C'est notamment le cas du *Quantified Self*, qui repose par ailleurs sur le paradigme dataïste incarné par les discours sur le *Big Data*, sans pour autant en représenter l'intégralité.

Les conceptions, ou courants de pensée, sur la vie privée qui sont présentés dans ce chapitre sont par ailleurs construits et présentés comme des ensembles cohérents, et clairement délimités entre eux. Si cette présentation s'est fondée sur des clivages et des filiations intellectuelles dont nous avons vérifié l'existence dans la littérature, elle est dans le même temps le fruit d'un processus de simplification. Par exemple, bien que le paradigme libéral de la vie privée soit dans l'ensemble individualiste, et qu'il motive un projet de reconnaissance d'un droit *à la* vie privée dans le chef des *individus* et non des *groupes* pour protéger des intérêts conçus comme *individuels* avant tout, Alan Westin, l'un des principaux théoriciens cités par la première génération de défenseurs de la vie privée dans les années 1970, évoquait encore de temps en temps dans ses écrits la possibilité et l'utilité pour des groupes de bénéficier d'une vie privée. Les catégories présentées dans ce chapitre sont donc des catégories idéal-typiques, en ce qu'elles sont une mise en cohérence artificielle et simplificatrice des phénomènes étudiés qui sont malgré tout un préalable indispensable à la compréhension et donc à l'étude de ces mêmes phénomènes.

Enfin, le fait qu'un corpus de discours soit présenté ici sous la forme d'une conception théorique de la vie privée ne signifie pas nécessairement qu'elle se soit retrouvée reflétée sur les terrains étudiés. Le travail de repérage a commencé avant les études de terrain, même si ce chapitre a été rédigé après la rédaction initiale des quatre suivants. De ce fait, certains des discours et conceptions présentés, détectés dans la littérature ou dans la presse sans critère de

ciblage particulier, ont été intégrés bien qu'ils n'aient que marginalement ou pas circulé dans les terrains de notre recherche.

2.2. Le paradigme libéral de la vie privée et son évolution foucaldienne

La notion de *paradigme de la vie privée* vient de Colin Bennett et Charles Raab (2003), dans leur ouvrage *The governance of privacy*. Pour eux, il s'agit du paradigme partagé par la « *privacy community* » des défenseurs de la vie privée, c'est-à-dire d'une coalition d'acteurs défendant la mise en œuvre de politiques publiques de protection *de la* vie privée. Comme ils l'affirment dans leur livre, et comme nous avons pu le confirmer[13], cette « communauté » est à l'origine de l'invention du droit *à la* protection des données à caractère personnel dans les années 1970.

Ce paradigme est fondé sur une vision du droit *à la* vie privée comme un droit distinct d'autres catégories de droits fondamentaux, comme le droit *à la* liberté d'expression. C'est également un paradigme que Colin Bennett et Charles Raab (2003) qualifient (tout en le critiquant) d'individualiste, en ce qu'il reconnaît un droit *à la* vie privée à des individus et non à un collectif. Philosophiquement, il s'agit d'une conception d'inspiration libérale. Notons d'ailleurs d'emblée que libéralisme et néolibéralisme sont à distinguer en raison de leurs différences à la fois dans leurs fondements philosophiques et dans les projets politiques qu'ils sous-tendent (Brouwer, 2008 ; Vergara, 2002). Nous y reviendrons dans le paragraphe sur la critique *néo*libérale de la « vie privée[14] ».

Le terme de « paradigme » est ici emprunté à l'épistémologue Thomas Kuhn, qui définissait un paradigme comme un ensemble de « découvertes scientifiques universellement reconnues qui, pour un temps, fournissent à une communauté de chercheurs un ensemble de problèmes types et de solutions » (Kuhn, 1972 [1962], p. 10). Sont associées à chaque paradigme un ensemble de connaissances et de pratiques partagées par une communauté scientifique, soudée par un accord sur des normes de scientificité. Colin Bennett et Charles Raab reprennent ce terme et expliquent de la façon suivante leur usage du terme :

13 Cf. chapitre 3.
14 Cf. section 2.3.1.

> « Nous employons le mot « paradigme » pour dénoter un ensemble de suppositions sur un phénomène ou un champ d'étude qui sont généralement admises sans question. Ces suppositions fixent collectivement l'agenda pour la recherche et pour les prescriptions de politiques publiques[15]. » (Bennett et Raab, 2003, p. 13)

Le terme de « paradigme » ainsi défini s'applique bel et bien au paradigme de la vie privée, tant selon Colin Bennett et Charles Raab que selon nos propres observations de terrain, décrites dans les deux prochains chapitres, dans la mesure où elle désigne une référence commune partagée pour la coalition des défenseurs de la vie privée. Ainsi :

> « Un groupe très soudé d'experts venus de différents pays se sont unis, ont partagé des idées, et généré un consensus général sur la meilleure façon de résoudre le problème de la protection de la vie privée des informations personnelles[16]. » (Bennett et Raab, 2003, p. 16)

Ce paradigme tiré du consensus ainsi généré est libéral :

> « Le paradigme de la vie privée repose sur une conception de la société comprenant des individus relativement autonomes. Il repose sur une conception atomistique de la société ; la communauté n'est pas plus que la somme des individus qui la composent. De plus, il repose sur des notions de différences entre les revendications de vie privée et les intérêts de différents individus. L'individu, dans sa liberté, son autonomie, sa rationalité et sa vie privée, est présumé connaître ses intérêts, et devrait avoir droit à une sphère privée sauvegardée de l'intrusion d'autrui[17]. » (Bennett et Raab, 2003, p. 14)

Le paradigme de la vie privée repose sur l'idée qu'« il y a pléthore de preuves anthropologiques que les êtres humains ont toujours eu besoin d'un certain degré de vie privée[18] »

15 Traduction de l'auteur. Texte original : « We use the word "paradigm" to denote a set of assumptions about a phenomenon or area of study which generally go unquestioned. These assumptions collectively set the agenda for research and for policy prescription ».

16 Traduction de l'auteur. Texte original : « a closely-knit group of experts in different countries coalesced, shared ideas, and generated a general consensus about the best way to solve the problem of protecting the privacy of personal information ».

17 Traduction de l'auteur. Texte original : « The Privacy paradigm rests on a conception of society as comprising relatively autonomous individuals. It rests on an atomistic conception of society ; the community is no more than the sum of the individuals that make it up. Further, it rests on notions of differences between privacy claims and interests of different individuals. The individual, with her liberty, autonomy, rationality and privacy, is assumed to know her interests, and should be allowed a private sphere untouched by others. ».

18 Traduction de l'auteur. Texte original : « there is plenty of anthropological evidence that human beings have always needed a degree of privacy ».

(Bennett et Raab, 2003, p. 13). Des auteurs comme Alan Westin (1967a, 1967b), Edward Shils (1966), Arthur Miller (1971), Irwin Altman (1977) ou, plus récemment, Adam Moore (2003) ont défendu l'idée que le droit *à la* vie privée a de la valeur car même si le besoin de vie privée s'est exprimé de façon différente selon les époques et les sociétés, différentes études en anthropologie et en psychologie ont montré que l'intimité et la possibilité de protéger un espace privé sont des conditions nécessaires à l'épanouissement individuel, au bonheur (Moore, 2003), ou, dans les termes de la philosophie libérale utilitariste : de l'utilité. Une telle conception de la vie privée s'oppose donc frontalement aux déclarations de personnes comme Vinton Cerf ou Mark Zuckerberg qui, comme nous l'avons vu, ont présenté la vie privée – et plus spécifiquement le droit *à la* vie privée – comme étant une « une anomalie historique » (Cerf, 2013).

La diffusion de l'informatique en réseaux et d'Internet en particulier n'est pas le premier moment où, dans l'Histoire, des transformations dans le milieu technique – et en particulier dans les moyens de communication – ont suscité des craintes en matière de « vie privée ».

En effet, l'acte de naissance de la vision dite *cohérentiste*[19] du droit *à la* vie privée est ainsi un article de Samuel Warren et Louis Brandeis (1890), deux juristes américains, qui fut une réaction au développement de la presse de masse et de la photographie instantanée, perçues par eux comme une menace à l'ordre social bourgeois (Glancy, 1979). Ils y proposèrent l'extension du droit à l'inviolabilité du domicile – garanti par le quatrième amendement à la constitution des États-Unis – à celle de la sphère de l'intime, et définirent la « vie privée » comme le « droit d'être laissé tranquille » (« *right to be let alone* »), en empruntant cette expression aux travaux d'un juge, Thomas Cooley, qui l'avait proposée dès 1879 pour définir un « droit à l'immunité » (Cooley, 1879, p. 29).

Pour Samuel Warren et Louis Brandeis, la reconnaissance d'un droit *à la* vie privée revêtait un caractère téléologique : ils rappelèrent que la *Common Law* a d'abord protégé l'intégrité physique de l'individu, puis son intégrité spirituelle – par le biais par exemple de la propriété intellectuelle ou de lois sur la diffamation – et devait selon eux, dans la suite de ce mouvement qu'ils qualifient de « civilisateur », s'attacher à protéger l'intégrité des émotions. C'est à ce dernier élément que se rattache la protection de la vie privée : « l'Homme, sous l'influence raffinante de la culture, est devenu plus sensible à la publicité, de sorte que la solitude et la vie privée soient devenues plus essentielles à l'individu[20] » (Warren et Brandeis, 1890, p. 196). La protection de cette solitude (*seclusion*), directe descendante de la pratique des chambres de lecture au tournant du Moyen-Âge et de la Renaissance (Braunstein, 1985, p. 606), suppose une extension du contrôle de l'individu sur la publication non seulement de ses œuvres de l'esprit mais également de ses pensées et émotions, qui n'ont pas à être connues du public, ni de l'État. L'« individu » dont parlent Samuel Warren et Louis Brandeis est un « homme » de la

19 Contrairement aux réductionnistes, les cohérentistes considèrent que le droit *à la* vie privée est une catégorie ontologique cohérente et correspond bel et bien à une catégorie de droit fondamental distinct d'autres droits comme le droit *à la* liberté d'expression, ou encore le droit *à* un procès équitable.

20 Traduction de l'auteur. Texte original : « man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual »

bourgeoisie, ce qui a alimenté de nombreuses critiques, notamment féministes, de leur théorie du droit *à la* vie privée, sur lesquelles nous aurons l'occasion de revenir[21]. En outre, pour Louis Brandeis et Samuel Warren, le droit devait non seulement défendre les intérêts de l'homme qui, en tant qu'individu, pouvait subir un préjudice du fait de l'intrusion dans sa vie privée, mais aussi défendre une barrière socialement et moralement nécessaire entre ce qui méritait d'être discuté dans l'espace public et ce qui ne le devrait pas. Ainsi, bien que l'idée qu'il soit possible de porter préjudice à un *individu* en raison d'une atteinte à son droit *à la* vie privée était bien formulée par Samuel Warren et Louis Brandeis dès leur article de 1890, celle-ci y côtoyait d'autres justifications de la valeur normative du nouveau droit dont ils défendaient la reconnaissance en *Common Law*.

Le droit *à la* vie privée tel que défendu par Samuel Warren et Louis Brandeis (1890) n'est pas simplement un droit négatif[22]. Si l'État, selon eux, doit bien entendu s'auto-limiter dans ses intrusions dans la sphère privée des citoyens, il doit aussi – et cela constitue un droit positif – garantir des voies de recours contre une intrusion par une personne privée dans la vie privée d'une autre personne privée. D'ailleurs, c'est surtout ce dernier type de cas qu'ils utilisent pour illustrer leur article, en rappelant qu'ils sont facilités par deux inventions alors récentes que sont la photographie couplée à la presse de masse[23].

À partir de la fin des années 1960 et des années 1970, à la suite d'un regain d'intérêt pour le droit *à la* vie privée aux États-Unis[24] comme dans certains pays européens (Holvast, 2013) pour le droit *à la* protection de la vie privée, certains théoriciens ont introduit un nouvel élément à la définition de ce droit : l'idée du *contrôle* exercé par l'individu sur la circulation des informations le concernant.

Selon Edward Shils, c'est cette idée de contrôle qui constituerait l'unité d'un concept cohérent de droit *à la* vie privée :

> « Mais la vie privée est-elle une simple affaire « d'information » ? Qu'est-ce que la « vie privée » a de « privé », dans lequel une « figure publique » peut se retirer ? Qu'en est-il de l'espace privé, comme un bâtiment ou une chambre ou tout autre espace délimité dans lequel nul ne peut entrer sans permission ? Qu'est-ce que la « propriété privée » a de privé ? Qu'est-ce que le visage d'une personne ou ses fonctions corporelles ont de privé ? Qu'est-ce que la vie privée de la propriété a de commun avec la vie privée de la « vie » ou de l'espace ou de l'image ou de l'information ? Dans tous ces usages, nous nous référons

21 Cf. section 2.3.2. et conclusion générale.
22 Nous empruntons la distinction entre droit positif et droit négative à Isaiah Berlin (1969).
23 Cf. section 3.2.1.
24 Cf. section 3.2.

à des situations dans lesquelles l'individu ou le groupe d'individus exerce un contrôle sur les ressources qui lui appartient[25]. » (Shils, 1966, p. 283)

Se référant à Edward Shils (Shils, 1956), Alan Westin distingue la « vie privée » (« *privacy* ») du « secret » (« *secret* ») : là où le « secret » ne peut ou ne doit être divulgué par l'individu le détenant, il est libre de divulguer ou de garder pour soi une information relevant de sa « vie privée » (Westin, 2015, p. 28). Pour Irwin Altman, le point commun de toutes les variantes de l'exercice d'un droit *à la* vie privée à travers des groupes culturels éloignés est qu'il s'agit d'une modalité de « contrôle sélectif de l'accès soi[26] » (Altman, 1977, p. 67). Pour Arthur Miller, enfin, le contrôle d'un individu sur l'information qui le concerne est « l'attribut basique[27] » (Miller, 1971, p. 25) d'un droit effectif *à la* vie privée sur lequel tous les juristes et chercheurs en sciences sociales seraient parvenus à se mettre d'accord.

Les travaux d'Alan Westin, Edward Shils, Irwin Altman ou encore Arthur Miller marquent ainsi le moment où le paradigme libéral de la vie privée est passé, selon la distinction proposée par Herman Tavani (2008), d'une théorie avant tout fondée sur la restriction de l'accès à la sphère privée, à une théorie du contrôle et de l'autonomie individuels. C'est cette définition du droit *à la* vie privée comme contrôle qui a donné naissance par la suite, dans le droit de nombreux pays européens, au droit *à l'*autodétermination informationnelle[28] et dans les arènes de standardisation du Web que nous avons étudiées, à la thématique du « *user control*[29] ». Nous aurons l'occasion de revenir en conclusion sur l'importance de ce passage, et sur ce qu'il implique selon nous dans la relation entre le droit *à la* vie privée et le droit *à la* protection des données à caractère personnel.

La justification morale de l'existence d'un droit *à la* vie privée ne réside pas, pour les théoriciens du paradigme libéral de la vie privée, dans une théorie du droit naturel, qui est l'une des traditions philosophiques du libéralisme (Vergara, 2002) que nous retrouvons par exemple dans l'argumentation de John Locke en faveur de la reconnaissance d'un droit *à la* propriété privée (Locke, 1999 [1690]). La « vie privée », c'est-à-dire, pour ces théoriciens libéraux que nous avons cités, la possibilité d'exercer ce « contrôle sélectif de l'accès à soi » (Altman, 1977, p. 67), est décrite par eux comme nécessaire à l'épanouissement de l'individu, à son bonheur, ou,

25 Traduction de l'auteur. Texte original : « But is privacy only about "information"? What is private about the "private life" into which a previously "public figure" withdraws? What about private space, such as a building or a room or some other bounded area into which no one may enter without permission? What is private about "private property"? What is private about a person's face or body or bodily functions? What does the privacy of property share in common with the privacy of "life" or space or image or information? In all these usages, we refer to situations in which the individual or a group of individuals exercises control over resources that belong to them ».

26 Traduction de l'auteur. Texte original : « the selective control of access to the self ».

27 Traduction de l'auteur. Texte original : « the basic attribute ».

28 Cf. sections 3.3.2. et 4.1.2.

29 Cf. section 5.6.1.

dans les termes de la philosophie libérale utilitariste, à la poursuite de son « utilité ». C'est ce à quoi conclue Adam Moore dans ses travaux sur la « valeur » de la vie privée (Moore, 2003). Dès les années 1960, Edward Shils, réfléchissant aux dommages que peut occasionner l'intrusion dans la vie privée d'une personne, écrivait : « Les individus sont rendus malheureux […][30] » (Shils, 1966, p. 306). Alan Westin estimait qu'avoir droit à la vie privée était nécessaire pour garantir l'autonomie personnelle des individus, mais aussi leur permettre de maintenir leur équilibre émotionnel (Westin, 2015, p. 35-46).

C'est pourquoi Colin Bennett et Charles Raab, mais aussi Christian Fuchs, ont affirmé que le paradigme de la vie privée s'inspire du libéralisme utilitariste de John Stuart Mill (Bennett, 1992, p. 23-24 ; Bennett et Raab, 2003, p. 14-21 ; Fuchs, 2011). En effet, les arguments de ce dernier en faveur de la liberté individuelle, dans son livre *De la liberté*, publié en 1859 (Mill, 1989 [1859]), sont très proches de ceux que nous venons de citer sur la justification morale du droit *à la* vie privée de ce paradigme. Bien que rarement cité (voir : US House of Representatives, 1966, p. 136 ; Westin, 2015 [1967], p. 330), il existe bien un parallèle entre les deux théories philosophiques. Par manque de preuves et parce qu'il ne faut pas confondre corrélation et causalité, nous ne pouvons conclure avec certitude à une inspiration directe des travaux de John Stuart Mill (et, de fait, Harriet Taylor[31]) sur le paradigme libéral de la vie privée ; mais nous pouvons toutefois bien confirmer le caractère millien du paradigme libéral de la vie privée. Christian Fuchs nous propose une analyse abondant en ce sens.

Comme il le rappelle (Fuchs, 2011), John Stuart Mill a explicitement défendu l'existence d'une sphère privée protégeant l'individu du regard de l'État et d'Autrui, dans ses *Principes d'économie politique*, publiés en 1848 :

> « There is a circle around each individual human being which no government, be it that of one, of a few, or of the many, ought to be permitted to overstep: there is a part of the life of every person who has come to years of discretion, within which the individuality of that person out to reign uncontrolled either by any other individual or by the public collectively[32]. » (Mill, 1965 [1848], p. 938 cité par : Fuchs, 2011, p. 223)

Par ailleurs, pour John Stuart Mill, le principe moral supérieur est l'utilité – c'est-à-dire le bonheur – et sa maximisation. Ni l'État, ni aucune autre puissance, ne peut selon lui prescrire de

30 Traduction de l'auteur. Texte original : « Individuals are made unhappy »

31 Voir à ce sujet : Miller, 2019

32 Traduction en français : « […] il existe autour de chaque homme un cercle qu'on ne devrait permettre à aucun gouvernement de franchir, soit que ce fût le gouvernement d'un seul ou celui d'un petit nombre, ou celui d'un plus grand nombre. Il est une portion de vie de tout homme arrivé à l'âge de raison, dans laquelle l'individualité de cet homme doit régner sans être contrôlée, soit par un autre individu, soit par le public pris collectivement » (Mill, 1861, p. 486).
Cette traduction en français ne reflétant pas parfaitement le sens original en langue anglaise, nous avons choisi de garder la version originale dans le corps du texte.

mode de vie à l'individu sans entraver ce dernier dans la poursuite de son utilité. C'est ce qu'il rappelle dans *De la liberté*, publié en 1859 :

> « Là où ce n'est pas le caractère d'une personne, mais les traditions ou coutumes d'autres personnes qui sont la règle de conduite, il manque un des principaux ingrédients du bonheur humain, et ce qui est véritablement l'ingrédient en chef du progrès individuel et social[33]. » (Mill, 1989 [1859], p. 57)

Cette citation nous fait entrevoir la façon dont, contrairement à ce qu'affirme Christian Fuchs (2011) dans un texte qui est une critique du paradigme libéral de la vie privée qu'il décrit, la vision que John Stuart Mill développe de ce qui est devenu plus tard le « droit à la vie privée » ne correspond pas tout à fait à ce que Herman Tavani (2008) appelle la théorie de l'accès restreint. L'autonomie, c'est-à-dire la possibilité de vivre selon ses propres règles, et d'exercer des choix libres, sont en effet au cœur de la philosophie utilitariste de John Stuart Mill. Un droit *à la* vie privée qui ne reposerait pas sur une pratique de partage informationnel choisie et consentie par l'individu, mais sur le respect de normes collectives de séparation entre public et privé, même si ces dernières ont vocation à protéger l'individu, n'est pas cohérente avec sa conception générale du libéralisme utilitariste (voir à ce sujet : Vergara, 2002). La notion de « contrôle » joue ici un rôle important et qui va à l'encontre de la théorie de l'accès restreint.

Tout ce que nous venons de voir fait du droit *à la* vie privée protégeant l'autonomie individuelle telle que conçue par le libéralisme utilitariste un droit fondamental essentiellement individuel.

Nous retrouvons dans la jurisprudence de la Cour européenne des Droits de l'Homme (CEDH) ce point de vue millien pour décrire sa conception du droit *à la* vie privée proclamé à l'article 8 de la Convention européenne des droits de l'Homme. Dans un arrêt de 2017, ses juges y évoquent ainsi l'« épanouissement personnel » comme une valeur à protéger :

> « […] la notion de vie privée est une notion large, qui ne se prête pas à une définition exhaustive […]. L'article 8 de la Convention protège **le droit à l'épanouissement personnel**[34] […], que ce soit sous la forme du développement personnel […] ou sous celle de l'autonomie personnelle, qui reflète un principe important sous-jacent à l'interprétation

33 Traduction de l'auteur. Texte original : « Where, not the person's own character, but the traditions or customs of other people are the rule of conduct, there is wanting one of the principal ingredients of human happiness, and quite the chief ingredient of individual and social progress »

34 Mise en forme ajoutée par l'auteur.

des garanties de l'article 8 [sur le droit à la vie privée] » (CEDH 5 septembre 2017. Affaire « Bărbulescu c. Roumanie ». Req. 61496/08, pt. 70)

Quant à la dimension individuelle du paradigme libéral de la vie privée, elle est illustrée dans de nombreux discours institutionnels, comme par exemple dans le rapport annuel de la CNIL de 2014 où Isabelle Falque-Pierrotin, présidente de cette autorité administrative indépendante, écrivait :

> « « *Privacy is dead!*[35] » entendait-on par exemple à Davos en janvier dernier. **Non, la vie privée n'est pas morte mais elle évolue incontestablement vers une dimension plus individuelle.**[36] Aujourd'hui, les données personnelles sont la particule élémentaire du monde numérique. Elles sortent du strict champ de la vie privée et participent à la construction d'une vie publique revendiquée par les individus eux-mêmes. Ces derniers font d'ailleurs la distinction entre ce qui relève de l'intime et qu'ils souhaitent préserver et ce qui peut contribuer à leur vie publique. Ils paramètrent leur vie privée pour obtenir une exposition sur-meure, « à façon ». Aujourd'hui, plus que de protection, c'est de maîtrise que les individus sont demandeurs. » (CNIL, 2015, p. 5)

Toutefois, si l'individu doit être, selon le paradigme libéral de la vie privée, protégé de toute intrusion dans son intimité, cela l'est *aussi* pour un impératif d'intérêt général. En effet, la vie privée, l'intimité, le droit de s'isoler du regard d'autrui jouent, en plus d'un rôle dans l'épanouissement des individus, un rôle social qui, pour John Stuart Mill, est essentiel : ils offrent la possibilité d'expérimenter différents styles de vie, et notamment des styles de vie nouveaux. Des modes de vie émergents, qui sont dans un premier temps bien sûr minoritaires et donc potentiellement objet d'opprobre sociale voire de répression étatique, peuvent se révéler plus « utiles » – pour reprendre la terminologie de John Stuart Mill – que le mode de vie hégémonique du temps, et il faut dès lors permettre à ceux qui le souhaitent de l'adopter.

Dans le prolongement de cette réflexion, la protection de la sphère privée de l'intrusion étatique est perçue par certains auteurs libéraux comme un des fondements de la démocratie libérale, ce qui lui confère alors une fonction macrosociale en plus de celle de la garantie de libertés individuelles. Cela est vrai pour John Stuart Mill pour les raisons que nous avons explicitées ci-dessus, mais également pour Alan Westin ou encore le juriste Edward Bloustein :

35 En anglais dans le texte.
36 En gras dans le texte.

> « [Un] équilibre qui garantit de fortes citadelles de vie privée individuelle et de groupe, et qui limite à la fois la publication et la surveillance, est un prérequis pour les sociétés démocratiques libérales. La société démocratique repose sur la publicité comme mécanisme de contrôle sur le gouvernement, et sur la vie privée comme bouclier pour la vie individuelle et de groupe […]. La théorie libérale démocratique admet qu'une bonne vie pour l'individu doit comporter des espaces substantiels d'intérêt distants de la participation politique[37]. » (Westin, 1967b, p. 24 cité par : Bennett et Raab, 2003, p. 14).

> « L'Homme qui est obligé de vivre chaque minute de sa vie parmi les autres et dont tous les besoins, pensées, désirs, caprices ou gratifications sont l'objet du regard du public, a été privé de son individualité et de sa dignité humaine. Un tel individu se fond dans la masse. Ses opinions, étant publiques, tendent à ne jamais être différentes ; ses aspirations, étant connues, tendent toujours à être celles qui sont conventionnellement acceptées ; ses sentiments, étant ouvertement exhibés, tendent à perdre leur qualité de chaleur personnelle unique et à devenir les sentiments de chaque Homme. Un tel être, quoique doué de sensations, est fongible ; il n'est pas un individu[38]. » (Bloustein, 1964 cité par : Posner, 1977, p. 407)

À ce stade de l'évolution du paradigme libéral de la vie privée, la vie privée est conçue comme une liberté négative – où l'État se restreint dans sa surveillance de la population – mais aussi un droit positif, puisque le citoyen peut faire appel à la puissance publique pour faire protéger sa vie privée contre une autre personne privée. Enfin, c'est donc également, comme le rappelle Alan Westin (Westin, 1967b), précédemment cité, un fondement de la démocratie libérale, jouant un rôle structurel sur le régime politique.

Une étape supplémentaire reliant la valeur normative du droit *à la* vie privée à l'architecture constitutionnelle générale d'une démocratie libérale a été franchie dans une Europe centrale encore sous domination soviétique par László Sólyom, élève du juriste helleno-allemand

37 Traduction de l'auteur. Texte original : « [A] balance that ensures strong citadels of individual and group privacy and limits both disclosure and suerveillance is a prerequisite for liberal democractic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and invidual life... Liberal democratic theory assumes that a good life for the individual must have substantial areas of interest apart from political participation »

38 Traduction de l'auteur. Texte original : « The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become feelings of every man. Such a being, although sentient, is fungible; he is not an individual »

qui inventa le terme de « protection des données »[39]. Futur président de la Cour constitutionnelle et futur président de la République, il eut, à ces titres, une profonde influence sur la formation de la doctrine et du droit positif *de la* protection des données à caractère personnel en Hongrie. Il écrivait ainsi en 1988, dans un article sur la protection des données, publié en contexte de « restructuration » (« *Perestroïka* », en cyrillique : « перестройка ») dont l'un des mots d'ordre devait être la « transparence » (« *Glasnost* » en cyrillique : « гласность ») qu'« aujourd'hui, le pouvoir du Parlement est handicapé par l'énorme quantité d'information et d'expertise supplémentaire que l'appareil administratif a accumulé, et contre lequel les outils classiques n'offrent aucune parade[40] » (Sólyom, 1988a, p. 14). Il précisa ainsi l'analyse libérale en indiquant que selon lui, la seule façon d'assurer la séparation des pouvoirs, tout en offrant à la presse une réelle possibilité de faire son travail, est d'instaurer la liberté de l'information et donc l'ouverture des documents administratifs, tout en préservant l'espace privé de cette ouverture.

Pour Stefano Rotodà comme pour László Sólyom, le droit informationnel est dans ce cadre un tout, qui participe à structurer et à rendre possible un régime démocratique libéral. Le droit *à la* vie privée, qui inclut dans ces exemples le droit *à la* protection des données à caractère personnel, est donc un droit dans le chef des individus qui a une valeur d'utilité pour les individus concernés. Mais cela n'empêche pas ce droit d'être une garantie essentielle pour le bon fonctionnement d'un ordre constitutionnel démocratique et libéral, perçu comme un bien public dans le paradigme libéral de la vie privée.

Fabrice Rochelandet propose de distinguer trois dimensions de la vie privée : le secret, la tranquillité et l'autonomie individuelle (Rochelandet, 2010, p. 8-10). Ce triptyque est une bonne synthèse du paradigme libéral de la vie privée tel que défini par Colin Bennett et Charles Raab (2003) que nous venons de décrire. La présence de « l'autonomie individuelle » dans ce triptyque reflète le rôle des arguments utilitaristes milliens dans la justification morale donnée dans le paradigme de la vie privée au droit *à la* vie privée. Elle peut également être interprétée comme le reflet de l'importance prise, à partir des années 1990, par des théories foucaldiennes qui ont contribué à un renouveau de ce paradigme.

Il existe un lien entre la théorie foucaldienne et celle de John Stuart Mill (Mill, 1989 [1859]) : il s'agit de l'idée forte selon laquelle l'État n'est pas le seul lieu de pouvoir, et que c'est non seulement contre une ingérence étatique mais aussi contre une contrainte sociale diffuse mais réelle que la sphère de la liberté individuelle doit nous protéger. L'apport principal de Michel

39 Cf. section 3.3.2.

40 Traduction de l'auteur. Texte original : « A parlamenti hatatlmat ma az igazgatási apparátusok hatalmas információs és szakmai többlettudásainak való kiszolgáltatottság bénítja meg, ami a klasszikus eszközökkel kivédhetetlen »

Foucault à la théorie du paradigme libéral de la vie privée a été sa réflexion sur la discipline, le biopouvoir, et surtout, sur les dispositifs panoptiques.

Selon Oscar Gandy (1993) les NTIC bâtissent une forme de panoptique numérique.

Le panoptique est un dispositif carcéral inventé par Jeremy Bentham (1791) dans lequel les prisonniers sont placés dans des cellules, d'où ils peuvent être surveillés à tout moment, sans qu'ils puissent eux-mêmes voir les surveillants ni savoir à quel moment ils sont surveillés. Michel Foucault a ensuite étendu la notion. Parlant de « panoptisme » (Foucault, 1975, p. 228), il décrit divers cas où des mécanismes de surveillance similaires au panoptique de Bentham ont été mis en place, par exemple dans les villes pestiférées de la fin du XVII^{e} siècle. L'effet d'un tel dispositif est d'« induire chez le détenu un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir » (Foucault, 1975, p. 234). Toujours selon lui, « le Panoptique est une machine à dissocier le couple voir-être vu » qui « automatise et désindividualise le pouvoir » (Foucault, 1975, p. 203) et produit à moindre frais de violence un contrôle des individus. Pour James Katz et Ronald Rice, un panoptique est « une surveillance constante d'individus par des mécanismes parasociétaux qui influencent les comportements simplement en raison de la possibilité d'être observé[41] » (Katz et Rice, 2002, p. 272 cité par Barnes, 2006). Foucault rend possible, avec ce concept, l'observation de dispositifs panoptiques ailleurs que dans son acception initiale benthamienne d'architecture pour prisons, pour l'appliquer par exemple à l'analyse du fonctionnement des armées, ou encore de l'industrie tayloriste. Ce concept, en rencontrant des imaginaires issus de la science-fiction, a permis de penser le rôle des ordinateurs et des réseaux informatiques dans la mise en place de dispositifs contemporains de surveillance.

Lorsque, dans les années 1960, la question de la protection de la vie privée revint à l'agenda politique aux États-Unis d'Amérique, l'image du « télécran » du roman *1984* de George Orwell (Orwell, 1949) joua un rôle considérable dans la construction des imaginaires sur l'informatique naissante et les ordinateurs[42]. George Orwell est d'ailleurs cité (entre autres) dans les travaux d'Alan Westin (Westin, 2015). Le télécran se rapproche du panoptique en ce qu'il est un objet placé dans chaque pièce habitée qui permet de placer chaque personne sous surveillance à n'importe quel moment, sans que la personne surveillée ne puisse l'éteindre, ni savoir à quel moment elle est observée. En cas de comportement déviant de la norme fixée par le surveillant (le personnage mystérieux de « *Big Brother* »), l'individu observé était sanctionné, et ce dernier savait qu'il pouvait s'attendre à une telle sanction. Le télécran d'Orwell est un dispositif panoptique.

41 Traduction de l'auteur. Texte original : « constant view of individuals through parasocietal mechanisms that influence behavior simply because of the possibility of being observed ».

42 Cf. 3.2.4.

À partir des années 1980 et 1990, de plus en plus de travaux sur la sociologie de la surveillance firent un parallèle entre informatique – et notamment informatique en réseaux – et dispositif panoptique rendant possible une société de la surveillance (voir : Simon, 2002). La métaphore du panoptique, bien que très débattue entre sociologues de la surveillance (Lyon, 1994 ; Simon, 2002) permettait de comprendre le rôle de dispositifs numériques en réseau dans la dispersion des relations de pouvoir de la société néolibérale. Selon Gilles Deleuze, l'informatique permit le passage de la discipline, qui encourage l'incarcération, au contrôle, qui encourage la mobilité et qui s'exerce non plus directement sur les personnes, sur les individus, mais sur des doubles numériques « dividuels » (Deleuze, 1990 ; Simon, 2002). Cette nouvelle forme de surveillance, dont le caractère de panoptique est toujours débattu à partir de l'étalon idéaltypique décrit par Michel Foucault dans *Surveiller et punir*, est comprise comme contemporaine à la société liquide, où les relations sociales sont en état de constante reconfiguration (Bauman et Lyon, 2013 ; Lyon, 1994). Pour Mark Poster, le rôle de l'informatique (et des « bases de données ») dans le régime de surveillance contemporain a, dans sa réalité *discursive* à défaut de matérielle, les caractéristiques d'un « super-panoptique » (Poster, 1995). Elle est le fait de l'État, mais s'observe également au sein des entreprises (Zuboff, 1989). Divers travaux ont cherché à montrer l'effet concret de cette « dataveillance » (Clarke, 1988) panoptique sur des populations aux marges de la société capitaliste. C'est ainsi que John Gilliom décrivit dans *Overseers of the Poor* les dispositifs de surveillance panoptique assistés par ordinateur appliqués aux pauvres, et notamment aux bénéficiaires d'aides sociales, aux États-Unis :

> « Je vais chercher à démontrer que le système était le nouveau « superviseur du pauvre ». Le pouvoir de l'État tente de se muer en présence constante dans la vie des pauvres, aspirant à une forme informatisée du « Panoptikon », le nom donné par Jeremy Bentham à une prison idéale où tout le monde serait observé, tout le temps[43]. » (Gilliom, 2001, p. 5)

Le droit *à la* vie privée, dans ce contexte, devient pour le paradigme libéral de la vie privée une forme de résistance à l'extension d'un régime de contrôle par la surveillance qui menacerait la liberté et l'autonomie individuelles, et qui ne se comprend plus comme lié à un mode de gouvernementalité propre aux États autoritaires, mais une forme diffuse de contrôle social étroitement lié à la culture (Lyon, 2015) et à l'économie (Zuboff, 2018), y compris dans les démocraties libérales capitalistes.

L'ordinateur et l'informatique en réseaux ont ainsi pu, à partir des théories foucaldiennes, être interprétées à divers degrés comme des dispositifs de surveillance panoptiques pouvant être

43 Traduction de l'auteur. Texte original : « The system was, I will argue, the new "overseer of the poor." In a computerized aspirant to the "panopticon" – Jeremy Bentham's name for an ideal prison in which everyone is watched, all the time – the state's power tries to be a constant presence in the lives of the poor. »

mis en œuvre tant par l'État que par des entreprises privées. Ces dispositifs restreignent la liberté de l'individu de se fixer ses propres règles, c'est-à-dire limitent son autonomie au sens étymologique du terme. Le droit *à la* protection des données à caractère personnel a été conçu comme un outil permettant de limiter le pouvoir des dispositifs de surveillance sur les individus, en complément des arguments déjà développés par le paradigme libéral de la vie privée dès les années 1960. C'est par exemple en ce sens qu'il faut comprendre la référence au panoptique dans le nom de la *Fundacja Panoptykon*, une ONG polonaise membre d'*European Digital Rights*, l'un des principaux groupes d'intérêt de la coalition des défenseurs de la vie privée pendant la procédure d'adoption du RGPD[44].

Les réflexions d'Antoinette Rouvroy et Thomas Berns sur la « gouvernementalité algorithmique » partent de cette théorie foucaldienne. Leur nouveau concept désigne l'émergence d'une nouvelle forme d'organisation du pouvoir, outillée par des ordinateurs capables de collecter et de traiter des masses de traces numériques en exécutant des algorithmes, notamment à des fins de profilage. Il s'agit, selon les auteurs, d'« un certain type de rationalité (a)normative ou (a)politique reposant sur la récolte, l'agrégation et l'analyse automatisée de données en quantité massive de manière à modéliser, anticiper et affecter par avance les comportements possibles » (Rouvroy et Berns, 2013, p. 173). Antoinette Rouvroy et Thomas Berns critiquent toutefois la nature individuelle du droit *à la* vie privée et *à la* protection des données à caractère personnel, en défendant l'idée que ce n'est pas véritablement l'individu qui serait « sujet » des traces utilisées dans les dispositifs de gouvernementalité algorithmique. Bien que leurs travaux héritent du paradigme libéral de la vie privée complétée par l'apport des conceptions foucaldiennes sur le pouvoir, la discipline et les dispositifs, ils se positionnent ainsi dans une posture critique à l'égard de ce même paradigme.

Dans le même temps, la critique par la gouvernementalité algorithmique cherche à dévoiler les mécanismes de contrainte qui sont construits autour des individus par des dispositifs machiniques et qui fonctionnent comme une forme de « paternalisme technologique ». Ainsi, comme le rappelle Cléo Collomb dans une discussion de la théorie d'Antoinette Rouvroy et Thomas Berns :

> « Produisant un type de connaissance – les profils – à des fins d'anticipation des comportements pour y adapter l'environnement, l'intelligence ambiante porte atteinte à la vie privée puisqu'elle a un effet sur l'auto-détermination des individus : non seulement en agissant sur le possible de leurs actions, en en organisant les cadres, mais aussi en construisant des normes, leur présentant ce qui est calculé pour être le plus probablement pertinent pour chacun d'eux. » (Collomb, 2016, p. 110)

44 Cf. section 4.6.

Nous retrouvons donc dans les travaux sur la gouvernementalité algorithmique une attention portée à un droit *à la* vie privée compris comme droit de contrôle individuel, d'auto-détermination, de souveraineté de l'individu sur soi souhaitant échapper à une forme de déterminisme aliénant dans lequel les dispositifs socio-techniques adaptant son environnement à son profil numérique l'y enfermeraient. La théorie de la gouvernementalité algorithmique nous semble donc bien se placer dans une forme de filiation – bien que critique – du paradigme libéral de la vie privée, retravaillé par des apports foucaldiens.

Le paradigme libéral de la vie privée est celui qui a inspiré et justifié le développement du droit *de la* protection des données à caractère personnel dans les années 1960 et 1970. Il permet de comprendre les choix défendus par la coalition des défenseurs de la vie privée dans les discussions sur l'adoption du RGPD entre 2009 et 2016, et les choix rédactionnels successifs du contenu de la définition de la notion de « donnée à caractère personnel » dans le droit en Europe mais également dans les arènes de standardisation du Web que nous avons étudiées. Dire qu'il fait unanimité serait toutefois faux. Comme nous venons d'en avoir un aperçu avec les travaux d'Antoinette Rouvroy et Thomas Berns sur la gouvernementalité algorithmique, de nombreuses critiques lui furent adressées. Nous allons exposer les principales avant d'aborder deux courants de pensée qui abordent la question des données à caractère personnel et du droit *à la* vie privée par l'angle d'une réflexion sur la technique, et non en réaction critique au paradigme que nous venons d'exposer.

2.3. Les critiques du paradigme libéral de la vie privée

2.3.1. La critique néolibérale par l'École de Chicago

Les économistes néolibéraux de l'école de Chicago, à laquelle appartenait Milton Friedman, se sont intéressés à la question de la vie privée à l'occasion de leur opposition au *Privacy Act 1974* aux États-Unis d'Amérique. Richard A. Posner[45] (1977, 1981) et George J. Stigler (Stigler, 1980), prix « Nobel » d'économie en 1982, en particulier, se sont intéressés de près à la question.

Précisons à ce stade que malgré un certain rapport de filiation entre les philosophies néolibérales[46] et les philosophies libérales classiques, néolibéralisme et libéralisme présentent

45 Juriste de formation mais ayant publié des analyses économiques s'inscrivant dans le paradigme monétariste.

46 Le pluriel a été choisi pour ne pas occulter l'existence de fortes différences entre, par exemple, la philosophie de Friedrich Hayek et celle de Milton Friedman. Frédéric Marty et Thierry Kirat (2018) ont montré qu'il y avait eu également de nombreuses évolutions entre une première et une seconde école de Chicago. Notre thèse ne portant

d’importantes différences et ne doivent pas être confondus. Cela est d’ailleurs bien illustré par le fait que l’une des critiques les plus radicales du paradigme libéral de la vie privée soit l’œuvre de penseurs néolibéraux.

L'école de Chicago a développé une théorie économique libérale favorable au laisser-faire et à la régulation de marché : le monétarisme, fortement inspiré des théories économiques néoclassiques (Friedman, 1960 ; Friedman, 1962). Selon la théorie économique néoclassique, pour être efficace, le marché doit reposer sur une concurrence pure et parfaite, laquelle repose à son tour sur cinq piliers (Knight, 1921) :

- L'atomicité, qui suppose qu'aucun acteur économique ne soit en mesure de déterminer les prix sur le marché ;
- La libre-entrée et libre-sortie : chaque acteur économique peut librement et sans coût entrer ou sortir d'un marché ;
- La libre-circulation des facteurs de production (travail et capital) ;
- L'homogénéité : il existe un marché par chaque type de produit, ce qui signifie, en d’autres termes, que sur un marché donné tous les produits concurrents doivent avoir exactement les mêmes caractéristiques ;
- La transparence, qui suppose un libre accès à une information exhaustive.

Or, pour les économistes de l'école de Chicago, qui avaient travaillé dès les années 1960 sur l'économie de l'information[47], la vie privée est un comportement de dissimulation de l'information dans la sphère privée (Posner, 1977, p. 393). Non seulement il s'agit pour Richard Posner d'un comportement suspect[48], mais ce comportement est selon lui socialement nuisible, puisqu'il ferait obstruction à cette condition de transparence des marchés de la concurrence pure et parfaite. Suivant ce raisonnement, le droit *à la* vie privée est alors un obstacle à l'efficacité allocative de tout marché, qu’il s’agisse des biens de consommation, ou d’autres sphères de la vie sociale que les économistes néolibéraux ont conceptualisé comme des marchés : le travail, la famille, le choix des partenaires romantiques… Une telle vision est cohérente avec une anthropologie néolibérale de l'*homo economicus*, qui est à la fois marchandise – par exemple sur le marché du travail – et aussi un acteur économique rationnel poursuivant son intérêt économique, matériel et égoïste. Si bien que :

pas sur le néolibéralisme en général, nous n’entrerons toutefois pas plus dans les détails.

47 Voir par exemple : Stigler, 1961.

48 « Pourquoi quelqu'un voudrait-il dissimuler un fait, si ce n'est pour induire en erreur les autres afin de faire des transactions avec eux ? » (Posner, 1981, p. 408 cité par : Rochelandet, 2010, p. 30).

> « Cela n’est pas une réponse de dire que […] les individus ont « le droit d’être laissés tranquilles » […]. Très peu de gens veulent être laissés tranquilles. Ils veulent manipuler le monde autour d’eux par la révélation sélective d’information à leur sujet[49]. » (Posner, 1977, p. 400)

Les informations personnelles sont pour Richard Posner des biens intermédiaires instrumentaux (Posner, 1977, p. 394) que certains voudront dépenser comme du temps ou de l’argent à cacher, tandis que d'autres, comme les services fiscaux, un fiancé, un concurrent ou encore les organismes de crédit, chercheront à se les approprier (Posner, 1977, p. 394-395). Protéger la vie privée et les données personnelles par la Loi réduirait la quantité d'information disponible sur un marché et sur un produit (humain).

La solution que Richard Posner préconise est l'instauration de droits de propriété aliénables sur certaines données personnelles dont la dissimulation n'aurait pas d'impact social négatif. Il s'oppose par exemple à l'octroi d'un droit de propriété sur les informations dont les organismes de statistique ont besoin, en raison des coûts de transaction trop élevés que cela engendrerait pour ces derniers, mais il donne l'exemple d'une photographie nue de soi comme d'un bien informationnel personnel sur lequel l'individu concerné dispose d'un droit de propriété aliénable (Posner, 1977, p. 400).

Richard Posner ne s'oppose pas à toute idée de vie privée. En appliquant un raisonnement économique néoclassique, il conclut que l'intimité permet de se passer de certains artifices gourmands en temps et en énergie, qui sont pour lui des ressources économiques. Ainsi, la brièveté du langage familier, permis par l'intimité, ou les normes d'habillement relâchées dans l'intimité de son propre logement, sont sources d'économie, et doivent donc pouvoir être conservées (Posner, 1977, p. 403). Cette conception de la « vie privée » n’est toutefois pas celle que met en valeur le paradigme libéral de la vie privée, fondé sur l’idée de « contrôle » opéré par l’individu sur les informations qui le concernent, mais repose au contraire sur l’idée d’une frontière à défendre entre espaces public et privé.

Quoi qu’il en soit, l'utilité, reconnue dans ces cas, d'une protection de la sphère privée de l'individu a pour fondement un raisonnement de nature économique néoclassique et matérialiste, et non la nécessité de protéger un droit à l'autonomie. Ainsi, Richard Posner conteste l'idée que l'absence de vie privée empêche l'émergence de créativité, en citant que ces qualités ont pu émerger chez des individus de la Renaissance italienne ou de l'Angleterre élisabéthaine, où, selon lui, la vie privée était nettement moins bien protégée que dans les États-Unis de la seconde moitié du XXe siècle (Posner, 1977, p. 407). Il poursuit sa critique du paradigme libéral de la vie privée en indiquant que si la protection de la vie privée est présentée comme une condition d'émergence

49 Traduction de l’auteur. Texte original : « It is no answer that […] individuals have “the right to be let alone” […]. Very few people want to be left alone. They want to manipulate the world around them by selective disclosure of facts about themselves ».

de la confiance, elle demeure à cet effet un mauvais substitut à la disponibilité de l'information et à la transparence (Posner, 1977, p. 408). Enfin, il évacue sommairement la question de la surveillance d'État, qu'il juge certes indésirable, mais anecdotique par rapport à la surveillance entre individus privés (Posner, 1977, p. 409).

Ainsi, au terme de son raisonnement, Richard Posner aboutit à la conclusion que protéger les données personnelles serait un mauvais choix économique, et donc un choix socialement indésirable. Quant aux autres considérations en rapport avec la protection de la vie privée, notamment en rapport avec la sécurité de la personne, ou les risques de diffamation, il les juge, à l'instar de Judith Thomson (1975), couvertes par les autres droits fondamentaux. Contrairement au paradigme libéral de la vie privée, sa critique néolibérale appartient donc à l'école réductionniste de la vie privée, selon laquelle l'expression « droit à la vie privée » ne fait que désigner un ensemble disparate et incohérent d'éléments qui sont déjà protégés par d'autres catégories de droits préexistantes.

Le raisonnement économique tenu tant par Richard Posner – dont nous avons brièvement détaillé la pensée – que par George Stigler a été critiqué par Jack Hirshleiffer (1971, 1980), un autre économiste de l'école de Chicago selon lequel il existe des défaillances sur le marché des données personnelles. Les agents économiques ont en effet tendance à surinvestir dans la collecte de données personnelles et dans leur dissimulation. Ce comportement est inefficace au niveau macroéconomique, car cela affecte une partie du revenu disponible de cette activité qui, en elle-même n'est pas productive. Une législation sur les données personnelles réduirait selon Jack Hirshleifer de tels comportements.

Richard Posner (1977, 1978) et George Stigler (1980) rejettent cet argument en soulignant le fait qu'une législation sur les données personnelles augmenterait fortement les coûts de collecte, et donc une hausse des prix et une baisse du bien-être collectif. Cette idée renvoie à l'anthropologie néolibérale : en effet, si, comme le pense Richard Posner, l'être humain a tendance à chercher à manipuler autrui par ses comportements de dissimulation afin de maximiser son utilité, alors la Loi n'y changera rien et ne réduira pas de tels comportements coûteux.

Si l'école de Chicago s'oppose au principe même d'une protection des données personnelles, notons que Richard Posner ne conteste pas le principe de l'existence d'une protection des informations commerciales et industrielles. Là où le paradigme libéral de la vie privée s'est désintéressé progressivement de la vie privée des groupes, il déclare ainsi :

> « Je remarque en passant l'ironie que la vie privée personnelle semble être plus valorisée que la vie privée organisationnelle, si l'on en juge des tendances actuelles en matière de

politiques publiques, alors qu'un renversement de ce rapport serait plus cohérent avec l'économie du problème[50]. » (Posner, 1977, p. 393-394)

Il s'oppose donc logiquement aux politiques de liberté de l'information, dont le *Freedom of Information Act* de 1966, qui organise le libre-accès aux informations détenues par l'administration aux États-Unis d'Amérique, en violation selon lui de ce droit *à la* vie privée des organisations (et non des individus) (Posner, 1977, p. 404).

Il convient de souligner que ces approches néolibérales de la vie privée développées par l'école de Chicago ont fait l'objet de nombreuses critiques. Parmi celles-ci, Fabrice Rochelandet leur reproche ainsi un racisme latent. Selon ce dernier, George Stigler et Richard Posner défendent une « position conservatrice tournée vers les intérêts des industriels » (Rochelandet, 2010, p. 33) et rappelle les préjugés racistes présents dans un texte de Richard Posner qu'il cite :

> « En fait, la *privacy* informationnelle bénéficierait essentiellement aux individus « à risques » : ancien criminels, mauvais payeurs, salariés non qualifiés, assurés fraudeurs, fiancés non solvables… De manière symptomatique, Posner [1981] va jusqu'à assimiler ces groupes à risques aux populations noires et hispaniques. Se fondant sur un test économétrique rudimentaire, il prétend que : « les principaux bénéficiaires d'une telle législation sont des gens caractérisés par plus d'arrestations ou de condamnations, ou de rapports de crédit pires que la moyenne. Ces groupes ne sont vraisemblablement pas suffisamment cohésifs […] pour former des coalitions politiques, mais ils recoupent fortement les groupes ethniques noirs et hispaniques, qui sont organisés politiquement. [….] Il peut être très probablement dans leur intérêt de faire pression pour le passage de lois qui interdisent la « discrimination » […] Si les employeurs et les organismes de crédit sont dans l'incapacité d'utiliser ces critères pour trier les risques […], une redistribution de richesse des Blancs vers les membres de ces groupes raciaux et ethniques pourrait bien en résulter. » (Rochelandet, 2010, p. 34 citant : Posner, 1981, p. 407)

L'idée de remplacer le droit *de la* protection des données à caractère personnel par la création de droits de propriété cessibles sur ces dernières ne s'est retrouvée ni dans les débats à l'OCDE et au Conseil de l'Europe dans les années 1970, ni dans les débats ayant entouré le RGPD, ni au sein des groupes dédiés à la protection de la vie privée du W3C. Cette idée semble donc périphérique au sous-système de politique publique de protection des données à caractère personnel. Elle n'a toutefois pas tout à fait disparu. En France, Gaspard Koenig défend ainsi

50 Traduction de l'auteur. Texte original : « I remark in passing the irony that personal privacy seems to be valued more highly than organizational privacy, judging by current public policy trends, although a reverse ordering would be more consistent with the economics of the problem. »

depuis plusieurs années, dans des conférences et des interviews, l'idée qu'il doit être possible de « vendre ses données personnelles » (Auffray, 2019 ; Mouron, 2018 ; Schmitt et Madelaine, 2018). Pierre Bellanger, auteur d'un livre sur la « souveraineté numérique[51] », défend également cette idée (Bellanger, 2014, p. 202).

Le RGPD et, de façon générale, le droit *de la* protection des données à caractère personnel en Europe s'est cependant construit en opposition à cette logique de patrimonialisation des données à caractère personnel. En France, la présidente de la CNIL, Isabelle Falque-Pierrotin, s'était d'ailleurs publiquement opposée à plusieurs reprises pour dénoncer cette idée (Auffray, 2019). Dans les corpus de documents analysés dans le cadre de l'étude de terrain sur l'adoption du RGPD, cette approche était marginale, les remises en cause du paradigme libéral de la vie privée, y compris par les acteurs de la coalition industrielle, ayant été elles-mêmes assez rares[52]. Ainsi, comme l'ont écrit Arnaud Anciaux, Joëlle Farchy et Cécile Méadel, « la mise en place de droits de propriété sur les données personnelles peut dès lors apparaître comme une revendication mort-née » (Anciaux, Farchy et Méadel, 2017, p. 37).

2.3.2. La critique féministe de la vie privée

Il existe une forte tradition critique de la notion de vie privée dans la littérature féministe (Decew, 2015 ; Landes, 2003), en particulier de la part d'auteures comme Catharine MacKinnon (MacKinnon, 1989), Anita Allen (Allen, 1988) ou encore Nancy Fraser (Fraser, 1990). Nous aurons l'occasion de revenir sur cette critique, car elle a eu une importante valeur heuristique pour la formulation d'une réponse à la question de recherche initiale et la compréhension du rapport entre le droit *à la* vie privée et le droit *à la* protection des données à caractère personnel[53].

Deux arguments peuvent se distinguer dans la critique féministe de la vie privée. Le premier critique l'opposition binaire entre espace public et sphère privée, et montre comment cette distinction peut en réalité exclure des espaces publics les discours de groupes sociaux dominés, dont les femmes, exclus d'accès à l'espace public. L'autre met en exergue l'assignation progressive des femmes à des espaces domestiques, « privés »[54], qui les a privées au nom de la « vie privée » de l'autonomie que le droit *à la* vie privée est pourtant censé garantir selon le paradigme libéral.

51 Cf. section 2.4.2.
52 Cf. section 4.6.
53 Voir notamment la conclusion générale.
54 Pour un aperçu historique de l'assignation progressive des femmes à des rôles domestiques, au domaine du « privé », et de leur exclusion des espaces publics, voir notamment les travaux de Silvia Federici (Federici, 2017 [2004]).

La critique de la séparation entre sphère privée et espace public part de la critique de la notion d'espace public, définie par Jürgen Habermas comme « étant la sphère des personnes privées rassemblées en un public » (Habermas, 1988, p. 38), et fondée sur une réactualisation des catégories aristotéliciennes entre le privée, c'est-à-dire le domestique (« *oikos* », « *οἶκος* ») et la Cité (« *polis* », « *πόλις* ») (Jaulin, 2014). L'accès à cet espace public est réputé égalitaire. Pourtant, comme Joan Landes l'a montré pour la France, le passage de la culture de salons à celle de la sphère publique bourgeoise décrite, théorisée et souhaitée par Jürgen Habermas, a eu pour effet de contraindre les femmes à l'espace privé (Landes, 1988). De plus, son universalisme supposé masque des logiques de délégitimation de points de vue minoritaires, et fait oublier l'existence en réalité d'une multitude d'espaces publics fragmentés et hiérarchisés (Fraser, 1990, Benoit, 2014). Vu sous cet angle, la distinction entre un espace public et un espace privé n'est plus protectrice, mais au contraire, elle interdit de rendre publics – et donc de politiser – des discours sur ce qui relève, dans un contexte social et culturel donné, du domaine du « privé ».

Un exemple éloquent est que les violences domestiques ont longtemps été considérées comme du domaine du « privé », et donc exclues de toute perspective de politisation. Elles ont même permis à des tribunaux de juger qu'ils n'avaient pas à connaître d'affaires de viol conjugal au nom du droit *à la* vie privée. N'oublions pas qu'il fallut attendre 1992 pour que la Cour de cassation rende possible de telles poursuites France[55].

Dans l'affaire ayant conduit à ce revirement de jurisprudence, une femme avait porté plainte pour viol contre son mari. Le juge d'instruction refusa d'instruire le dossier en avançant l'argument que les actes sexuels commis contre le gré de l'épouse « entraient dans le cadre du mariage tel qu'il est traditionnellement admis[56] ». La chambre d'accusation avait suivi cet avis en énonçant « qu'à juste titre, le juge d'instruction a estimé que le mariage a pour effet de légitimer les rapports sexuels et que l'épouse ne peut invoquer son absence de consentement ou l'agressivité qui a accompagné des actes sexuels normaux pour soutenir avoir été victime de viols[57] ». La victime dut se pourvoir en cassation pour que la Cour de cassation indique clairement que : « en confirmant par ces motifs l'ordonnance de refus d'informer du juge d'instruction, alors que la présomption de consentement des époux aux actes sexuels accomplis dans l'intimité de la vie conjugale ne vaut que jusqu'à preuve contraire, la chambre d'accusation a méconnu le sens et la portée de l'article 332 du Code pénal[58] ».

C'est en ayant ce type d'affaires en tête que nous pouvons comprendre que, pour Catherine MacKinnon :

55 Cour de cassation, Ch. Crim. du 11 juin 1992. En 1984 (C. Cass. Ch. Crim. 17 juillet 1984), la Cour de Cassation avait déjà ouvert la possibilité de porter plainte pour viol contre son conjoint ou sa conjointe uniquement à des époux en instance de divorce.

56 Cour de cassation, Ch. Crim. du 11 juin 1992.

57 Cour de cassation, Ch. Crim. du 11 juin 1992.

58 Cour de cassation, Ch. Crim. du 11 juin 1992.

> « Le droit de la vie privée [« *law of privacy* »] traite la sphère privée comme une sphère de liberté personnelle. Pour les hommes, ça l'est. Pour les femmes, le privé est la sphère distincte de violence [« *violation* »[59]] et de maltraitance [« *abuse* »] intimes, qui n'est ni libre ni particulièrement personnelle. Le règne de la liberté privée des hommes est celui de la subordination collective des femmes[60]. » (MacKinnon, 1989, p. 168)

Elle en tire la conclusion qu'il faudrait donc faire exploser la distinction entre public et privé et le droit *à la* vie privée (MacKinnon, 1989, p. 191).

Ce point de vue n'est pas partagé par l'ensemble de la critique féministe de la vie privée. Ainsi, pour Judith DeCew, énoncer comme le fait Catherine MacKinnon des « faits descriptifs sur les limites pratiques de la vie privée échoue à impliquer quoi que ce soit sur la valeur normative de la quête de vie privée pour les femmes[61] » (DeCew, 2015, p. 90). Pour Anita Allen, une autre théoricienne féministe de la vie privée, l'existence d'une sphère privée est non seulement souhaitable, sous certaines conditions, mais devrait même pouvoir être imposée contre le gré de certaines personnes, ce qui en fait un point de désaccord entre elle et les théories libérales de la vie privée fondées sur le contrôle.

Anita Allen distingue deux types de « vie privée » : l'une est subie, l'autre, positive, est un facteur d'autonomie et d'émancipation. Le premier type décrit l'enfermement des femmes dans des rôles – et des espaces – domestiques, qui les contraint dans leurs choix et limite leur autonomie, tout en réduisant les occasions de pouvoir être laissées tranquilles, isolées, lorsqu'elles le désirent. Ce premier type rappelle la critique formulée par Catherine McKinnon sur la vie privée comme forme d'isolation et de dépolitisation. Le second correspond à la possibilité de pouvoir faire ses propres choix et de bénéficier lorsqu'elles le souhaitent d'espaces où se retirer de toute interaction sociale et du regard d'autrui (Allen, 2000, 1988). Anita Allen considère toutefois que, dans certains cas, il est nécessaire d'*imposer* un comportement de pudeur, c'est-à-dire de respect des normes sociales de distinction entre le « public » et le « privé », afin de ne pas mettre en péril la solidité de cette barrière protectrice reposant sur une construction sociale (Allen, 1999). Elle écrit ainsi que :

> « La critique féministe nous a permis de comprendre que les conditions de confinement, pudeur forcée, obéissance et irresponsabilité qui constituaient naguère la sphère privée ne sont pas un modèle de vie privée digne de ce nom. Ironiquement, alors même que des formes sérieuses [*meaningful*] et non-oppressantes de vie privée et de choix privé

59 NdT : Ce mot peut signifier à la fois « violence » et « viol » en anglais.

60 Texte original : « The law of privacy treats the private sphere as a sphere of personal freedom. For men, it is. For women, the private is the distinctive sphere of intimate violation and abuse, neither free nor particularly personal. Men's realm of private freedom is the women's realm of collective subordination ».

61 Traduction de l'auteur. Texte original : « descriptive facts about actual limitations on privacy fail to imply anything about the normative value of seeking privacy for women ».

deviennent envisageables et disponibles aux femmes, la vie privée est en train de perdre son lustre [*losing its cache*][62]. » (Allen, 1999, p. 728)

Cette érosion de la vie privée est due selon elle à une érosion pour du « goût » (« *taste* ») pour la vie privée (Allen, 1999, p. 756). Elle cite comme exemple d'une telle perte d'appétence le cas d'une femme faisant payer l'accès au flux vidéo d'une caméra filmant en permanence son domicile. Selon elle, cela illustrerait que le « personnel est devenu commercial » au lieu de devenir « politique » (« *the personal is commercial* ») (Allen, 1999, p. 751). Face à cela, elle appelle à l'adoption de politiques publiques qui redonneraient ce goût pour la vie privée, afin de « sauver le Public et le Privé » (« *rescuing the Public and the Private* ») (Allen, 1999, p. 749).

Ainsi, pour Anita Allen, à condition que les femmes aient le droit de faire leurs propres choix de vie au sein de la sphère privée, c'est bien la solidité de la frontière socialement construite entre cette sphère et la sphère publique qu'il faut défendre. À l'inverse, Julian Gill-Peterson a dans un article sur la pratique du sexting discuté de la possibilité d'adopter une lecture de ce phénomène présentant la pratique comme encapacitante (« *empowering* »). En effet, le sexting peut constituer une forme d'exercice de souveraineté sur soi à l'abri de formes de contrôle patriarcal. En ce sens, même si Julian Gill-Peterson ne partage finalement pas entièrement cette lecture de cette pratique, son article montre qu'une pratique qu'Anita Allen jugerait dangereuse pour le maintien d'un droit *à la* vie privée dans nos sociétés libérales contemporaines, peut être présentée dans d'autres discours féministes comme la mise en pratique même d'un droit *à la* vie privée fondé sur une notion de contrôle individuel sur la diffusion et la circulation de ses informations personnelles, émancipé des normes de contrôle social (Gill-Peterson, 2015).

La critique féministe de la vie privée et sa diversité font apparaître avec netteté la différence entre des théories fondées sur la vie privée comme restriction de l'accès à une sphère délimitée socialement, et des théories fondées sur le contrôle. Elle permet également de saisir les enjeux de la tension entre ces deux conceptions. Nous reviendrons sur ce point dans notre conclusion du présent chapitre.

2.3.3. Les critiques marxistes et marxiennes

La critique marxiste des années 1960 et 1970 s'intéressa d'abord à la façon dont l'informatique s'insérait dans les modes de production capitalistes. Pour Jean-Claude Quiniou,

62 Traduction de l'auteur. Texte original : « As a result of the feminist critique, we understand that the conditions of confinement, forced modesty, obedience, and accountability that once constituted the private sphere are not a model of privacy worthy of the name. Ironically, just when meaningful, unoppressive forms of privacy and private choice are becoming imaginable and available to women, privacy is losing its cache ».

auteur de *Marxisme et informatique*, le capitalisme n'est pas apte à permettre à l'industrie de faire des gains de productivité, parce que les logiques de marché affectent l'usage de l'informatique à des tâches selon lui improductives, comme le marketing (Quiniou, 1971, p. 46-47). Dans une société capitaliste, l'informatique accélérerait par ailleurs la socialisation des forces de travail de professions jusqu'alors libérales, notamment celle des professions intellectuelles, permettant ainsi l'exploitation de la part sociale de ce travail (Quiniou, 1971, p. 96). Or, selon Karl Marx :

> « Le mode de production capitaliste se présente […] comme nécessité historique pour transformer le travail isolé en travail social ; mais, entre les mains du capital, cette socialisation du travail n'en augmente les forces productives que pour l'exploiter avec plus de profit. » (Marx, 1872 [1867], p. 145)

Un autre point soulevé par Jean-Claude Quiniou dans sa critique de l'informatique capitaliste était d'une part les risques que l'automatisation ferait peser sur les services publics, avec la suppression des guichets qu'elle rend possible (Quiniou, 1971, p. 123-131) et, d'autre part, le risque que l'informatique soit utilisée pour centraliser les données produites par certains groupes sociaux, notamment professionnels, afin de renforcer le contrôle exercé par la classe capitaliste (Quiniou, 1971, p. 129-130). Cette dernière crainte fait écho à celles de Stefano Rodotà, constitutionnaliste italien qui fut élu député en 1979 avec le soutien du Parti communiste italien. Pour lui, la vie privée avait historiquement été une prérogative bourgeoise en raison du coût des conditions matérielles préalables à son exercice, comme celui de disposer de chambres individuelles. Elle soulève également des enjeux collectifs, et pas simplement individuels :

> « […] la défense de la vie privée, autrefois circonscrite par les limites de classe, s'étend actuellement à la collectivité. […] Cependant, cette dimension collective prise par la question comporte certaines conséquences immédiates qui restent inacceptables pour ceux qui abordent le problème du point de vue traditionnel de l'individu. Prenons par exemple le cas des fichiers de recherche utilisés par les pouvoirs publics pour décider des programmes et des actions à entreprendre en matière d'investissement. On a pu dire que ces fichiers, qui ne concernent que des agrégats de données, ne présentaient aucun danger pour le secret de la vie privée […]. Il est cependant facile de rétorquer que les mêmes fichiers de données anonymes peuvent être utilisés de façon à porter un préjudice grave aux droits individuels. Il suffit d'évoquer le tort que peut faire l'utilisation d'un agrégat de données concernant une minorité ethnique ou linguistique […]. Ayant franchi cette étape – qui mène de l'individu isolé à l'individu en tant que membre d'un groupe […] – il apparaît clairement qu'en refusant le droit d'accéder aux données anonymes on reste captif de la logique individuelle. On renonce ainsi à se prévaloir de l'occasion offerte par l'informatique dans la mesure où elle donne aux individus plus de possibilités d'intervention et de participation. […] Le fait de continuer à refuser l'autorisation

d'accéder très largement à ces données signifie non seulement que le pouvoir de prendre ces décisions reste aux mains des groupes privilégiés, mais surtout que ceux qui sont en dehors du « cercle magique » où réside l'autorité véritable de l'État n'ont pas la possibilité de critiquer les choix gouvernementaux en temps utile ni de proposer d'autres solutions adaptées à la réalité des faits » (Rodotà, 1974, p. 155-156)

Stefano Rodotà, bien qu'il n'ait pas été au sens strict un théoricien du paradigme libéral de la vie privée et qu'il se rapproche sur certains aspects de la critique marxiste, était, comme nous aurons l'occasion de le revoir[63], un défenseur de la vie privée, et défendait l'adoption d'une réglementation contraignante en matière de protection des données à caractère personnel. En France, plusieurs députés communistes avaient également déposé sur le bureau de l'Assemblée nationale française, le 21 juin 1977, une proposition de loi sur les libertés, les fichiers et l'informatique, montrant l'attention qu'ils accordaient à la question[64].

L'approche marxiste – lorsqu'elle reprend à son compte le projet politique de Karl Marx – ou marxienne – qui emprunte son appareil théorique sans nécessairement adhérer au projet politique – a développé au fil du temps sa propre critique du paradigme libéral de la vie privée. Cette critique entend resituer la notion de droit *à la* vie privée dans son contexte d'antagonisme d'intérêts de classe, et mieux prendre en compte les dimensions collectives de la vie privée. Elle est également influencée par les réflexions de Marx sur l'aliénation de la part collective du travail par la classe capitaliste, et par les théories sur le capitalisme cognitif et le *digital labor*, qui s'intéressent notamment à la captation de la valeur des données à caractère personnel produites gratuitement mais disposant d'une valeur marchande, à la base du modèle économique de nombreuses entreprises dites du « numérique ».

Le capitalisme informationnel (Castells, 1998), désigné dans le langage des stratégies de la Commission européenne[65] par la formule d'« économie fondée sur le savoir » (« *knowledge-based economy* ») est théorisé par Yann Moulier-Boutang comme étant un « capitalisme cognitif ». Après le capitalisme mercantile, et le capitalisme industriel, il s'agit d'une nouvelle phase de la grande transformation décrite par Károly Polányi (Moulier Boutang, 2007, p. 24 ; Polanyi, 2009 [1944]) où après la terre, le travail et la monnaie, l'information a été transformée en marchandise entrant dans le processus d'accumulation capitalistique. Il est également une transformation des modes de production (Moulier Boutang, 2007, p. 90) qui a des incidences sur le marché du travail qui se précarise (Moulier Boutang, 2007, p. 176) et où le modèle historique du salariat (Federici, 2017 [2004] ; Moulier Boutang, 1998) se trouve remis en question face à

63 Cf. sections 3.6. et 6.2.2.

64 Assemblée nationale (France), Ve Législature de la Ve République. Proposition de loi n° 3092 enregistrée le 21 juin 1977.

65 Cf. section 4.4.

l’émergence d’un « cognitariat », le prolétariat du capitalisme cognitif (Moulier Boutang, 2007, p. 179).

Plusieurs nouveaux types de propriété et de travail se sont en effet constitués dans cette nouvelle forme du capitalisme. Ainsi, beaucoup a été dit et écrit sur l'économie « collaborative » dans laquelle des entreprises comme Uber ou Airbnb fournissent un service de mise en relation algorithmique et souvent de paiement et « disruptent » des secteurs traditionnels comme celui des taxis ou de l'hôtellerie (Casilli, 2015)[66]. Dans ce modèle, les seuls salariés sont ceux des entreprises proposant ces services algorithmiques et de mise en relation. Une partie des utilisateurs enregistrés sur ces plateformes est composée des personnes qui effectuent le travail pour lequel une autre partie des utilisateurs utilise la plateforme de mise en relation. Ainsi, les utilisateurs inscrits sur Airbnb qui proposent leurs appartements ne sont pas salariés de cette entreprise. Les chauffeurs auxquels des applications comme Uber permettent de faire appel ne sont pas non plus des salariés, mais disposent en France d’un statut d’auto-entrepreneur. Les contraintes que ces plateformes sont capables d’exercer sur ces travailleurs sont toutefois telles que des tribunaux requalifient régulièrement cette relation en contrat de travail[67].

Une autre forme nouvelle de travail précaire que le capitalisme cognitif a fait émerger aux marges du salariat est celui de ceux qu’Antonio Casilli appelle les « travailleurs du clic » et qui fournissent la part humaine du travail faisant fonctionner des logiciels se présentant comme de pures intelligences artificielles. Une part de ce travail correspond au *digital labor* (Casilli, 2019).

Il ne faut toutefois pas confondre la notion de *digital labor stricto sensu* avec celle de travail numérique, qui elle fait plus aisément référence au travailleur cognitif de Yann Moulier-Boutang. Pour Antonio Casilli, le *digital labor* est « une contribution à faible intensité et à faible expertise mise à profit via des algorithmes et des fouilles de données » (Casilli, 2015, p. 21). Ce type de travail, comme le rappelle Antonio Casilli lui-même (Casilli, 2015, p. 31), s'inscrit bien dans le cadre du capitalisme cognitif analysé par Yann Moulier-Boutang. Mais il s'agit d'un type de travail bien particulier au sein de ce « cognitariat » émergent, qui, concrètement, correspond à l'exploitation des contenus mis en ligne par les utilisateurs de services en ligne. Ainsi, Youtube et Dailymotion ne seraient rien sans le travail des vidéastes, souvent amateurs, qui y mettent leurs vidéos en ligne, et qui ne sont pas ou mal rémunérés. Dans l'ancienne version du système « reCAPTCHA » de Google, les utilisateurs sont mis à profit pour numériser des ouvrages.

66 Voir également les numéros 212 et 213 de la revue *Réseaux*, publiés en 2018 et 2019, les numéros 1 et 2 de 2019 de la revue *Surveillance & Society*, dédiés à la question des plateformes offrant ce type de service d’intermédiation.

67 Voir par exemple : Cour d’appel de Paris (France), pôle 6, 2e chambre, arrêt du 10 janvier 2019, « M. X contre Uber ».

Figure 8 : *Capture d'écran de l'ancienne version de reCAPTCHA*[68]

Dans cette capture d'écran, le deuxième mot, généré par reCAPTCHA, ne sert véritablement qu'à vérifier que la page n'est pas consultée par un robot, mais bel et bien par un être humain. Le premier mot, « I'm », est, lui, tiré d'un livre numérisé, dont la conversion en fichier texte est réalisée de façon plus fiable par un œil humain, qui doit vérifier et valider le travail de la machine. L'internaute qui, dans cet exemple, complète le test et effectue la vérification de la qualité de la reconnaissance de caractères, n'est toutefois pas rémunéré.

Les messages publiés sur les réseaux sociaux, et les données personnelles des utilisateurs, sont soumis à cette même logique de captation de la valeur ajoutée qu'ils produisent souvent gratuitement, et qu'ils sont même incités à produire à travers une interface ludique. Ces services en ligne captant la production gratuite de leurs utilisateurs sont comparés à une aire de jeux (*digital playground*) (Scholz, 2012), qui aboutit à une situation dans laquelle :

> « […] à l'opposé du travail traditionnel, le travail numérique décontracté ne ressemble qu'à la dépense d'un surplus cognitif, qu'à l'acte d'être un locuteur dans un système de communication. Cela n'est pas du tout vécu, vu ou senti comme du travail. Ce travail numérique est très similaire à ces formes moins visibles et dévalorisées du travail traditionnel des femmes comme la garde des enfants, le travail domestique, et l'adoption (*surrogacy*)[69] » (Scholz, 2012, p. 3)

Le public des réseaux sociaux devient selon cette logique une force productive, où la frontière entre loisir et travail se brouille (Casilli, 2015, p. 28), où l'exploitation et l'aliénation, et la conflictualité, se transforment, s'invisibilisent, mais persistent.

68 Capture d'écran réalisée par l'utilisatrice "iris" sur Flickr : https://www.flickr.com/photos/irisphotos/, et disponible sous licence Creative Commons BY-ND, téléchargée le 18 juillet 2016.

69 Traduction de l'auteur. Texte original : « […] in opposition to traditional labor, casual digital labor looks merely like the expenditure of cognitive surplus, the act of being a speaker within communication systems. It doesn't feel, look, or smell like labor at all. This digital labor is much akin to those less visible, unsung forms of traditional women's labor such as child care, housework, and surrogacy. »

Antonio Casilli partage le constat de la mise en place d'une société de la surveillance (Cardon et Casilli, 2015, p. 82-83), dont le pouvoir discriminant exacerbe les inégalités. En cela, il rejoint en partie les tenants du paradigme libéral de la vie privée, et surtout sa version actualisée par les thèses de Foucault sur la gouvernementalité panoptique. Mais il insiste sur la captation de la production gratuite des utilisateurs du Web par des logiques capitalistes.

Antonio Casilli s'oppose fermement à la création d'un marché des données personnelles fondé sur la création d'un droit de propriété aliénable sur les données personnelles, arguant du risque de création d'un nouveau « marché répugnant » (Casilli, 2015, p. 38), et rappelle que, pour lui, les données personnelles sont, dans le cadre des rapports de production du capitalisme cognitif, un bien commun qu'il convient de considérer comme tel (Casilli, 2015, p. 38-39). De ce fait, la protection de la vie privée se serait transformée dans une société de capitalisme informationnel en une négociation collective entre les citoyens et les entreprises et institutions publiques traitant massivement les données personnelles de ces derniers (Casilli, 2013).

Pour Lionel Maurel et Laura Aufrère, intellectuellement proches d'Antonio Casilli, l'exploitation non-consentie de données à caractère personnel est à la fois, et de façon entremêlée, une intrusion dans la vie privée des individus et une aliénation d'une forme de travail productif :

> « Si ce qui nous échappe, ce sont simultanément les gestes de production et l'expression de soi, non consentis, alors il y a violence tant par la pénétration de notre vie privée par des acteurs extérieurs, qui viennent collecter pour les exploiter les traces de cette vie, que dans le risque de voir projeter cette intimité sur la place publique, potentiellement exposée au-dehors ce que nous pensions déposer au-dedans du privé. Il s'agit d'une violence technique, économique et politique qui demande à ouvrir une conversation collective sur la façon dont nous voulons faire société. » (Aufrère et Maurel, 2018, non paginé)

Ainsi, pour eux, les plateformes ont imposé « aux individus d'inscrire leur intimité dans un rapport de production » (Aufrère et Maurel, 2018a, non paginé), liant irrémédiablement les deux questions. L'octroi de droits de propriété cessibles sur ses données personnelles, et donc d'une rémunération en échange de leur utilisation, qui est proposée par le courant néolibéral, pourrait alors paraître une solution, puisque permettant de redistribuer à ces travailleurs une partie de leur revenu. Toutefois, selon la perspective marxienne sur la vie privée, accorder, comme le propose la conception néolibérale de la vie privée, des droits de propriété aliénables sur des données à caractère personnel dont la définition serait individualiste n'aurait pas de sens, puisque ce qui créée la valeur de ces données, ce sont les inférences statistiques qui supposent leur agrégation (Aufrère et Maurel, 2018a). Nous retrouvons ici en filigrane l'idée marxienne de l'appropriation capitaliste de la part socialisée du travail. Sous cette perspective, selon Laura

Aufrère et Lionel Maurel comme selon Antonio Casilli, le débat sur la protection des données à caractère personnel doit être une façon de faire émerger une conflictualité collective qui engage un rapport de force pour lutter contre la captation de la plus-value engendrée par les *digital laborers.*

Une telle perspective collective devrait aboutir à des décisions collectives sur les usages autorisés des données à caractère personnel, y compris des masses de données à caractère personnel, au motif qu'il s'agirait d'un bien commun (Aufrère et Maurel, 2018a). Cette idée, en se doublant d'une critique de la capacité de l'individu à consentir librement à l'usage de ses données à caractère personnel, aboutit à discréditer la définition du paradigme libéral de la vie privée comme « contrôle », au profit de la préservation imposée par des décisions collectives et démocratiques d'un espace privé libéré du regard d'Autrui mais également de l'exploitation économique, et donc d'une réhabilitation de l'idée d'une frontière public-privé garantie par la collectivité.

Christian Fuchs, un autre théoricien du *digital labor*, a lui aussi développé une critique du paradigme libéral de la vie privée. Empruntant le concept de « fétichisme » de Marx, défini comme la croyance en la naturalité intemporelle et universelle d'un phénomène socialement et historiquement situé, il reproche à des théoriciens comme Alan Westin le fait d'avoir « fétichisé » la vie privée (Fuchs, 2011, p. 224-225). Selon lui, ces derniers ont tendance à ne parler que des effets positifs de la vie privée. Rejoignant sur ce point Amitai Etzioni (1999), dont nous reparlerons, il affirme qu'une trop forte protection de la vie privée individuelle peut avoir des conséquences indésirables à l'échelle de la communauté (Fuchs, 2011, p. 224). Pour illustrer cet argument, il donne l'exemple du secret bancaire dans des pays comme la Suisse ou le Liechtenstein, qu'il accuse de favoriser l'évasion fiscale au nom du respect du droit *à la* vie privée, et donc d'être au service de la classe capitaliste (Fuchs, 2011, p. 229). Dans le même temps, il rappelle la surveillance à laquelle sont soumis les employés et les consommateurs (Fuchs, 2011, p. 230), ce qui l'amène à affirmer que « le capitalisme protège la vie privée des riches et des entreprises, mais légitime dans le même temps la violation de la vie privée des consommateurs et des citoyens[70] » (Fuchs, 2011, p. 231). Selon lui, le paradigme libéral de la vie privée est incapable de saisir la façon dont le droit libéral *à la* vie privée renforce les rapports de domination de classe et de genre, car il repose sur une conception individualiste, dérivée du droit à la propriété privée. Comme Laura Aufrère, Lionel Maurel et Antonio Casilli, il affirme que « les conceptions libérales de la vie privée échouent dans leur appréhension de l'existence sociale des humains[71] » (Fuchs, 2011, p. 226) en concevant le droit *à la* vie privée comme strictement individuel. Il propose à la place une conception qu'il qualifie de « socialiste » de la vie privée, qui inverserait les rapports de surveillance en instaurant une surveillance des riches et des

70 Traduction de l'auteur. Texte original : « Capitalism protects privacy for the rich and companies, but at the same time legitimates privacy violations of consumers and citizens. »

71 Traduction de l'auteur. Texte original : « liberal privacy conceptions fail to grasp the social existence of humans. »

entreprises, renforcerait la protection de la vie privée des pauvres, et mettrait l'exploitation des données à caractère personnel au service de l'intérêt général (Fuchs, 2011, p. 231-233). Ce faisant, il rejoint des préoccupations de Laura Aufrère et Lionel Maurel (2018) ainsi que de Stefano Rodotà (1974) sur le lien entre données à caractère personnel et données d'intérêt général.

Les critiques marxistes ou marxiennes du paradigme libéral de la vie privée ont ainsi pour point commun de rejeter la conception individualiste du droit *à la* vie privée, et de concevoir la production de données à caractère personnel dans le cadre des rapports de classe dans l'économie capitaliste, tenant compte de leur valeur économique. Nous verrons que l'existence de cette critique marxiste a généré des débats entre acteurs de la coalition des ONG pendant le processus d'adoption du RGPD, sans pour autant qu'elle ne soit parvenue – ou qu'elle n'ait stratégiquement cherché – à remettre en cause les dispositions juridiques qui sont la traduction concrète, dans ce règlement, de la conception du paradigme libéral du droit *à la* vie privée et *à la* protection des données à caractère personnel[72].

2.3.4. La critique communautariste

Christian Fuchs, dont nous venons de résumer la proposition marxienne de reformulation du droit *à la* vie privée, cite et reprend à son compte la critique dite « communautariste » du paradigme libéral de la vie privée (Fuchs, 2011).

Là où la critique par l'école de Chicago cadrait la question en fonction d'un axe opposant vie privée et bien-être macoéconomique, la critique communautariste d'Amitai Etzioni (1999) oppose le droit *individuel* à la vie privée à une diversité d'intérêts collectifs, comme la santé publique ou la sécurité :

> « Les champions de la vie privée s'opposent aussi à l'idée d'adapter les conceptions de la vie privée aux conditions sociales contemporaines – même lorsqu'ils font face à l'évidence de déficits spécifiques et significatifs en matière de sûreté publique et de santé publique – en raison d'une croyance largement partagée que la concentration de nos efforts sur le maintien de la vie privée n'a pas de conséquences négatives[73]. » (Etzioni, 1999, p. 7)

72 Cf. section 4.6.

73 Traduction de l'auteur. Texte original : « Champions of privacy also oppose the idea of adapting conceptions of privacy to contemporary social conditions – even when faced with evidence of specific and significant public safety and public heatlh deficits – because of a widely shared belief that our emphasis on maintaining privacy has no negative consequences. »

Sa critique, adressée à ceux qu'il nomme les « *champions of privacy* » (Etzioni, 1999, p. 7) est moins radicale que celle des économistes monétaristes ou que celle de Catherine MacKinnon, car elle ne remet pas en cause le principe même du droit *à la* vie privée, y compris le droit *à la* vie privée informationnelle. Ainsi, il note bien, dès ses propos liminaires, que le droit d'être laissé tranquille (« *right to be left alone* ») est nécessaire dans une société libre (Etzioni, 1999, p. 1-2), alors que l'importance de la vie privée pour l'autonomie individuelle et l'épanouissement de soi et de sa créativité était explicitement niée par Richard Posner (1977).

La problématique centrale de sa réflexion est exprimée dans son ouvrage *The Limits of Privacy* (1999) :

> « La vie privée est traitée dans notre société (plus que dans toute autre) comme une valeur hautement précieuse. Les questions sur lesquelles ce livre s'interroge sont : sous quelles conditions morales, légales et sociales ce droit devrait-il être limité ? Quels sont les dommages spécifiques et significatifs que nous subissons lorsque nous n'autorisons pas de remise en cause de la vie privée ?[74] » (Etzioni, 1999, p. 3)

Or :

> « Les champions immodérés de la vie privée n'ont pas seulement commis des excès rhétoriques, mais […] ces excès ont eu des effets significatifs et néfastes[75]. » (Etzioni, 1999, p. 7)

Ces effets sont notamment, selon lui (Etzioni, 1999, p. 7-8) :

- Le retard pris dans certaines décisions publiques qu'il juge nécessaires ;
- Le blocage de politiques publiques utiles au motif qu'elles limiteraient la vie privée ;
- Le fait d'avoir eu un effet décourageant (« *chilling effect* ») sur de telles politiques publiques ;

74 Traduction de l'auteur. Texte original : « Privacy is treated in our society (more than in any other) as a highly privileged value. The questions this book grapples with are: under which moral, legal, and social conditions should this right be curbed? What are the specific and significant harms that befall us when we do not allow privacy to be compromised? »

75 Traduction de l'auteur. Texte original : « […] Immoderate champions of privacy have not merely engaged in rhetorical excesses, but […] these excesses have had significant and detrimental effects. » (Etzioni, 1999, p. 7)

- Le fait d'avoir empêché pendant des années la mise en place d'outils d'action publique utiles pour la santé publique.

La question est donc celle d'un compromis entre les bienfaits, tant spirituels ou psychologiques que sécuritaires, de la vie privée pour un individu, et le bien commun (« *common good* »). Il choisit en particulier deux types de biens communs contre lesquels peser le droit à la vie privée : le droit à la sécurité et la santé publique (Etzioni, 1999, p. 4). Une « bonne société » (*good society*) (Etzioni, 1999, p. 5) doit trouver le bon équilibre entre liberté individuelle et responsabilité collective à l'égard de la communauté, justifiant l'appellation (revendiquée) de *communautariste* de la pensée d'Amitai Etzioni. Elle est une critique du libéralisme, puisqu'il reproche à la société américaine d'avoir, depuis les années 1960, donné une importance à l'autonomie individuelle telle, qu'elle finirait par primer sur toute considération sociétale.

Il propose un raisonnement en quatre étapes pour juger si une politique publique respecte ou non un équilibre entre protection de la vie privée et bien commun.

Tout d'abord, Amitai Etzioni estime qu'une société communautaire bien équilibrée ne limitera la vie privée que si elle se retrouve face à une menace établie, documentée et macroscopique, comme par exemple celui du SIDA, et contrairement à celle de la consommation de cannabis, qui, selon lui, étant bien moins grave, n'est pas une justification suffisante à la limitation de la vie privée (Etzioni, 1999, p. 12).

Il faut ensuite selon lui examiner dans quelle mesure la société communautaire lutte avec prudence contre ce danger tangible et macroscopique sans utiliser de mesures limitant la vie privée, par exemple en anonymisant les données de santé utilisées dans la lutte contre le SIDA (Etzioni, 1999, p. 12-13).

Il conviendrait ensuite de vérifier que les mesures mises en œuvre dans une société communautaire soient aussi peu intrusives que possible dans la vie privée des individus (Etzioni, 1999, p. 13).

Enfin, le dernier critère consiste à préférer des mesures incluant des mécanismes correctifs à l'intrusion dans la vie privée des individus nécessitée par la mesure de lutte contre la menace identifiée (Etzioni, 1999, p. 13-14).

Il illustre ce raisonnement par étapes en l’appliquant à plusieurs cas.

Dans un premier exemple, il se demande s'il est justifié d'informer une mère contre sa volonté du résultat d'un test de dépistage du SIDA effectué sur son enfant lors de la naissance. S'agit-il d'une invasion dans sa vie privée justifiée dans une bonne société communautaire ? Selon Amitai Etzioni, les « champions de la vie privée », c'est-à-dire les tenants du paradigme libéral de la vie privée, s'opposeraient certainement à une obligation d'information de la mère nonobstant son absence de consentement, et ce malgré l'intérêt de la santé de l'enfant, là où lui considère que

les intérêts de la communauté priment sur l'éventuelle volonté de la mère d'ignorer les résultats du dépistage, voire de s'opposer à ce dernier (Etzioni, 1999, p. 17-42).

Dans un autre exemple, il s'est intéressé à une loi des États-Unis d'Amérique permettant à un voisinage d'être informé lorsqu'un ancien criminel pédophile ayant purgé sa peine s'y installe[76]. De telles lois sont une intrusion dans la vie privée des anciens condamnés, les exposant à la violence de leurs voisins, et portant donc manifestement atteinte à leur sécurité. De l'autre côté, les voisins peuvent se prévaloir de l'intérêt du voisinage à se protéger des effets d'une éventuelle récidive. Finalement, Amitai Etzioni tranche en défaveur de ces lois, non pas en raison de l'intérêt du criminel, qui demeure protégé par la loi contre d'éventuels agissements violents de la part de ses voisins, mais parce qu'il juge ces lois de toutes façons inefficaces. Dès lors, elles ne sauraient être justifiées par un but qu'elles sont incapables d'atteindre[77].

En conclusion, fondamentalement, la critique d'Amitai Etzioni s'adresse au paradigme individualiste du libéralisme, qui accorderait une priorité trop grande aux intérêts individuels, dont ceux à la vie privée. En décentrant la question de la vie privée de l'individu, l'approche communautariste ne fait finalement que déplacer le curseur d'appréciation de ce qui constitue une invasion inacceptable dans la vie privée de gens de là où il est communément placé par les tenants du paradigme libéral de la vie privée, comme les juges de la Cour européenne des droits de l'Homme (CEDH)[78]. Notons à ce sujet qu'en Europe, le principe du test de proportionnalité qu'il défend est déjà mis en œuvre en la matière depuis longtemps par les juges de la CEDH et de nombreux autres tribunaux européens.

Des arguments proches de ceux d'Amitai Etzioni ont été utilisés par les acteurs de la coalition industrielle pendant le processus d'élaboration du RGPD. Ceux-ci ont en effet défendu dans leurs discours un « rééquilibrage » de la valeur relative du droit *à la* vie privée par rapport à des intérêts collectifs comme la croissance économique[79]. L'argument communautariste (selon l'acception d'Amitai Etzioni) a été mis en avant de façon encore plus évidente par la sous-coalition de l'industrie pharmaceutique, défendant (avec efficacité) de larges exemptions au régime général de la protection des données à caractère personnel au nom de l'intérêt général de la recherche médicale et de la santé publique (Rossi et Bigot, 2018).

Mais, en définitive, contrairement aux critiques marxistes et marxiennes, la critique communautariste de la vie privée ne remet pas vraiment en cause la conception libérale d'un droit

76 Megan's Law: An Act To amend the Violent Crime Control and Law Enforcement Act of 1994 to require the release of relevant information to protect the public from sexually violent offenders, 1996.

77 La capacité d'une mesure limitant la vie privée à atteindre l'objectif légitime qu'elle poursuit fait partie du test de proportionnalité effectué par la Cour européenne des droits de l'Homme et la Cour de justice de l'Union européenne.

78 Le test de proportionnalité de la CEDH, sensiblement différent de celui proposé par Amitai Etzioni, est détaillé dans les arrêts suivants : CEDH 26 mars 1987 « Leander contre Suède » Req. 9248/81 CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04

79 Cf. section 4.4.

individuel à la vie privée. Elle exacerbe même le caractère individuel de la valeur de ce droit, en l'opposant absolument aux intérêts de la « communauté », là où le paradigme libéral de la vie privée a échafaudé à partir des années 1970 et 1980 une justification qui combine la valeur de la vie privée pour l'utilité individuelle à la fonction instrumentale d'un tel droit pour l'équilibre des pouvoirs et le fonctionnement de la démocratie libérale. L'utilisation d'arguments « communautaristes » dans les discours d'acteurs de la coalition industrielle dans les négociations sur le RGPD, n'était de ce fait pas de nature à s'attaquer à la conception individualiste du droit *à la* vie privée[80].

2.3.5. L'approche par les contextes : critique ou reformulation du paradigme libéral de la vie privée ?

Une autre critique du paradigme libéral de la vie privée est la théorie de l'intégrité contextuelle proposée par Helen Nissenbaum (Nissenbaum, 1998, 2004, 2010).

Sa réflexion se fonde principalement sur la théorie que Herman Tavani (2008) appelle la théorie de l'accès restreint, qui domine selon elle le débat public aux États-Unis d'Amérique, et qui s'attache à protéger les intrusions dans l'espace privé :

> « En étudiant les champs du développement de politiques publiques, de la régulation et de la réglementation, de la jurisprudence, des pratiques sociales et commerciales au vingtième siècle, nous observons que trois principes dominent le débat public sur la vie privée. Ces trois principes s'attachent à : (1) limiter la surveillance des citoyens et l'usage d'information les concernant par des agents du gouvernement, (2) restreindre l'accès aux informations sensibles, personnelles ou privées et (3) limiter les intrusions dans des lieux considérés comme privés ou personnels[81]. » (Nissenbaum, 2004, p. 125)

Ces principes ne permettraient pas, selon elle, d'expliquer ce qui pose problème et ce qui créée la controverse dans des cas de surveillance dans l'espace public, lesquels peuvent concerner des informations qui ne sont « ni privées ni intimes[82] » (Nissenbaum, 1998, p. 559). Par exemple, pourquoi cela pose-t-il problème que des documents de l'administration publique (« *public*

80 Cf. section 4.6.

81 Traduction de l'auteur. Texte original : « Surveying the fields of public policy development, regulation and statutory law, court decisions, and social and commercial practices during the twentieth century we find that three principles dominate public deliberation surrounding privacy. The threee principles are concerned with: (1) limiting surveillance of citizens and use of information about them by agents of governement, (2) restricting access to sensitive, personal or private information, and (3) curtailing intrusions into places deemed private or personal. »

82 Traduction de l'auteur. Texte original : « neither intimate nor sensitive ».

records ») déjà accessibles au public dans des modalités d'accès hors ligne, soient mis en ligne ? Pourquoi tant de réactions lorsque les traces d'achats en ligne sont revendues par des sociétés comme Axciom ? Et pourquoi la mise en place de puces RFID dans des espaces publics, par exemple dans le domaine des transports publics, provoque-t-elle autant d'indignation ? Quid de la vidéosurveillance dans l'espace public ? (Nissenbaum, 2004).

Helen Nissenbaum écrit que le sentiment d'intrusion, dans ces affaires, n'est pas tant provoqué par le fait qu'un agent extérieur franchisse la barrière de l'espace privé ou de l'intimité, mais le fait que les informations recueillies quittent les « contextes » où il est socialement accepté qu'elles circulent dans une société donnée :

> « Un principe central de l'intégrité contextuelle est qu'il n'y a pas d'arène de la vie qui ne soit gouverné par des normes de circulation de l'information, pas d'information ou de sphères de la vie pour lesquelles « tout est permis ». Presque toutes les choses que nous faisons, les événements qui ont lieu, les transactions qui sont réalisées, se déroulent dans un contexte non seulement de lieu, mais de politique, de conventions sociales, et d'attentes culturelles. Ces contextes peuvent être définis à grands traits comme, disons, des sphères de la vie comme l'éducation, la politique, le marché ou tracés de façon fine comme des routines conventionnelles comme rendre visite au dentiste, se rendre à un mariage de famille, ou passer un entretien d'embauche. Pour certaines finalités, une définition à grands traits est suffisante. Comme précédemment mentionné, public et privé définissent une dichotomie de sphères qui ont démontré leur utilité dans la réflexion juridique et politique. Les intuitions robustes sur les normes de vie privée paraissent toutefois enracinées dans les détails de contextes plus limités, de sphères, ou de situations archétypales[83]. » (Nissenbaum, 2004, p. 137)

Selon ce principe, « une intrusion dans la vie privée a eu lieu lorsqu'une norme contextuelle de convenance ou des normes de circulation [de l'information] ont été enfreintes[84] » (Nissenbaum, 2004, p. 143). Elle trace un parallèle entre ce principe, les craintes qu'il permet d'expliquer vis-à-vis du sentiment de perte de contrôle informationnel provoqué par l'irruption de l'informatique en réseau, et celles qu'exprimaient Samuel Warren et Louis Brandeis (1890) face

83 Traduction de l'auteur. Texte original : « A central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which "anything goes." Almost everything-things that we do, events that occur, transactions that take place-happens in a context not only of place but of politics, convention, and cultural expectation. These contexts can be as sweepingly defined as, say, spheres of life such as education, politics, and the marketplace or as finely drawn as the conventional routines of visiting the dentist, attending a family wedding, or interviewing for a job. For some purposes, broad sweeps are sufficient. As mentioned before, public and private define a dichotomy of spheres that have proven useful in legal and political inquiry. Robust intuitions about privacy norms, however, seem to be rooted in the details of rather more limited contexts, spheres, or stereotypic situations. »

84 Traduction de l'auteur. Texte original : « a privacy violation has occurred when either contextual norms of appropriateness or norms of flow have been breached. »

aux évolutions de la presse et aux progrès de la photographie instantanée (Nissenbaum, 2004, p. 122). Elle définit la notion d'« information personnelle » (« *personal information* ») comme étant toute donnée, quelle que soit sa nature ou son contenu, qu'il relève ou non de l'intimité des personnes (Nissenbaum, 2004, p. 124), et qu'elle ne s'intéresse qu'à la vie privée des individus, pas celle des groupes (Nissenbaum, 2004, p. 123-124). Cela pourrait donner l'impression qu'elle se place dans la parfaite continuité du paradigme libéral de la vie privée, puisqu'elle reprend à son compte la définition de la notion de « donnée à caractère personnel » qui traduit les préoccupations et les objectifs de ce paradigme[85].

Une telle lecture serait se méprendre sur la nature de sa théorie. Là où nous avons vu qu'avec Alan Westin, Edward Shils, Arthur Miller et d'autres, le paradigme libéral, à partir des années 1960 et 1970, s'est construit sur une théorie du contrôle individuel des flux d'information, Helen Nissenbaum a bâti sa théorie sur celle de la restriction d'accès. Nous avons en effet vu, à travers quelques unes de ses citations, qu'elle conçoit sa notion de « contexte » comme un raffinement des catégories « public » et « privé ». Elle indique d'ailleurs dès 2004 ne pas adhérer aux théories de la vie privée comme contrôle :

> « La conception largement partagée d'un droit à la vie privée comme droit au contrôle de l'information sur soi, par exemple, est suffisamment capable d'impliquer des protections même dans le cas de catégories d'informations dites publiques, d'espaces publics, et contre des agents non-gouvernementaux. […] Selon la perspective de l'intégrité contextuelle, où les prescriptions sont toujours formulées en des termes contextuellement spécifiques, ces conceptions seraient considérées comme trop émoussées, et possiblement dogmatiques[86]. » (Nissenbaum, 2004, p. 154)

La théorie de l'intégrité contextuelle a connu un certain succès. Il y a plusieurs fois été fait référence dans les discussions sur l'adoption du RGPD par des acteurs de la coalition industrielle. Nous verrons ainsi comment le *Future of Privacy Forum* y a fait référence pour tenter l'une des rares remises en cause frontales du paradigme libéral de la vie privée que nous avons recensées (cf 6.10. et document FPF1, 2013, p. 7). Leur argument était de dire que le régime de protection des données à caractère personnel fondé sur le droit à l'auto-détermination informationnelle et le consentement était dépassé, et qu'un régime fondé sur l'obligation pour les entreprises de respecter les normes d'intégrité contextuelle dans la façon dont elles faisaient circuler les données serait plus pertinent.

---

85 Cf. chapitre 6.

86 Traduction de l'auteur. Texte original : « The widely held conception of a right of privacy as a right to control information about oneself, for example, is sufficiently capacious to entail protections even in categories of so-called public information, public spaces, and against non-governmental agents. […] From the perspective of contextual integrity, where prescriptions are always couched in context-specific terms, these conceptions would be considered too blunt, possibly dogmatic. »

À l'inverse, pour d'autres, consentement et intégrité contextuelle sont complémentaires. Helen Nissenbaum a été fréquemment citée en entretiens par des défenseurs de la vie privée œuvrant dans des arènes de standardisation techno-politiques du W3C, et notamment des membres du *Tracking Protection Working Group*[87]. Or, les mêmes personnes définissaient généralement la vie privée comme la possibilité d'un « contrôle » des « utilisateurs » sur les données qui les concernent. De fait, sur le terrain du W3C, nous avons observé une ré-interprétation des théories d'Helen Nissenbaum faisant la synthèse entre sa théorie – fondée sur la restriction de l'accès et le raffinement des catégories public/privé – et l'idée d'un contrôle individuel, où ce contrôle est l'outil dans les mains de l'utilisateur visant à faire respecter les règles contextuelles qu'il juge pertinentes.

Toutefois, Helen Nissenbaum elle-même s'est prononcée, ces dernières années, de façon très critique vis-à-vis du consentement (Berinato et Nissenbaum, 2018). Dans une interview publiée dans la *Harvard Business Review* en 2018, elle parle de « farce du consentement ». Elle illustre ses propos par la façon dont le consentement est souvent extorqué aux internautes par des mécanismes de manipulation (Hémont et Gout, à paraître, à paraître ; Gray et al., 2018), sur lesquels elle a d'ailleurs publié un article avec plusieurs co-auteurs (Susser, Roessler et Nissenbaum, 2018). Elle insiste également en évoquant l'affaire *Cambridge Analytica* :

> « Arrêtez de penser au consentement ! Ce n'est pas possible, et ce n'est pas bien ! Je suis respectueusement mais résolument en désaccord avec mes collègues qui croient qu'une amélioration incrémentielle des mécanismes de consentement serait la solution. Ma position n'est pas de dire que trouver un « vrai » modèle de consentement en cette ère de technologies numériques soit difficile ou même impossible, mais qu'au bout du compte, ce n'est tout simplement pas une mesure de protection de la vie privée ! Prenez le cas de Cambridge Analytica. Des personnes très éclairées se sont plaintes que « Facebook a partagé de l'information sans consentement. » Mais est-ce que c'était vraiment une affaire de consentement ? Sur la base de tous nos comportements, tout le temps, je vous jure que s'ils avaient cherché à obtenir un consentement, ils l'auraient obtenu. Ce n'est pas ça qui nous a insurgés. Ce qui nous a insurgé, c'est ce que Cambridge Analytica était en train de faire, et a fait, aux institutions démocratiques, et aussi le fait que Facebook ait été si veule qu'ils s'en soient lavé les mains. Le consentement n'aurait rien changé à l'affaire ; il aurait été facilement acquis[88]. » (Berinato et Nissenbaum, 2018, non paginé)

87 Cf. section 5.6.2.

88 Traduction de l'auteur. Texte original : « Stop thinking about consent! It isn't possible, and it isn't right. I respectfully but strongly disagree with my colleagues who believe that incremental improvement in consent mechanisms is the solution. My position is not that modeling "true" consent in this age of digital technologies is hard or even impossible, but that in the end, it's simply not a measure of privacy! Take the Cambridge Analytica case. Very enlightened people complained, "Facebook shared the information without consent." But was it really about consent? Based on all our behaviors, all the time, I promise you, if they had sought consent, they'd have gotten it. That's not what outraged us. What outraged us was what Cambridge Analytica was doing, and has done, to democratic institutions and the fact that Facebook was so craven they didn't care. Consent wouldn't

Bien qu'une synthèse de la théorie d'Helen Nissenbaum avec le paradigme libéral de la vie privée ait été faite sur le terrain par des acteurs comme ceux qui ont contribué aux travaux du W3C sur le projet de standard *Do Not Track*, elle-même se positionne bel et bien en tant que critique du paradigme libéral de la vie privée, qui tente de réhabiliter la théorie de la vie privée comme accès restreint en remplaçant les catégories floues et englobantes et « public » et de « privé » par les notions de « contexte » et d'« intégrité contextuelle ».

Après avoir décrit, sans pouvoir prétendre à l'exhaustivité, quelques unes des principales critiques adressées au paradigme libéral de la vie privée, nous étudierons quelques propositions théoriques sur le droit *à la* vie privée et/ou le droit *à la* protection des données à caractère personnel qui ne partent pas du paradigme libéral de la vie privée ou de sa critique, mais qui ont la technique et le rapport que nous entretenons avec elle comme objet principal de réflexion, plutôt que la vie privée ou les libertés fondamentales.

2.4. Les entrées par la technique

2.4.1. Utopies communicationnelles, *Big Data* et *Quantified Self*

À partir des années 1970, un courant de pensée né de la rencontre entre la cybernétique (Wiener, 1962 [1950], 2014 [1948]), de l'informatique, des utopies contre-culturelles des années 1960, et d'un imaginaire du cyberespace[89], donna naissance à diverses « utopies communicationnelles » ayant pour point commun une croyance enthousiaste en la capacité transformatrice positive des technologies numériques de l'information et de la communication, et de l'informatique en réseaux (Breton, 1997 ; Flichy, 2001 ; Turner, 2008). Selon les termes (critiques) d'Evgeny Morozov, ces technologies seraient capables d'offrir des « solutions » techniques à des problèmes économiques, sociaux ou encore environnementaux (Morozov, 2015). Ces utopies ont également pour point commun de souhaiter remettre en cause l'autorité de l'État.

---

have mattered; it would have easily been attained. »

89 Cet imaginaire d'un « cyberespace » comme « nouvelle frontière », né avec le roman de science-fiction de William Gibson, *Le Neuromancien*, en 1984 (Gibson, 1984). Il a donné lieu à la rédaction d'un texte fréquemment cité : la *Déclaration d'indépendance du cyberespace*, par John Perry Barlow (1996). Ce texte se trouve par exemple sur le site web de l'*Electronic Frontier Foundation*, une organisation non-gouvernementale états-unienne dont le nom évoque aussi cet imaginaire de la « Frontière », d'un nouvel espace à conquérir : https://www.eff.org/fr/cyberspace-independence (page consultée le 19 juillet 2019). Le texte de Pierre Lévy intitulé « La montée vers la noosphère », publié en 2000, illustre aussi l'enthousiasme utopique et fantastique engendré par cet imaginaire (Lévy, 2000).

Nous verrons qu'elles ont eu, de ce point de vue, une influence certaine sur la constitution des arènes de gouvernance d'Internet[90].

Notre propos n'est pas, ici, de dresser un panorama de ces utopies communicationnelles. Elles sont en effet très diverses ; utopie du *Libre* (Broca, 2013) et utopie transhumaniste (Kurzweil, 2010 ; Yudkowsky, 2001) ne sauraient être confondues. Également, comme le rappellent Fidelia Ibekwe-Sanjuan et Françoise Paquienséguy dans un article sur l'*Open Data* et le *Big Data*, il convient de distinguer les courants techno-utopistes néolibéraux (ou ultralibéraux) des courants libertariens, qui, s'ils peuvent avoir des revendications convergentes, n'en sont pas moins différents du point de vue du noyau de leurs convictions (Ibekwe-Sanjuan et Paquienséguy, 2015). De même, lorsque Benjamin Loveluck parle de « libéralisme informationnel », il montre bien que des inspirations axiologiques différentes aboutissent sur le Web à des modèles d'organisation différents selon les sites étudiés (Loveluck, 2015). Présenter ces théories de façon exhaustive demanderait donc un investissement considérable en temps et en écriture. De surcroît, toutes les utopies communicationnelles ne proposent pas nécessairement de discours sur la vie privée, ou sur les données à caractère personnel. Nous nous intéresseront donc ici à un type de discours particulier, au sein du paradigme « dataïste » (van Dijck, 2014) : le mouvement dit du « *Quantified Self* ».

Le *Quantified Self Movement*, ainsi qu'il est désigné par ses membres, bien que n'étant pas en tant que tel un mouvement politique au sens où il n'a pas vocation à participer au processus partisan institutionnel ni n'appelle explicitement à un changement de société, s'inscrit dans le mouvement utopiste de la Silicon Valley étudié entre autres par Fred Turner et, plus récemment, Félix Tréguer (Fotopoulou, 2014 ; Ruckenstein et Pantzar, 2019 [2017] ; Tréguer, 2019 ; Turner, 2008). Pour Minna Ruckenstein et Mika Pantzar, le « *Quantified Self* » est une « métaphore ontologique » (Ruckenstein et Pantzar, 2019, p. 57) qui désigne un ensemble de pratiques appuyées par des discours et « l'idée que divers outils et applications d'autosuivi, comme les dispositifs de suivi des émotions ou de l'alimentation ou les podomètres, présentent à tout un chacun une bonne opportunité de comprendre son corps, son esprit et sa vie quotidienne, exprimés en séries de mesures pouvant être étudiées et travaillées » (Ruckenstein et Pantzar, 2019, p. 57)[91]. Ces pratiques se sont développées notamment dans le domaine de la santé. Elles peuvent être des pratiques de groupe (Lanzing, 2016). Le *Quantified Self* s'inscrit dans la continuation de ce que Michel Foucault désigne par les « technologies de soi » (Foucault, 1988). Sa nouveauté réside dans l'utilisation croissante de capteurs connectés pour générer des données se présentant comme plus « objectives », et dans l'introduction d'un rapport cybernétique au corps. Les boucles de rétroaction générées à partir des données collectées – et de leur comparaison à des agrégats statistiques – doivent aider l'individu à s'améliorer. Ainsi, « dans le

90 Cf. sections 5.1. et 5.2.

91 Voir aussi, au sujet des pratiques de mesure de soi, les articles de Moustafa Zouinar (2019), Éric Dagiral *et al.* (2019), Anne-Sylvie Pharabod (2019) et Marjolein Lanzing (2016).

contexte du [*Quantified Self*], les flux de données personnelles, y compris les informations sur le matériel génétique, les réactions physiologiques et les mouvements quotidiens, s'inscrivent dans un cadre de communication plus large, dans lequel les données personnelles sont considérées comme dotées de sens et d'agentivité, en ce sens qu'elles favorisent de nouveaux modes de conduite et de relation aux autres » (Ruckenstein et Pantzar, 2019, p. 60).

Le magazine *Wired* a joué un rôle important dans la construction théorique de l'idéologie du *Quantified Self*. Il s'agit d'un magazine influent de la Silicon Valley ayant poursuivi l'œuvre entamée par les auteurs du *Whole Earth Catalog* (Turner, 2008), avec une ligne éditoriale techno-optimiste, et proposant un programme de transformation sociale par la technologie. C'est dans ce magazine qu'en 2008, Chris Anderson avait publié un article annonçant la « fin de la théorie », en raison du « déluge de données » (« *data deluge* ») qui rendrait une science hypothético-déductive s'attachant à la recherche de liens causaux obsolète (Anderson, 2008). Le « déluge de données » dont parle Chris Anderson dans son article évoque le volume de données qui sont l'une des trois caractéristiques du *Big Data*, aux côtés de la variété des données utilisées et de la vitesse de calcul permettant de les traiter de façon pertinente (Laney, 2001).

Quantified Self et *Big Data* appartiennent au même paradigme dataïste, selon lequel la collecte d'une quantité massive de données doit permettre un meilleur accès au réel, en raison du caractère supposément *im*médiat des traces numériques (Jeanneret, 2011 ; Schmitt, 2015). De la même façon que les masses de données doivent permettre une connaissance en temps-réel de la réalité macroscopique – y compris sociale – le *Quantified Self* propose, à une échelle micro, aux individus de « vraiment » se connaître grâce à l'objectivité machinique (Bonenfant et al., 2015 ; Lanzing, 2016 ; Ruckenstein et Pantzar, 2019). Notons que les statistiques de mesure individuelle sont comparées aux statistiques agrégées de toutes les mesures individuelles collectées par un fournisseur de services de mesure de soi afin de pouvoir situer sa performance quantifiée au sein d'un groupe, d'une norme statistique.

Une telle mesure, quantification et mise en données du monde et de soi peut être perçue comme la participation à un dispositif disciplinaire, comme un « asservissement » à une « sémiotique machinique » (Bonenfant et al., 2015). D'autres peuvent s'inquiéter de la difficulté à garantir la confidentialité de ses données et l'absence de détournement des finalités pour lesquelles elles ont été collectées (voir : Lanzing, 2016). En bref, il est possible de faire une lecture aliénante et limitante pour l'autonomie individuelle des pratiques de quantification de soi. De telles lectures seraient cohérentes avec le paradigme libéral de la vie privée réactualisé par les théories foucaldiennes. Les partisans du *Quantified Self* voient au contraire quelque chose d'émancipateur dans ces pratiques. Pour eux, elles permettraient de renforcer le contrôle sur soi de l'individu.

Kevin Kelly, un ancien de la *Whole Earth Review*, co-fondateur de *Wired*, et Gary Wolf, contributeur dans ce dernier magazine, ont contribué à façonner le concept de *Quantified Self* dans un article de 2009, où ils exposent l'intérêt selon eux de la quantification de soi dans le but d'améliorer la connaissance de soi :

> « Mon collègue auteur chez *Wired* Kevin Kelly et moi avons remarqué que beaucoup de nos proches commençaient à s'infliger cette chose terrible : trouver des façons astucieuses d'extraire des flux de nombres d'activités humaines ordinaires. Une nouvelle culture des données personnelles était en train de prendre forme. La cause immédiate de cette tendance était évidente : de nouveaux outils ont rendu le suivi de soi plus facile. Dans le passé, les méthodes d'évaluation quantitative étaient laborieuses et ésotériques. Vous deviez prendre les mesures à la main et les inscrire dans un registre ; vous deviez entrer les données dans des feuilles de calcul et opérer des calculs en utilisant des logiciels peu conviviaux ; vous deviez construire des graphs pour extraire une compréhension de ces nombres. Maintenant, une large part de cette collecte de données peut être automatisée, et la tenue de registres et l'analyse peuvent être déléguées à une foule d'applications Web simples. Accompagnant l'apparition presque quotidienne de nouveaux systèmes de suivi, nous avons décidé de créer un site Web pour les lister. **Nous avons appelé notre projet le Quantified Self**. Nous n'avons pas de slogan, mais si nous devions en avoir un, ce serait probablement : « **La connaissance de soi par les nombres** »[92]. » (Wolf[93], 2009, non paginé)

Les auteurs de l'article cité ci-dessus ont fondé en Californie une compagnie appelée *Quantified Self Labs* qui organise des conférences, réunions et expositions sur le thème du *Quantified Self*[94]. Cette compagnie est mécénée par Autodesk, Intel et Scanadu[95].

---

92 Traduction et mise en forme de l'auteur. Texte original : « My fellow Wired writer Kevin Kelly and I noticed that many of our acquaintances were beginning to do this terrible thing to themselves, finding clever ways to extract streams of numbers from ordinary human activities. A new culture of personal data was taking shape. The immediate cause of this trend was obvious: New tools had made self-tracking easier. In the past, the methods of quantitative assessment were laborious and arcane. You had to take measurements manually and record them in a log; you had to enter data into spreadsheets and perform operations using unfriendly software; you had to build graphs to tease understanding out of the numbers. Now much of the data-gathering can be automated, and the record-keeping and analysis can be delegated to a host of simple Web apps. With new tracking systems popping up almost daily, we decided to create a Web site to track them. We called our project the Quantified Self. We don't have a slogan, but if we did it would probably be "Self-knowledge through numbers." »

93 L'article est rédigé à la deuxième personne du pluriel. Gary Wolf parle bien de « Kevin Kelly » et lui. Toutefois, Kevin Kelly n'est pas crédité sur le site de *Wired* comme co-auteur de l'article.

94 Voir leur site Internet : www.quantifiedself.com (page consultée le 19 juillet 2019).

95 Information indiquée sur la page d'accueil du site Internet www.quantifiedself.com (page consultée le 29 avril 2016).

Sans qu'ils ne cherchent à dialoguer avec le paradigme libéral de la vie privée, nous voyons se dessiner dans la citation tirée de leur article les contours d'un discours sur la collecte de données à caractère personnel alternatif à celui selon lequel la mise en données numériques ferait courir des risques à la vie privée et, ce faisant, à l'autonomie individuelle.

Selon Marjolein Lanzing (2016), l'idée fondamentale sous-tendant le mouvement du *Quantified Self* est que la collecte de données sur ses activités renforce l'auto-transparence, permet une meilleure connaissance de soi, débarrassée de biais car quantifiée et mesurable. L'utilisateur d'objets mesurant ses activités en voit sa capacité d'action sur soi accrue, permettant une extension de sa volonté à travers eux. Se mesurer soi-même permet de suivre sa performance, de s'améliorer, d'agir sur soi (Lanzing, 2016 ; Ruckenstein et Pantzar, 2019). Vu sous cet angle, la collecte de données personnelles est un facteur d'émancipation, de construction d'un individu autonome *agissant*. Marjolein Lanzing illustre cela en citant le cas d'une femme atteinte de Parkinson qui, lors d'une conférence à Amsterdam sur le *Quantified Self*, avait expliqué que grâce à des capteurs numériques, elle était désormais capable de fixer elle-même la posologie de ses médicaments, renforçant son autonomie vis-à-vis de ses médecins (Lanzing, 2016, p. 3). L'article signé par Gary Wolf en 2009 mentionnait aussi d'autres objectifs, comme celui d'améliorer sa performance sportive ou de perdre du poids (Wolf, 2009), qui sont ceux repris et promus par les entreprises fabriquant des objets connectés comme FitBit :

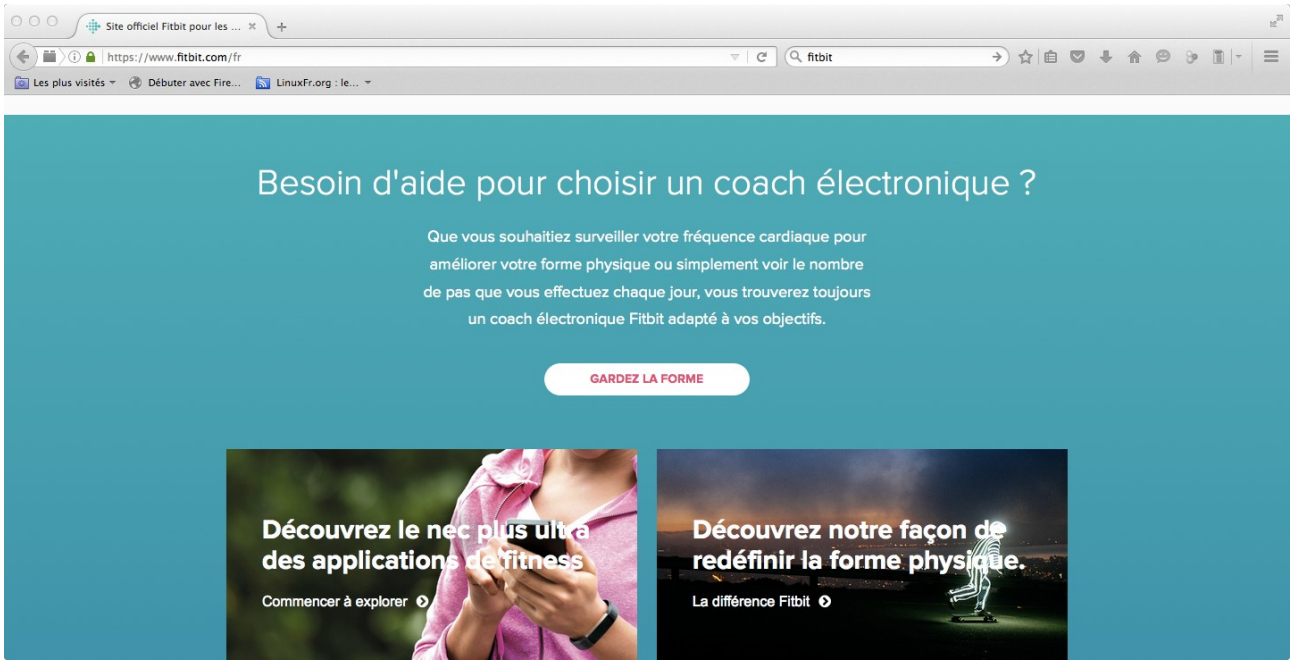


Figure 9 : *Capture d'écran du site Internet www.fitbit.com/fr prise le vendredi 29 avril 2016*

Les pratiques de suivi de soi (*self-tracking*) ne se limitent pas à la mesure ubiquitaire et continue de données souvent physiologiques sur ses activités. Elles s'accompagnent de pratiques de dévoilement de soi :

« Fitbit et Strava emploient des stratégies sociales différentes. À travers ces stratégies, l'utilisateur autorise quelqu'un d'autre à exercer un contrôle sur lui ou sur elle. Des exemples de stratégies sociales sont les dates butoirs, le travail d'équipe et la quête de la « bonne » compagnie pour soutenir le comportement désiré. Fitbit et Strava offrent des fonctionnalités de médias sociaux, des forums et des groupes où les utilisateurs peuvent partager de l'information tant avec des « amis » qu'avec des étrangers virtuels. C'est ainsi que les utilisateurs peuvent se surveiller et s'encourager mutuellement.

Beaucoup de *self-trackers*[96] sont fiers de partager leurs informations personnelles. Pourtant, beaucoup d'entre eux sont préoccupés par leur vie privée. Les producteurs de technologies de suivi de soi ont intérêt à encourager l'auto-divulgation d'informations personnelles ; la vente de données personnelles de santé agrégées est un commerce lucratif[97]. » (Lanzing, 2016, p. 5)

Ce partage de données, loin toutefois d'être jugé négativement par le *Quantified Self Movement*, est au contraire perçu comme positif, et comme le signe que la pratique du traçage de soi n'est pas simplement narcissique :

« Bizarrement, toutefois, la culture du *self-tracking* n'est pas particulièrement individualiste. En fait, il y a une tendance forte parmi les *self-trackers* à partager les données et à collaborer sur de nouvelles façons de s'en servir. Les gens surveillent leur régime en utilisant *Tweet What You Eart!*, peuvent profiter de compteurs de calories crowdsourcés ; les gens peuvent suivre le rythme du sommeil de leurs bébés avec *Trixier Tracker* et le comparer à celui d'autres enfants ; les femmes peuvent observer leur cycle menstruel avec *MyMonthlyCycles* et utiliser des outils en ligne pour corréler leurs diagrammes avec celui des autres. Les sites les plus ambitieux agrègent les données personnelles pour des tests pharmaceutiques conduits par les patients et la recherche médicale.

Les *self-trackers* semblent impatients de contribuer à notre connaissance de la vie humaine.[98] » (Wolf, 2009, non paginé).

96 NdT : le mot anglais « self-tracker » était difficile à traduire. Nous avons choisi de le laisser en anglais afin de faciliter la traduction, sa compréhension en français étant de plus suffisamment transparente pour ne pas gêner la lecture. Une traduction par périphrase aurait pu être : « personnes pratiquant la quantification de soi à des fins de suivi personnel ».

97 Traduction de l'auteur. Texte original : « Fitbit and Strava employ social strategies. Through these strategies the user authorizes someone else to exercise control over her. Examples of social strategies are deadlines, teamwork and seeking out of the "right" company to support the desired behavior. Fitbit and Strava offer social media options, forums and groups where users can share information with anyone ranging from "friends" to virtual strangers. Hence users can check on and encourage each other.
Many self-trackers proudly share their personal information. Yet, many of them are concerned about privacy. Producers of self-tracking technologies have an interest in encouraging self-disclosures of personal information; selling aggregated personal health data is a lucractive business. »

Ainsi, la quantification de soi permet pour les partisans du *Quantified Self* une émancipation par l'autonomisation[99] par la génération de données personnelles à partir de leurs activités et le suivi de ces données quantitatives. Leur partage est perçu comme un acte altruiste permettant d'accroître la quantité d'information disponible, de la faire circuler, et ainsi d'améliorer nos vies[100]. Enfin, le contrôle par les pairs est sous ce paradigme un exercice disciplinaire utile aux fins poursuivies par l'usager de capteurs connectés. Le mouvement du *Quantified Self* s'oppose donc au paradigme libéral de la vie privée selon lequel la protection de la sphère de l'intime (*privacy*) est une condition nécessaire et essentielle à l'autonomie de l'individu, puisqu'il avance au contraire l'idée que la collecte et le partage ubiquitaires de données personnelles permet une autonomisation des individus tout en augmentant le bien être social.

2.4.2. La souveraineté numérique

La « souveraineté numérique » est un thème très présent, notamment en France, dans l'espace public médiatique[101]. En 2016, François Pellegrini, membre du collège de la CNIL depuis 2014, publiait une tribune sur son site où il disait l'importance à ses yeux de créer un « système d'exploitation souverain » (Pellegrini, 2016). La même année, le « renforcement » de la « souveraineté numérique » a fait l'objet d'une déclaration lors d'un conseil des ministres franco-allemand[102]. En 2018, le think-tank *European Council on Foreign Relations* publiait un article prônant une « souveraineté numérique » européenne[103]. En mai 2019, le Sénat français a constitué une commission d'enquête parlementaire sur la « souveraineté numérique[104] ». En collaboration avec l'ANSSI, l'Institut des hautes études de défense nationale français organise une formation intitulée « souveraineté numérique et cybersécurité[105] ».

98 Traduction de l'auteur. Texte original : « Oddly, though, self-tracking culture is not particularly individualistic. In fact, there is a strong tendency among self-trackers to share data and collaborate on new ways of using it. People monitoring their diet using Tweet What You Eat! can take advantage of crowdsourced calorie counters; people following their baby's sleep pattern with Trixie Tracker can graph it against those of other children; women watching their menstrual cycle at MyMonthlyCycles can use online tools to match their chart with others'. The most ambitious sites are aggregating personal data for patient-driven drug trials and medical research. Self-trackers seem eager to contribute to our knowledge about human life. »

99 Autonomisation est le terme recommandé par l'Office québécois de la langue française pour traduire la notion anglaise d'*empowerment*.

100 Nous retrouvons ici l'inspiration cybernétique qui promeut la circulation de l'information.

101 Voir, par exemple : Ashley, 2019 ; Berretta, 2016 ; Guiton, 2019 ; Wang, 2019.

102 Voir : https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany/ (page consultée le 25 juillet 2019).

103 Voir : Hackenbroich, 2018.

104 Voir le communiqué de presse du Sénat (France) du mardi 7 mai 2019 « La commission d'enquête sur la souveraineté numérique a constitué son Bureau ». Disponible en ligne : http://www.senat.fr/presse/cp20190507.html (page consultée le 26 juillet 2019).

105 Voir : https://www.ihedn.fr/formation/session-nationale-souverainete-numerique-et-cybersecurite (page consultée le 25 juillet 2019).

La souveraineté, implicitement nationale, est une construction politique du système international westphalien, qui s'est peu à peu imposé au détriment d'espaces non-étatiques précédemment majoritaires (Scott, 2009). Elle a été conceptualisée notamment par Machiavel (2007 [1532]), Jean Bodin (Bodin, 1576) et Thomas Hobbes (Hobbes, 2000 [1651]). Pour Jean Bodin, elle est la « puissance absolue et perpétuelle d'une république » (Bodin, 1576, p. 152). Cette indivisibilité absolue (en théorie) de la souveraineté étatique est rappelée par la définition que Max Weber donnait de l'État : l'organisation détentrice du monopole de la violence physique légitime (Weber, 2011 [1917-1919 ; 1959]).

L'expression « souveraineté numérique » a été précédée par celle de « souveraineté technologique », qui fut proposée par Paul Grant dans un article publié en 1983 dans la revue *Prometheus*. Il définit cette notion comme la « capacité et la liberté de sélectionner, générer ou acquérir et de mettre en œuvre, utiliser comme base et exploiter commercialement la technologie nécessaire à l'innovation industrielle » (Grant, 1983, p. 239).

Les discours sur la « souveraineté numérique » apparaissent en réaction à la crise de la souveraineté westphalienne (Couture et Toupin, 2017), qui éclate l'indivisibilité de cette souveraineté d'une part par des mouvements de transferts de compétence vers l'échelon intergouvernemental voire supranational, vers l'échelon infra-étatique avec des logiques de décentralisation, mais aussi, d'autre part, au profit de modes de gouvernance privée ou « multi-partie-prenantes » comme dans le modèle de la gouvernance d'Internet (Belli, 2016 ; Kleinwächter, 2012). Ils sont aussi une réaction à des discours et pratiques inspirés par la « déclaration d'indépendance du cyberespace » de John Barlow (Barlow, 1996). Ils reflètent souvent les craintes d'une hégémonie des États-Unis d'Amérique et des entreprises américaines sur les technologies de l'information et la communication (Couture et Toupin, 2017). Le thème a ainsi été évoqué par Dilma Roussef, l'ancienne présidente du Brésil, en réaction aux révélations d'Edward Snowden, pour défendre un plan visant à « extraire » son pays du contrôle qu'elle accusait les États-Unis d'exercer sur Internet (Holpuch, 2013). Des pays comme la Chine et la Russie ont mis en place des stratégies visant à défendre leur « souveraineté » étatique. Début 2019, le gouvernement russe annonçait un test de « déconnexion » du pays d'Internet, qui visait à vérifier s'il était possible de couper la connexion entre les réseaux informatiques (ou systèmes autonomes) russes avec tous les réseaux étrangers (Cimpanu, 2019). Les détracteurs d'une telle approche parlent d'un risque de « balkanisation » et, *in fine,* d'éclatement d'Internet (voir par exemple : Ferran, 2019).

L'adoption du RGPD a été présentée dans des communiqués de presse comme étant une bonne nouvelle pour la « souveraineté numérique » de l'Europe. La commissaire Věra Jourová

indiqua ainsi dans un communiqué de presse publié la veille de l'entrée en application du règlement que « par le règlement général sur la protection des données, l'Europe assoit sa souveraineté numérique et se prépare à l'ère numérique » (Commission européenne, 2018b, STATEMENT/18/3889). Cet argument n'a toutefois pas joué le rôle central qu'a joué, par exemple, l'argument de la « nécessité » d'un règlement de protection des données garantissant la « confiance » des citoyens et des consommateurs en « l'économie numérique[106] ». Il est plutôt venu en complément de tous les autres, et n'a pas été évoqué par les acteurs interrogés en entretien, sauf pour répondre à une question portant directement dessus et dire qu'il n'avait pas été un argument central.

Argument de complément ou non, les auteurs de théories et de discours sur la « souveraineté numérique » ont accordé une importance particulière à la question des données à caractère personnel, sans toutefois qu'il y ait de consensus entre eux sur les mesures concrètes (ou « mesures secondaires » dans le vocabulaire de l'ACF) à adopter pour permettre tant à l'État qu'aux individus de « regagner le contrôle » sur les données à caractère personnel. Tristan Nitot, Nina Cercy et Pierre Bellanger sont trois auteurs français ayant écrit à ce sujet. Sans présumer de leur représentativité sur l'ensemble de discours produits sur le sujet dans le monde, leurs livres sont pertinents ici dans la mesure où ils proposent des discours sur les données à caractère personnel fondés sur l'idée de la souveraineté numérique.

Les « GAFAM », c'est-à-dire les entreprises états-uniennes comme Google, Amazon, Facebook, Apple et Microsoft, sont accusées par ces auteurs de « piller » les données à caractère personnel (Nitot et Cercy, 2016, p. v). Pour Pierre Bellanger :

> « L'Europe est le Pays de Cocagne du vol de données. Imaginez : 500 millions d'habitants, 13 trillions d'euros de produit intérieur brut, supérieur à celui des États-Unis et triple du PIB chinois… Et aucune réglementation efficace sur les données… […] Une étude récente du Boston Consulting Group évalue la valeur de ces données informatiques personnelles en Europe à un trillion d'euros en 2020. » (Bellanger, 2014, p. 185)

Adhérant au paradigme dataïste (Dijck, 2014) sur l'efficacité des méthodes reposant sur le « Big Data », Pierre Bellanger, qui dirige l'entreprise française Skyrock, est sensible à la valeur économique des données à caractère personnel. Pour Tristan Nitot et Nina Cercy aussi, les données sont le « pétrole du XXI^{e} siècle » (Nitot et Cercy, 2016, p. v). Ces préoccupations économiques sont en lien direct avec celles sur la garantie de la souveraineté de l'État-Nation. Pour Pierre Bellanger :

106 Cf. section 4.5.

> « C’est non seulement un enjeu de vie privée pour des millions de personnes, mais aussi de compétitivité économique et de sécurité nationale pour tous. » (Bellanger, 2014, p. 202)

> « Une nation sans secret n’a plus d’économie : sa propriété intellectuelle est maraudée. Une nation sans secret n’a plus de défense : sa stratégie connue d’avance restera sans effet. Pour les individus, c’est leur être intime qui est menacé. Leur intégrité et leur dignité sont en jeu. Ils sont à la merci de toute interprétation, altération, manœuvre, manipulation, chantage, déstabilisation, malveillance. Leur vulnérabilité est totale. » (Bellanger, 2014, p. 187)

La dernière citation montre le lien fait dans les discours sur la « souveraineté numérique » entre la souveraineté de l’État et celle de l’individu, repéré par Stéphane Couture et Sophie Toupin dans leurs travaux à ce sujet (Couture et Toupin, 2017). Pour Tristan Nitot et Nina Cercy, la « souveraineté numérique » serait nécessaire pour retrouver le « contrôle » sur les données – personnelles comme non-personnelles – tant pour l’État que pour les individus. Nous retrouvons ici des notions d’autonomie et de liberté, mais contrairement aux discours libéraux sur la vie privée, ce droit au contrôle n’est pas accordé seulement aux individus mais également à un collectif, la « Nation », sur laquelle repose la légitimité d’un État dont l’indivisibilité du pouvoir doit être garantie au nom de la « souveraineté ».

Toujours selon ces mêmes auteurs, la solution à la « perte de contrôle » repose dans l’adoption et à la mise en œuvre des principes du logiciel libre (Nitot et Cercy, 2016), c’est-à-dire de logiciels dont le code source est publié et librement modifiable par la communauté de ses utilisateurs (Broca, 2013). Cela passe également, pour lui, par le « rapatriement » (Nitot et Cercy, 2016, p. 3) des données chez soi, c’est-à-dire sur ses propres équipements, et donc également sur le territoire national de résidence de la personne sur qui portent les données en question :

> « Nos données sont stockées chez les acteurs qui les récupèrent : impossible de demander à Facebook de communiquer avec Google pour améliorer ses services, interdiction à ma banque de récupérer en direct ma consommation électrique (et heureusement !) pour provisionner la somme d’argent correspondante en direct. Mais si je récupère toutes ces données, rien ne m’empêche d’en faire ce que je veux tant que c’est moi qui le décide. Ces données m’appartiennent. Être souverain sur elles, c’est gagner en autonomie. » (Nitot et Cercy, 2016, p. 2-3)

Ces propositions sont directement inspirées des discours sur le Libre.

À l'inverse – et nous entrons là dans l'exposition de points de désaccord – Pierre Bellanger opte pour une solution inspirée des conceptions néolibérales de l'École de Chicago, en proposant de reconnaître des droits de propriété cessibles sur les données à caractère personnel. Cette mesure serait plus efficace, selon lui, que le droit *de la* protection des données à caractère personnel alors en vigueur :

> « À ce jour, les données n'appartiennent en droit à personne. Elles sont *res nullius*. Dans les faits, même si l'usage en est plus ou moins réglementé, c'est celui qui collecte l'information qui en dispose. » (Bellanger, 2014, p. 178)
>
> « Jusqu'à présent, les pouvoirs publics abordent la question des données sous l'angle du contrôle et de l'usage, cherchant à en modérer les abus par les entreprises du réseau et à garantir certains droits des utilisateurs. […] Ce sont des demis-mesures qui ne s'en prennent pas à la racine du problème : la propriété des données. Il faut désormais étendre le statut de données personnelles à l'intégralité de la trace informatique d'une personne et lui reconnaître la nature de bien incorporel dont la propriété revient à la personne concernée. » (Bellanger, 2014, p. 202)

Pierre Bellanger se montre donc en désaccord avec les dispositions juridiques inspirées par le paradigme libéral de la vie privée, et leur préfère celles proposées par l'école néolibérale. Pourtant, Tristan Nitot et lui s'accordent avec le paradigme libéral sur une théorie de la vie privée fondée sur la notion de « contrôle individuel », synonyme pour eux de « souveraineté individuelle ».

2.4.3. Critique écologiste, antiproductiviste et technocritique de l'informatique et questions de « vie privée »

Le rapporteur du RGPD, Jan Philipp Albrecht, était un eurodéputé écologiste allemand. Mais là où les arguments qu'il développe dans son livre plaidant pour une adoption rapide du RGPD s'inspirent surtout du paradigme libéral de la vie privée et n'accordent pas de place centrale aux questions écologiques (Albrecht, 2015a), il existait dans les années 1970, un courant de pensée de critique radicale antiproductiviste vis-à-vis de l'informatique.

Ainsi, la thèse d'André Vitalis, l'une des premières écrites en France sur la protection des données à caractère personnel, soutenue en 1979, a été publiée sous la forme d'un ouvrage (Vitalis, 1988 [1981]) préfacé par Jacques Ellul (Ellul, 1981), considéré comme l'une des

principales sources d'inspiration théoriques par les auteurs du mouvement politique de la Décroissance, mouvement écologiste antiproductiviste (Latouche, 2003). Arthur Miller, l'un des principaux théoriciens du paradigme libéral de la vie privée, entame et conclut son ouvrage *The Assault on Privacy* par des références à la critique du système technicien de ce même Jacques Ellul (Ellul, 1954 ; Miller, 1971). Pour ce juriste états-unien, le point de départ de la réflexion porte sur les transformations engendrées par la convergence, dans les années 1960 puis 70, entre l'industrie de l'informatique et celle des télécommunications. C'est un regard technocritique porté sur ces processus qui l'amène à s'inquiéter de la possibilité du maintien d'un droit *à la* vie privée – dont il défend une conception libérale – dans une société technicienne informatisée.

Selon André Vitalis, c'est aussi cette prise en compte de la critique du système technicien de Jacques Ellul qui aurait influencé les prises de position de la CFDT dans son engagement en faveur de la loi Informatique et Libertés en France dans les années 1970, là où la CGT, marxiste, demeurait marquée par le productivisme :

> « L'affaire SAFARI, par exemple, les syndicats […] n'étaient pas tellement contre. La CGT tout ça n'était pas tellement contre. Parce que […] la CGT [était] productiviste. Donc [dans] *Marxisme et informatique*[107], c'est de dire : […] les capitalistes ils s'en servent pour le profit, nous on s'en servira pour [le progrès]. […] Alors qu'effectivement la problématique que portait Lemoine, […] à la CFDT, [montrait] que la technologie elle-même, dans une problématique plus ellulienne, justement, […] n'est pas neutre. » (Entretien avec André Vitalis)

La période des années 1970 et 1980 a été marquée en France par l'existence d'un mouvement néo-luddite anti-informatique. Les luddites étaient des personnes qui rejetaient la mécanisation de l'industrie dans les années 1810 en Angleterre, et détruisaient les métiers à tisser. Au début des années 1980, en France, un groupe anarchiste, le CLODO (Comité libérant ou détournant les ordinateurs) organisa même des attentats contre des usines d'ordinateurs (Auteur inconnu, 1980b). La revue *Terminal*, fondée en 1980, s'inscrivait dans ce courant de pensée, et était à l'origine un magazine militant techno-critique. Son numéro 2 contenait ainsi un appel au boycott de la carte d'identité informatisée (Auteur inconnu, 1980a).

Dans *Informatique, pouvoir et libertés*, publié en 1981, André Vitalis écrivait :

> « […] l'émergence de la problématique « informatique et libertés » est tout à fait remarquable. Avant même la contestation écologiste sur le nucléaire et le débat éthique

107 Note de l'auteur : il s'agit d'une référence à l'ouvrage de Jean-Claude Quiniou (1971), discuté dans la section sur l'approche marxiste ou marxienne de ce chapitre.

sur les manipulations génétiques, cette problématique est une des premières à ouvrir une brèche dans la logique technicienne » (Vitalis, 1981, p. 313)

Dans sa préface à cet ouvrage basé sur la thèse de cet auteur, Jacques Ellul décrit l'informatique comme le fruit d'un système technicien, désencastré des besoins de la société et soumettant celle-ci à la logique de sa rationalité (Ellul, 1981, 2004 [1977]). Il y parle également des craintes de substitution de l'humain par la machine (Ellul, 1981, p. 19). Il y évoque aussi la multiplication des « informations » enregistrées par les ordinateurs :

> « Je suis informé de n'importe quoi, à tout hasard, peut-être que dans le lot quelque chose sortira. Bric-à-brac le plus extraordinaire qu'aucune société ait jamais fourni à ses membres. Mais si j'oublie 999/1000 de ces informations, l'ordinateur lui ne va rien oublier. Il est sans intérêt pour l'une ou l'autre de ces informations, il enfourne tout, et peut-être un jour, je serai heureux de les consulter. Mais le pouvoir, lui, ne le consultera pas peut-être un jour, mais chaque jour et pour tout. La royauté de l'informatique conduit à la royauté tout court. » (Ellul, 1981, p. 16)

L'ordinateur serait également selon Jacques Ellul un « prodigieux instrument d'ordre » (Ellul, 1981, p. 19) et la « mort du spécifique vivant » (Ellul, 1981, p. 20). Plus tard, les thèmes de cette critique ont été repris par d'autres auteurs, comme Bernard Stiegler, pour qui « être entièrement calculable par des algorithmes nous réduit à rien » (Stiegler et Durand, 2016). Elle semble toutefois largement absente des discours que nous avons observés dans les « disussions » sur le RGPD ou les débats sur la protection de la « vie privée » par la standardisation technique au sein du W3C.

Aujourd'hui, une part de la recherche se concentre sur l'évaluation du coût écologique du déploiement d'outils numériques d'information et de communication. En 2003, 7 % de la consommation d'électricité en Allemagne était due à l'informatique (Cremer et al., 2003). En 2014, une étude évaluait à 10 % de la consommation mondiale en électricité le poids des technologies de l'information et de la consommation, avec une progression de 7 % par an (Van Heddeghem et al., 2014). Les déchets électroniques sont également une source de préoccupation environnementale, représentant 41, 8 millions de tonnes en 2014, dont seuls 6,5 étaient pris en charge par des circuits de recyclage (Baldé, 2015). En novembre 2019, la session de la *Dyanmic Coalition on Internet Rights and Principles* s'est concentrée sur ces questions[108]. Quelques temps plus tôt, lors de la 41e réunion de l'ICDPPC à Tirana, Brad Smith, président de Microsoft, avait

108 Voir sur le programme de l'Internet Governance Forum de 2019 : https://www.intgovforum.org/multilingual/content/igf-2018-dc-internet-rights-and-principles-sustainable-futures-the-internet-human-rights-and (page consultée le 7 décembre 2019)

également évoqué l'empreinte écologique des infrastructures de communication numériques[109]. Mais ces réflexions institutionnelles sur les impacts environnementaux s'éloignent de la réflexion théorique sur le lien entre l'humain, son environnement et son milieu technique.

Plus proches des préoccupations qui pouvaient être celles de Jacques Ellul, André Vitalis ou encore Arthur Miller, de nombreux auteurs s'attachent aujourd'hui à dénoncer ce qui est pour eux un « mythe » ou une « illusion » : la dématérialisation (Bourg, 2007 ; Dias, 2007 ; Flipo, 2007 ; Flipo, Dobré et Michot, 2013). Pour eux, l'image d'un « cyberespace » indépendant, fait de pures « données », « dématérialisées », que promeuvent les utopies de la Silicon Valley décrites par Fred Turner (2008), a pour fonction de masquer les impacts tout à fait matériels des outils informatiques sur l'environnement. Face à cela, ils cherchent à rappeler ce qu'ils considèrent comme étant des « limites » à la croissance (Latouche, 2012), constituées par les limites de la capacité de reproduction des ressources naturelles exploitées pour faire fonctionner l'infrastructure informatique (Flipo, Dobré et Michot, 2013). La négligence de ces limites pourrait entraîner des catastrophes irréversibles qui entraînerait un « effondrement » de la société (Cochet, 2017).

Les auteurs se réclamant du courant de pensée décroissant réfutent toutefois, en général, l'étiquette de « technophobie » (Dias, 2007, p. 31). S'appuyant sur des réflexions antérieures sur le rapport entre objets techniques et éthique (Jonas, 1982 ; Mumford, 1964 ; voir aussi : Lavelle, 2009), et reprenant un concept d'Ivan Illich (Illich, 2014 [1973]) ils prônent le passage à une technique « conviviale », caractérisée selon Mathilde Szuba par « l'autonomie et la décentralisation politique » (Szuba, 2017, p. 96).

Ce raisonnement avait déjà été appliqué à l'informatique par les contributeurs à la revue *Terminal* des années 1980. Dans un numéro de *Terminal* de 1984, Mike McCullough passe en revue une liste de projets contre-culturels de la micro-informatique aux États-Unis, qu'il désigne sous le terme d'« informatique alternative » (McCullough, 1984). Dans le même numéro, Guy Lacroix opposait « informatique dure » à « informatique molle » (Lacroix, 1984), dans un parallélisme qui n'est pas sans rappeler la distinction que Richard Stallman opère entre les systèmes « privatifs » – au code source verrouillé, hors du contrôle de l'utilisateur – et « libres » – au code source ouvert, modifiable par quiconque a les compétences requises dans le langage de programmation pertinent (Broca, 2013). Nous trouvons aussi dans ce numéro le manifeste d'une association, le Centre associatif pour une informatique différente (CAID), qui énonce :

> « La technologie informatique actuelle est rigide et orientée par les constructeurs d'ordinateurs ; c'est une informatique « dure ». Un des objectifs du CAID est de rechercher les bases théoriques d'une informatique nouvelle, « molle », qui donnerait les

109 Voir la vidéo de son intervention mise en ligne par l'autorité albanaise de protection des données sur Youtube : https://www.youtube.com/watch?v=g_0k5vwxN0k (page consultée le 7 décembre 2019)

> possibilités de réaliser des systèmes adaptables par les utilisateurs. » (Centre associatif pour une informatique différente (CAID), 1984)

Les articles des années 1980 de la revue *Terminal* ne liaient toutefois pas encore la question de la technologie « conviviale », « décentralisée », aux questions écologiques. Entre temps, les deux questions se sont liées dans la théorie politique décroissante. Pour Mathilde Szuba, par exemple, le développement d'un projet technologique « convivial » est une façon de parvenir à atteindre les objectifs de décroissance de la consommation énergétique qu'elle juge indispensable à la survie écologique de la planète (Szuba, 2017). De cette façon, la théorie antiproductiviste radicale propose de lier des objectifs politiques, de liberté et de démocratie technique qui nous libérerait du « système technicien » décrit par Jacques Ellul, tout en répondant au besoin d'adaptation de nos outils techniques à la réalité de la crise écologique.

Le thème du droit *à la* vie privée et des données à caractère personnel, très présent dans la revue *Terminal* dans les années 1980, n'est aujourd'hui plus vraiment étudié par le courant décroissant (Rossi, 2016). Cela peut contribuer à expliquer son absence de nos corpus de documents, que ce soit dans les « discussions » sur le RGPD ou dans les groupes de standardisation techno-politique qui, au sein du W3C, s'intéressent à la protection de la vie privée. Il est donc difficile de dire ce que serait une perspective « décroissante » contemporaine sur le droit *à la* protection des données à caractère personnel, sinon de dire que la nature et la configuration du milieu technique dans lequel ce droit est amené à s'exercer est déterminant.

Quant aux auteurs de la revue *Terminal* des années 1980, leur vision semblait rejoindre au moins en grande partie celle du paradigme libéral de la vie privée, mettant l'accent sur des logiques de contrôle de la circulation de l'information et d'idéal d'autonomie. Ainsi, en 1983, un éditorial de la revue *Terminal* s'exprimait ainsi à propos de la contestation du recensement informatisé en RFA qui a abouti à la décision de la Cour constitutionnelle fédérale reconnaissant le droit à l'auto-détermination informationnelle[110] :

> « Non ! Les données n'appartiennent ni à l'État, ni aux administrations, c'est aux utilisateurs et aux collectivités concernées, avec l'accord explicite des personnes membres de ces groupes, de construire leurs propres données selon la logique de leurs besoins. Les technocrates, aménageurs et planificateurs du bonheur collectif, prétendent se saisir de soi-disant besoins sociaux pour rationaliser leur mode de gouvernement des hommes et des groupes : mais comme le montre le boycott du recensement en RFA […] la mobilisation politique ne se fait pas pour plus de rationalité, mais pour plus de liberté et d'autonomie, pour la défense du droit à notre propre intimité et à notre identité, pour le

110 Décision du Tribunal constitutionnel fédéral allemand BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil)

droit à contrôler la définition et l'usage des informations nous concernant. » (Auteur inconnu, 1983)

Quant à Arthur Miller, si sa réflexion sur les ordinateurs et leur rôle politique avait pour point de départ une critique elluliste du système technicien, ses convictions sur le droit à la « vie privée » sont, comme nous l'avions déjà vu, celles du paradigme libéral.

En conclusion, les théories politiques écologistes antiproductivistes et technocritiques contemporaines se fondent sur des réflexions d'auteurs comme Jacques Ellul et Ivan Illich qui ont également inspiré, en France, des auteurs ayant publié dans la revue *Terminal*, parmi lesquels André Vitalis, qui y publiait sous un nom de plume, et qui, proche de défenseurs de la vie privée comme Louis Joinet, Marie Georges et Philippe Lemoine – sur lesquels nous reviendrons dans le chapitre suivant – allait travailler pour la CNIL à la fin des années 1980. Une partie des auteurs d'articles pour la revue *Terminal*, comme Yves Cochet ou Serge Latouche, ont contribué à fonder un mouvement politique écologiste radical inspiré de l'ensemble de ces réflexions. Si la question des données à caractère personnel s'est effacée des discours produits par ces acteurs au cours des décennies suivantes, la volonté de transformer la société par la transformation d'un milieu technique qui devrait devenir « convivial » a survécu. Cette « convivialité » serait la promesse d'une technologie respectueuse des limites naturelles à la production. Elle était la garantie, dans des écrits des années 1980, des libertés décrites comme menacées par l'informatique centralisée. Cette garantie devait être le complément nécessaire, selon ces auteurs, au droit à l'auto-détermination informationnelle inspiré du paradigme libéral de la vie privée, au nom des libertés individuelles et d'aspirations à l'autonomie.

2.5. Conclusion du chapitre

Nous voyons donc que ni la valeur, ni le contenu du droit *à la* vie privée ne font consensus. Le paradigme libéral de la vie privée, par lequel nous avons commencé notre exploration, a fait l'objet de nombreuses critiques, par de nombreux courants différents. Le débat porte sur la nature du droit *à la* vie privée : contrôle individuel sur la circulation d'informations sur soi, ou bien protection de la frontière protégeant un espace privé borné par des normes sociales et collectives de l'œil d'autrui ? Catégorie cohérente ou ensemble incohérent de droits déjà protégés, comme par exemple par le droit à la propriété ? Il porte aussi sur sa désirabilité, certains auteurs néolibéraux ou féministes considérant la reconnaissance d'un tel droit comme étant « nuisible ». De nombreux autres points de controverse théorique ont été développés sur lesquels il serait long de revenir.

Ce bref panorama de différentes façons de penser le droit *à la* vie privée et le droit *à la* protection des données à caractère personnel, qu'il est généralement difficile de distinguer dans les discours présentés, a été nourri par des lectures de sources publiques effectuées avant de partir sur le terrain, puis alimenté progressivement lorsque des références théoriques évoquées dans des discours d'acteurs nous ont amené à aller les étudier de plus près. Il n'a donc pas de prétention à l'exhaustivité, mais servira de clef de lecture pour comprendre et interpréter les références que les acteurs des terrains étudiés y font dans les discours que nous avons analysés. L'une des questions auxquelles nous nous efforcerons de répondre sera de voir laquelle ou lesquelles des conceptions théoriques décrites dans ce chapitre peuvent expliquer les choix rédactionnels des dispositions de la Convention 108 du Conseil de l'Europe et des Lignes directrices de l'OCDE de 1980[111], du RGPD[112], des documents normatifs sur la vie privée produits par le W3C, l'organisme de standardisation du Web[113], puis de la définition de la « donnée à caractère personnel » qui s'est imposée de façon transversale à ces trois terrains[114].

111 Cf. chapitre 3
112 Cf. chapitre 4
113 Cf. chapitre 5
114 Cf. chapitre 6

Chapitre 3 : La généalogie du droit à la protection des données à caractère personnel

3.1. Introduction

Qu'est-ce que la protection des données à caractère personnel ?

Une des manières de répondre à cette question est de s'intéresser à l'origine de la formule « protection des données », et à la façon dont la mise sur support numérique d'informations sur des personnes physiques a été transformée en un problème public, auquel cette formule fait indirectement référence en désignant un ensemble de mesures censées y répondre. Ce faisant, nous étudierons les premières étapes de la spécialisation d'acteurs et d'institutions constituant progressivement un nouveau secteur de l'action publique, en charge de sa gestion. En particulier, en gardant en tête notre deuxième hypothèse, nous chercherons à voir ce que fut le rôle de l'ordinateur et des imaginaires sociaux autour de l'ordinateur, combiné à des conceptions relatives à la « vie privée » exposées dans le chapitre précédent, dans la façon dont ce nouveau problème public fut cadré et mis à l'agenda administratif et politique.

Les premières lois réglementant l'usage informatisé d'informations sur des personnes pour protéger le droit *à la* vie privée datent des années 1970. Comme nous le verrons, ces lois ont de nombreux points communs, qui s'expliquent par le fait qu'elles ont été rédigées par un réseau d'acteurs, souvent des universitaires et des hauts-fonctionnaires, qui échangeaient régulièrement des informations et des idées et se rencontraient lors de réunions sous l'égide d'organisations intergouvernementales.

L'*Advocacy Coalition Framework* (ACF) est utilisé pour étudier la relation entre coalitions de cause fondées sur une rivalité de systèmes de convictions dans des sous-systèmes de politique publique qui ont déjà un degré de maturité et de stabilité, que Paul Sabatier estime à dix ans d'existence (Sabatier, 1993). Pour la part de nos recherches qui ont concerné l'émergence de la protection des données, nous nous sommes donc attaché à compléter le cadre méthodologique de l'ACF par une généalogie des politiques publiques de protection des données.

La démarche généalogique fut utilisée par Michel Foucault pour « problématiser » des pratiques ou des connaissances, comme le biopouvoir ou la sexualité (Foucault, 1975, 1976). Selon l'analyse qu'en fait Colin Koopman, la problématisation foucaldienne est une mise en lumière de ce qui doit « attirer notre attention sérieuse[1] » (Koopman, 2013, p. 90). La méthode

1 Traduction de libre de « demand our serious attention ».

généalogique est ainsi une histoire du présent : elle ne cherche pas à raconter le passé mais à opérer un diagnostique du présent.

La méthode généalogique s'est développée, chez Michel Foucault, à partir de sa méthode d'archéologie des savoirs, qui consistait à enquêter sur le moment de discontinuité temporelle où une connaissance est apparue, afin d'en problématiser l'apparition (Foucault, 2008 [1969]). La méthode généalogique, selon Colin Koopman, a étendu le champ de l'investigation de l'archéologie au-delà des connaissances, aux pratiques (Koopman, 2013, p. 31).

Comme notre recherche s'est concentrée sur l'émergence de connaissances, de croyances et de discours sur la vie privée, le droit *à la* vie privée, l'ordinateur et l'informatique, nous pourrions dire que nous nous contentons d'une approche archéologique. Nous avons en effet voulu comprendre comment est née la formule de « protection des données », avec elle, la catégorie juridique du droit *à la* protection des données à caractère personnel, et les savoirs qui y sont associés.

Si cette formule a circulé et a été traduite dans différentes langues (González Fuster, 2014a), elle est d'abord née dans un contexte social, historique et culturel singulier. Des idées, savoirs, des valeurs et des discours de légitimation spécifiques y sont associés, qui parfois ont été oubliés ou, dans d'autres cas, passent pour évidents voire naturels et ne sont plus explicités.

Toutefois, comme, en politique et en droit, la parole et le discours sont des actes[2], les savoirs et les connaissances sur la « protection des données », qui ont émergé dans un contexte particulier, sont aussi des pratiques discursives qui visent à agir, à modifier l'ordre juridique et, par l'ordre juridique, certaines pratiques sociales ainsi que, dans le cas de l'informatique, la configuration de matérialités techniques. La ligne de division entre discours et pratique étant floue en matière d'action publique, nous ne reprendrons donc pas à notre compte, dans le cadre de l'étude présentée dans ce chapitre de thèse, la distinction entre archéologie et généalogie présente chez Michel Foucault et soulignée par l'analyse que Colin Koopman fait de l'œuvre de ce dernier. Nous emploierons les deux termes de façon indifférenciée.

Concrètement, faire une généalogie des politiques publiques de protection des données à caractère personnel, et du droit *à la* protection des données à caractère personnel, n'a pas été simple. De façon courante, l'histoire de la protection des données est présentée comme ayant pris naissance dans les années 1970 et 1980, lorsque les gouvernements ont commencé à vouloir mettre en place des identifiants informatiques uniques pour cataloguer la population. En France, l'histoire de la protection des données est généralement présentée comme étant la conséquence de réactions politiques à un article que Philippe Boucher (1974) a publié dans *Le Monde* en 1974 : « Safari ou la chasse aux Français », dans lequel il dénonçait un projet d'interconnexion de plusieurs répertoires de données personnelles détenus par l'État à l'aide du numéro d'inscription au registre, connu sous le nom de numéro de sécurité sociale. Pour l'Allemagne, le point de départ du droit à l'auto-détermination informationnelle le plus souvent retenu est une décision de

2 Cf. paragraphe « Le droit saisi par une approche communicationnelle » dans l'Introduction générale.

1983 de la Cour constitutionnelle fédérale[3], adoptée dans le cadre d'un recours contre une loi de recensement de la population.

Le récit de la nomogenèse[4] du droit *de la* protection des données est donc le suivant : l'informatique aurait entraîné des usages à des fins de surveillance, qui auraient été dénoncés dans l'espace public médiatique, entraînant des réactions politiques et judiciaires aboutissant mécaniquement, logiquement et rationnellement à l'adoption de ces règles de droit. Cette chronologie, qui fonde le récit des origines des autorités de protection des données en Europe occidentale, ne résiste pourtant pas à un examen méticuleux.

Ayant travaillé comme stagiaire auprès des autorités hongroise puis française de protection des données, avant la thèse, et fréquenté comme membre les professionnels français de la protection des données de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP), c'est bien cette narration que j'y avais retenue[5]. Elle correspondait aux schémas d'analyse que j'avais acquis, en cours de science politique à l'Institut d'études politiques de Lille, qui faisaient la part belle aux approches séquentielles des politiques publiques selon lesquelles la prise de décision est toujours précédée d'une mise à l'agenda conçue comme médiatique et consécutive à un mouvement social. Pourtant, alors que j'écrivais mon mémoire de Master sur les autorités de protection des données (Rossi, 2013), j'avais découvert par hasard, prenant la poussière sur la bibliothèque de mes grands-parents, un fascicule édité par le Conseil d'État qui contenait un rapport, daté 1970, et qui parlait déjà, plusieurs années avant l'affaire Safari, de protection des libertés individuelles face au développement de l'informatique et à la numérisation des banques de données personnelles de l'État. Comment expliquer ce qui, selon la narration répandue sur l'origine des lois de protection des données à laquelle j'avais été socialisé, apparaissait comme une incohérence chronologique manifeste ? Si ce n'était pas l'affaire Safari qui avait conduit mécaniquement à l'adoption de la loi Informatique et Libertés, comme réponse à une problème et à un mouvement social ayant émergé à cette occasion, qu'est-ce qui a fait que des gens – y compris au Conseil d'État – se soient interrogés sur la meilleure façon de réguler l'usage de l'informatique afin qu'il ne mette pas en péril le droit à la vie privée ? Cela paraît d'autant plus mystérieux qu'il s'agit d'une époque où les ordinateurs étaient rares et inaccessibles pour le commun de la population et qu'Internet n'était encore qu'un rêve dans l'esprit de quelques informaticiens.

Peu de travaux ont été publiés sur l'histoire de la protection des données, et parmi ceux-ci, la plupart ne racontent pas la période qui a précédé la moitié des années 1970[6]. Étant donné l'existence d'une littérature plus abondante sur l'histoire du droit *des* données à caractère

3 Décision du Tribunal constitutionnel fédéral allemand BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil).

4 Genèse, généalogie, d'une règle de droit. Terme emprunté à Jean Carbonnier (2001).

5 Le pronom personnel « je », plus personnel, a été retenu parce que préférable pour parler des expériences personnelles ayant influencé le point de départ de la recherche.

6 Parmi ceux qui existent, voir : Bennett, 1992 ; Flaherty, 1989 ; González Fuster, 2014 ; Newman, 2008 ; Rule et Greenleaf, 2010 ; Sziklay, 2011 ; Vitalis, 2009.

personnel après 1980, j'ai choisi de borner chronologiquement mon étude en commençant par l'émergence des premiers discours sur les « dangers » de l'informatique pour le droit *à la* vie privée, au milieu des années 1960, et en m'arrêtant à l'adoption de deux textes : les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de 1980, et le premier traité international de protection des données : la Convention 108 du Conseil de l'Europe de 1981.

Nous chercherons à identifier les co-rédacteurs de ces textes ainsi que les systèmes de conviction, imaginaires sur l'informatique et conceptions sur la « vie privée » auxquels leurs discours ont fait référence pour justifier et légitimer leurs propositions de mesures concrètes devant constituer le droit *de la* « protection des données ». Nous étudierons à ce titre les discours d'opposition auxquels la communauté transnationale ayant porté à l'agenda politique le problème public qu'elle voulait traiter par l'invention de ce nouveau corpus de règles de droit a été confrontée. Nous nous interrogerons aussi sur les stratégies argumentatives qui ont permis à cette coalition d'articuler leur référentiel au référentiel global alors en place au Conseil de l'Europe, de l'OCDE.

Comme annoncé dans l'introduction, notre recherche a porté sur le terrain des groupes d'experts où ont été rédigées les premières versions de ces textes avant leur adoption formelle. Toutefois, pour comprendre comment s'est construite l'image de l'ordinateur comme danger pour la « vie privée », il est nécessaire de s'intéresser à ce qui s'est passé dans les années 1960 aux États-Unis d'Amérique. C'est en effet là-bas que furent publiés les premiers travaux sur le sujet, et que des institutions, comme la Chambre des Représentants, s'y intéressèrent en premier. De plus, que ce soit dans les entretiens qui ont été réalisés avec des anciens membres des groupes d'experts de l'OCDE et du Conseil de l'Europe, ou dans les documents d'archives que nous avons trouvés, il est souvent fait référence à ces travaux américains. La compréhension de la construction en Europe, dans les années 1970, de la « protection des données » comme formule désignant un projet de règles de droit devant encadrer une informatique perçue comme dangereuse pour une certaine conception de la « vie privée » ne peut donc se passer d'une exploration de ces travaux conduits outre-Atlantique pendant la décennie antérieure.

3.2. Le retour à l'agenda du droit *à la* vie privée aux États-Unis dans les années 1960

3.2.1. L'échec des premières tentatives de faire reconnaître le droit *à la* vie privée au début du XX^{e} siècle

La théorisation, en doctrine juridique, d'un droit fondamental *cohérent* à la « vie privée », en tant que nouvelle catégorie de droit, remonte au XIX^{e} siècle. Si, en France, l'expression « vie privée » se trouve dans quelques textes de la fin du XVIII^{e} et du milieu du XIX^{e} siècle, notamment en matière de droit de la presse, c'est d'abord aux États-Unis que cette notion a connu une théorisation doctrinale (Halpérin, 2005). À cette époque, l'essor des techniques de la presse de masse et de la photographie est perçu comme une menace envers le sanctuaire du domicile par une partie de l'élite bourgeoise (Glancy, 1979) :

> « La photographie instantanée et l'entreprise de la presse ont envahi l'enceinte sacrée de la vie privée et domestique ; et nombre d'objets mécaniques menacent de donner raison à la prédiction selon laquelle : « ce qui est chuchoté dans le placard sera proclamé sur les toits[7] » »(Warren et Brandeis, 1890, p. 195)

Comme nous l'avons vu dans le chapitre précédent, les auteurs de la citation ci-dessus ont été les premiers à proposer la reconnaissance d'un droit *à la* vie privée, défini comme un « droit à être laissé tranquille » (« *right to be let alone* »), dans dans cet article publié en 1890 *Harvard Law Review* (voir : Glancy, 1979 ; González Fuster, 2014).

Leur principal apport a été de proposer pour la première fois une vision cohérente (DeCew, 2018) de la vie privée, dans le sens où leur notion de droit à la vie privée regroupe dans une catégorie juridique nouvelle un ensemble épars de droits comme le droit au secret des correspondances, certains éléments du droit de la propriété ou encore certaines garanties déjà protégées à un niveau constitutionnel aux États-Unis au moment où ils écrivent, comme la protection du domicile prévue dans le IV^{e} amendement de la Constitution (Glancy, 1979).

Louis Brandeis devint juge à la Cour Suprême des États-Unis d'Amérique en 1916, où il milita en faveur d'une reconnaissance constitutionnelle, au niveau fédéral, de ce droit à la vie privée dont il avait exposé la teneur dans son article avec Samuel Warren. Ce ne fut cependant

7 Traduction de l'auteur. Texte original : « Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life ; and numerous mechanical devices threaten to make good the prediction that : "what is whispered in the closet shall be proclaimed from the house-tops". »

pas une chose aisée, malgré l'adoption, au niveau de certains États, de lois instaurant une protection juridique de ce concept nouveau de droit *à la* vie privée[8]. Le 4 juin 1928, la Cour Suprême refusa de reconnaître le droit *à la* vie privée et de considérer comme contraire aux libertés constitutionnelles le fait que des policiers aient obtenu des preuves contre des personnes ayant enfreint la Prohibition en écoutant leurs lignes téléphoniques sans mandat d'un juge (Cour Suprême des Etats-Unis d'Amérique, 4 juin 1928, *Olmstead contre Etats-Unis*, 277 U.S. 438). Louis Brandeis, toujours juge à la Cour suprême à ce moment-là, publia son désaccord dans un avis divergent (« *dissenting opinion* ») où il argumenta que la finalité du quatrième amendement, qui protège le domicile contre les perquisitions sans mandat, et le cinquième amendement, qui interdit d'obliger quelqu'un à témoigner contre lui-même, avaient tous deux pour but implicite de protéger la vie privée des citoyens, dans le contexte des techniques disponibles à l'époque pour l'enfreindre. Or, poursuivait-il, les évolutions techniques, qui permettaient désormais notamment de procéder à des écoutes téléphoniques, renforcent la pression exercée contre « le sanctuaire du domicile d'un homme et de l'intimité de la vie » (« *the sanctities of a man's home and the privacies of life* ») (Brandeis, 1928, p. 473). À l'instar de ce que suggère notre seconde hypothèse – comme avant pour la photographie instantanée, et plus tard, chez d'autres auteurs, l'ordinateur – ce sont des transformations dans le milieu technique qui, perçues d'une certaine façon, lui ont donné un argument en faveur d'une évolution juridique dans la reconnaissance du droit *à la* vie privée. Mais cette fois-ci, son argumentation échoua.

3.2.2. La reconnaissance du droit *à la* vie privée à la fin du McCarthyisme

En 1948, l'adoption de la Déclaration universelle des droits de l'Homme allait, avec son article 12, proclamer l'existence d'un droit *à la* vie privée au niveau international. Mais cela ne s'est pas traduit pour autant par une reconnaissance de ce droit dans les ordres juridiques internes des États signataires.

Il fallut attendre finalement les années 1960 pour voir la Cour Suprême des États-Unis d'Amérique reconnaître un droit constitutionnel à la vie privée, bien des années après la mort du juge Brandeis, dans une série de trois jugements qui ont renversé la jurisprudence précédente. Tout d'abord, dans *Griswold contre Connecticut* (Cour Suprême des États-Unis, 1965, 318 US 479), elle reconnut l'existence d'un droit constitutionnel à la vie privée « dans la pénombre » (*in penumbra*) des droits explicitement reconnus par la constitution fédérale et le *Bill of Rights*. Puis, en 1967, dans *Katz contre États-Unis* (Cour Suprême des États-Unis, 1967, 389 US 347), elle revint sur sa décision *Olmstead contre États-Unis* de 1928 en reconnaissant qu'une écoute téléphonique constitue une atteinte au droit à la vie privée. Enfin, en 1977, dans *Whalen contre*

8 Nous pouvons relever, à titre d'exemple, la création d'un délit d'invasion de la vie privée en 1903 par le New York Civil Rights Act de 1903 (N.Y. Civ. Rights Act 1903, § 51).

Roe (Cour Suprême des États-Unis, 1977, 429 US 589), elle reconnut l'existence d'un droit à la vie privée informationnelle, c'est-à-dire le fait que le droit à la vie privée implique de placer certaines restrictions à la libre-circulation des informations concernant la vie privée des citoyens[9].

Ce regain d'intérêt pour le droit *à la* vie privée dans les années 1960 aux États-Unis d'Amérique, et le succès posthume des arguments de Louis Brandeis et Samuel Warren en faveur de sa reconnaissance au niveau constitutionnel, s'expliquent par deux facteurs. Le premier est qu'il est intervenu à la sortie de la période du McCarthyisme. Le second est l'existence d'un imaginaire présentant l'ordinateur comme une menace, notamment pour une protection déjà très éprouvée de la vie privée, et qui était alors très répandue dans le cinéma, dans la littérature, mais aussi, nous le verrons, dans de nombreux discours médiatiques comme institutionnels.

À partir des années 1940, la Seconde guerre mondiale puis la Guerre froide ont contribué à la mise en œuvre technique et institutionnelle d'une surveillance de masse, en Union soviétique et dans ses pays satellites du futur Pacte de Varsovie, mais aussi aux États-Unis et chez nombre de ses alliés de ce qui allait devenir l'Organisation du traité de l'Atlantique nord (OTAN). Le rapport des services de renseignement à l'action se transforme. Alors qu'à l'origine, les services de renseignement sont perçus, en tout cas aux États-Unis d'Amérique, comme illégitimes dans une société démocratique, et ne devant qu'aider à préparer la guerre, sans jamais que les savoirs produits ne servent directement à l'action en temps de paix (Rios-Bordes, 2018), la Guerre Froide brouille la limite entre temps de guerre et temps de paix. Le thème de la sécurité intérieure prend de l'ampleur, et un couplage progressif des savoirs produits par les services de renseignement s'opère avec l'action exercée par les militaires, la police et la justice.

Une véritable chasse aux communistes est mise en place aux États-Unis, notamment sous l'influence du sénateur Joseph McCarthy. L'*Executive Order* 9835 du 21 mars 1947, signé par le président Harry Truman, impose la vérification de la « loyauté » de tous les employés civils de l'Etat fédéral. Entre autres critères de « déloyauté » figurait toute forme d'association à une organisation « totalitaire, fasciste, communiste ou subversive » (Executive Order 9835, cité par : Goldstein, 2006). Ces organisations étaient énumérées dans une *Attorney General's List of Subversive Organizations* (AGLOSO), qui existait en secret depuis le début des années 1940 sur la base d'une loi adoptée dès 1939 (Goldstein, 2006). Cette liste fut adoptée par de nombreuses entreprises privées comme une liste noire dont les membres ne devaient pas être embauchés.

En 1950, le *Subversive Activities Control Act of 1950* établit un *Subversive Activities Control Board* chargé d'enquêter sur les organisations et les personnes suspectées d'être « fascistes » ou « communistes ». En 1952, la Cour suprême valida une loi de l'État de New-York

9 Notons qu'au niveau étatique, il fallut attendre 1998 pour que le Minnesota, dernier des États des États-Unis à ne pas l'avoir alors encore fait, reconnaisse l'existence d'un droit *à la* vie privée (Lake v. Wall-Mart Stores, Inc. 582 N.W. 2d. 231 (Minn 1998)).

permettant de licencier les enseignants « subversifs » (Adler v. Board of Education of New York, 1952). La nomination de deux juges, Earl Warren et William Brennan Jr. en 1953 modifia cependant le rapport de force au sein de la Cour Suprême, et dès 1956, une décision vint renverser celle de 1952 (Slochower v. Board of Education, 1956). En 1958, une autre décision vint interdire au Département d'État (*State Department*) de décider de façon arbitraire d'attribuer ou non un passeport à un citoyen en fonction de ses opinions politiques réelles ou supposées (Kent v. Dulles, 1958).

Le McCarthyisme en tant que tel déclina donc fortement dès le milieu des années 1950, même si cela n'a pas empêché le FBI de mener d'autres opérations visant à déstabiliser, parfois illégalement, des organisations politiques jugées « dissidentes »[10].

Entre les années 50 et 70, de nombreuses techniques de surveillance, mises en œuvre tant par des organismes publics que par des entreprises privées, ont été expérimentées et déployées : vidéosurveillance, écoutes téléphoniques, invention de « détecteurs de mensonge », obligations de répondre à des questionnaires intrusifs, mise en place d'un marché de cotes de crédit sur la solvabilité des débiteurs, mais aussi de fichiers d'informations sur les habitudes de consommation, l'orientation sexuelle ou encore les antécédents de santé… Les employeurs, en particulier, se montrèrent friands d'accéder à ces informations (Packard, 1965).

C'est dans ce contexte de l'après McCarthyisme que William Prosser contribua au droit états-unien *de la* vie privée en proposant une taxonomie des délits coutumiers (*torts*) qui touchent au droit *à la* vie privée (Prosser, 1960 ; Richards et Solove, 2010) : l'intrusion dans l'espace privé (« *intrusion upon the plaintiff's seclusion or solitude* »), la publication de faits embarrassants qui relèvent de l'intimité de la personne (« *public disclosure of embarrassing private facts* »), la diffamation (« *publicity which places the plaintiff in a false light in the public eye* ») et l'usurpation d'identité (« *appropriation […] of the plaintiff's name or likeness* ») (Prosser, 1960, p. 389 cité par Richards et Solove, 2010, p. 1889-1890). Si cette classification a été critiquée pour son absence de prise en compte de la dimension informationnelle du droit à la vie privée (Richards et Solove, 2010), l'irruption de l'informatique, combinée à l'imaginaire social se rattachant aux ordinateurs, allait mettre à l'agenda la question de la vie privée informationnelle aux États-Unis à partir du milieu des années 1960.

10 Par exemple, le programme COINTELPRO en est un exemple criant. Les personnes sous surveillance étaient harcelées, par exemple par les services fiscaux, afin de pouvoir les incriminer pour des délits réels. Des campagnes de diffamation étaient également menées dans les médias. Ce programme fut mis en place en 1956 en réaction à la limitation des opérations légales menées sous l'ère du McCarthyisme, et ne fut démantelé qu'à la suite de sa révélation en 1971 (Church et Tower, 1976).

3.2.3. L’ordinateur dans l’imaginaire social des années 1960 : une figure inquiétante du complexe militaro-industriel de la Guerre froide

À ce stade, il est important de rappeler que l’imaginaire social entourant la figure de l’ordinateur n’était pas encore celui qui, inspiré des utopies californiennes des années 1970, marque aujourd’hui le débat public actuel sur Internet et les technologies de l’information en général (Morozov, 2015 ; Tréguer, 2019). Comme le rappelle Fred Turner en propos liminaire de son livre sur les utopies de la Silicon Valley, l’imaginaire collectif prédominant, surtout dans les milieux contestataires mais aussi au-delà, voit en l’ordinateur quelque chose de dangereux, un produit du complexe militaro-industriel de la Guerre froide :

> « Pour les étudiants du *Free Speech Movement* (Mouvement pour la liberté d'expression), le rôle de l'université en tant que producteur de connaissances ne pouvait être distingué de son engagement politique en période de guerre froide. De plus, cette imbrication menaçait nombre de personnes, sur un plan très personnel. Pour les contestataires, l'université était à la fois une usine à savoir en elle-même, et un microcosme du complexe militaro-industriel rigide et hautement rationalisé qu'elle servait. Dans ce sens, l'université modélisait le monde hiérarchisé de l' « adulte entreprenant dans la guerre froide », et nombre de jeunes s'inquiétaient d'être formés à ce rôle. Et à l'époque, aucune machine ne représentait aussi communément que l'ordinateur cet ordre social stratifié et dépersonnalisé[11]. » (Turner, 2008, p. 12)

Il cite à titre d’illustration Hal Draper, bibliothécaire à l'université Berkeley, expliquant en 1964 que : « *the mass university of today is an empowering, over-towering, impersonal, alien machine in which [the student] is nothing but a cog going through pre-programmed motions – the IBM syndrome*[12] » (Draper, 1965, p. 153, cité par Turner, 2008, p. 12). Les ordinateurs personnels, par exemple ceux inventés par des membres du *Homebrew Computer Club* dans les années 1970 afin de faire de cette technologie de masse un outil individuel d'émancipation informationnelle (Turner, 2008), n'existaient pas encore. L’image de l’ordinateur était encore celle de puissants calculateurs, physiquement massifs, comme nous le montre l’image ci-

11 Traduit de l’anglais. Texte original : « For the students of the Free Speech Movement, the university's role as knowledge producer could not be separated from its engagement with cold war politics. Moreover, the entanglement threatened many at a deeply personal level. To the protestors, the university was both a knowledge factory in its own right and a microcosm of the rigid, highly rationalized military-industrial complex it served. In that sense it modeled the hierarchical wold of cold war croporate adulthood for which many feared they were being trained. And at the time, no machine more commonly represented this stratified, depersonalized social order than the computer. »

12 Traduction : « L'université de masse d'aujourd'hui est une machine empouvoirante (empowering), étrangère, dominante, dans laquelle [l'étudiant] est un simple rouage suivant des mouvements programmés. C'est le syndrome IBM. »

dessous ; et dans une bonne partie de la littérature de science-fiction, cette image perdura jusqu'aux années 1980[13].

Figure 10 : *La console d'un IBM System/360, ordinateur mis sur le marché en 1965*[14].

Il serait certainement à la fois utile et passionnant d'étudier dans le détail la façon dont s'est forgée dans les arts, entre les années 1940 et la fin des années 1960, l'image d'un ordinateur menaçant, bureaucratique au potentiel totalitaire, de la même façon que Fred Turner s'est employé à étudier le phénomène qui s'est développé à partir des années 1970 et qui, autour notamment du *Whole Earth Review* et de *Wired*, a popularisé l'image concurrente de l'ordinateur individuel émancipateur. Ce travail n'est pas l'objet de notre thèse, mais nous devons cependant garder ces éléments à l'esprit pour nous rappeler que l'informatique n'a pas toujours et partout bénéficié d'une image positive dans l'espace public. Or, confortant notre seconde hypothèse, nous verrons que l'image d'un ordinateur au mieux ambivalent et inquiétant, issu de la science-fiction, a eu un effet direct sur la façon dont la discussion sur le rapport entre informatique et protection de la vie privée a été cadrée aux États-Unis, puis plus tard en Europe, dans les années 1960, y compris dans des arènes institutionnelles officielles comme le Congrès des États-Unis (US House of Representatives, 1966). Commençons par un bref aperçu de l'image de l'ordinateur dans la

13 Ainsi, encore dans *Terre et Fondation* d'Isaac Asimov (1986), l'univers entier est contrôlé par un robot qui, bien que respectant des règles l'empêchant de nuire à des humains, n'en est pas moins menaçant et inquiétant.

14 Crédits photo : *Bundesarchiv*, B 145 Bild-F038812-0014 / Schaack, Lothar / sous licence CC-BY-SA 3.0.

science fiction de l'époque, puis voyons comment il y est fait référence dans les discours institutionnels.

L'une des principales métaphores de l'ordinateur est, à cette époque, le télécran du roman dystopique de George Orwell (1949), *1984*. Nous avons retrouvé des références à ce roman dans de nombreux documents de notre corpus couvrant la période de 1965 à 1975. Cette machine, une télévision impossible à éteindre complètement, sert aussi de mouchard, et est, dans le roman d'Orwell, installée dans toutes les pièces de tous les bâtiments, de sorte à former un dispositif ubiquitaire et omniscient de surveillance totalitaire. Cet univers a longtemps été associé avec l'image de l'entreprise IBM, qui était devenue le symbole d'une techno-science froide, lointaine, bureaucratique et menaçante.

Une autre représentation de l'ordinateur nous est fournie par le film *2001, l'Odyssée de l'espace*, de Stanley Kubrick, sorti en 1968. Cet ordinateur est une figure anxiogène, qui sait beaucoup de chose sur l'équipage d'un vaisseau spatial, jusqu'à être en mesure de prendre le contrôle sur celui-ci. Le nom de cet ordinateur, HAL 9000, est une référence directe à la compagnie IBM, les lettres H, A et L précédent les lettres I, B et M dans l'alphabet.

Dans *Star Trek*, série originale, saison 2, épisode 26, diffusé en 1968, l'un des personnages est un ordinateur. L'agent Gary Seven, le protagoniste principal, doit, dans un épisode qui se joue à l'époque de la Guerre Froide, empêcher une guerre mondiale nucléaire. Pour mener à bien sa mission, il dispose d'un ordinateur caché dans son appartement. Cet ordinateur, qui fait la taille d'un mur et qui n'affiche rien d'intelligible à l'écran sauf dans une courte scène vers la fin de l'épisode, est doté de la parole et paraît omniscient : il est capable de repérer les autres agents où qu'ils soient et de suivre l'état d'avancement de leurs missions, d'intercepter toutes les communications sur Terre, mais aussi de suivre le lancement de missiles nucléaires, et d'identifier des individus par leur nom. Une scène en particulier montre la puissance terrifiante de cette machine fictive en termes de surveillance : lorsque l'agent Gary Seven lui demande d'identifier une femme travaillant dans son bureau. Il répond en indiquant son nom, son âge, sa profession, son poids, la couleur de ses cheveux, mais aussi des caractéristiques psychologiques et la description de ses tâches de naissance. À ce moment, ce second personnage se retourne, court vers un bouton relié à l'ordinateur pour arrêter la voix de ce dernier et l'empêcher de révéler plus d'informations. Le jeu d'acteur suggère clairement le malaise ressenti par le personnage, qui met ce dernier en position d'infériorité face à Gary Seven.

Nous allons maintenant voir comment cet imaginaire dystopique a joué un rôle dans l'identification des ordinateurs comme étant un problème public faisant peser un risque pour la « vie privée ». Nous verrons ensuite que le paradigme libéral présenté dans le précédent chapitre a commencé à jouer à ce moment-là un rôle central dans les controverses autour de l'ordinateur et de la « vie privée ».

3.2.4. De la science-fiction à la politique : les fichiers informatisés deviennent un problème public

Les premières réflexions institutionnelles au sujet de la protection de la vie privée des personnes sur lesquelles des informations sont stockées dans des ordinateurs remontent au tout début de l'informatique, aux États-Unis, dans les années 1950. Elles sont encore tout à fait confidentielles.

C'est à cette époque que sont lancés des projets qui visaient à faciliter l'accès aux données collectées par les autorités publiques à des fins de recherche scientifique, notamment en sciences sociales (Kraus, 2013). Pour Robert Burgess, directeur du *Census Bureau* (bureau du recensement), il était indispensable de garantir la confidentialité de ces informations pour conserver la *confiance* de la population auprès de laquelle elles étaient recueillies[15]. Il écrit en 1957 :

> « Peu de chercheurs souhaiteraient assouplir les règles de divulgation au point que la qualité des statistiques en soit diminuée. Si cela se produisait, personne n'en souffrirait plus que les chercheurs eux-mêmes, et la plupart d'entre eux, en prenant la mesure de cette gravité, nous ont poussé à protéger les informations données en confidentialité[16]. » (Burgess, 1957, p. 4, cité par : (Kraus, 2013, p. 2-3))

De telles prises de position semblent cependant avoir été très rares. Michel Atten écrit ainsi à ce sujet : « nous n'avons guère trouvé de prises de position touchant aux questions de confidentialité dans les revues examinées avant les années 1960 » (Atten, 2013, p. 40).

Au début des années 1960, les évolutions de l'informatique permettent d'envisager une informatisation du traitement des données statistiques, rendant plus facile l'indexation des données, leur croisement, et leur mise à disposition pour des chercheurs. Ces évolutions techniques accompagnent une forte croissance de la collecte de données. Entre 1961 et 1963, les financements fédéraux d'enquêtes statistiques font un bond de 23 % (Atten, 2013, p. 34). Entre 1963 et 1966, selon un rapport de Willis Ware, le nombre d'ordinateurs passe de 350 à 700 pour

15 Nous voyons ainsi dès les années 1950 se construire l'argument de la confiance : sans confiance de la part du public, celui-ci va se méfier, et cette méfiance va gêner l'efficacité de la collecte de données et, in fine, empêcher d'atteindre les finalités pour lesquelles cette collecte est entreprise. Nous aurons l'occasion d'y revenir.
Cf. sections 3.8., 4.5. et 5.6.3.

16 Traduction. Texte original : « Few research workers would wish to relax the disclosure rules to the extent that this would lower the quality of statistics. In such an event, no one would be harmed more than the research people themselves, and many of them, realizing this, have urged us to protect information given in confidentiality. »

la seule armée de l'air américaine (Ware, 1966). En 1964, l'État de New York lance un plan appelé « *State Identification and Intelligence System* » destiné à rassembler dans des ordinateurs des informations provenant de 3600 sources différentes (Westin, 1967, cité par : Atten, 2013, p. 34), notamment pour améliorer l'efficacité de la police (Atten, 2013, p. 34).

Toujours à cette même époque, des scientifiques commencent à voir dans les ordinateurs autre chose que de simples machines à calculer. Pour eux, ces machines servent également à traiter de l'information. Ils y voient la possibilité d'inventer une nouvelle science interdisciplinaire, alliant mathématiciens, logiciens, bibliothécaires, linguistes et ingénieurs (Atten, 2013, p. 35). L'informatique était née.

Toutes ces nouvelles possibilités furent perçues comme un progrès par le *Social Science Research Council* (SSRC) qui, en avril 1965, publia un rapport dénonçant l'éparpillement à travers 20 agences fédérales de statistiques de plus de 600 jeux de données répartis sur une centaine de millions de cartes perforées, et une trentaine de milliers de bandes magnétiques, dont l'accès à des fins de recherche scientifique est très compliqué (Social Science Research Council, 1965, cité par : Kraus, 2013). En 1966, un comité dirigé par Carl Kaysen recommande la mise en place d'un centre de données national (*national data center*) (Kraus, 2013).

Mais la presse avait commencé à la même époque à s'intéresser de près au rôle des ordinateurs dans les dispositifs de surveillance de la population. En 1964, *The New York Times* révèle l'une des premières ventes de données personnelles (Atten, 2013, p. 41). La même année, *Naked Society*, un essai de Vance Packard, avait déjà obtenu un grand succès de librairie et est rapidement ré-édité (Packard, 1965 [1964]). Ce livre dresse un réquisitoire contre les abus du MacCarthyisme, et avertit le lecteur du danger de nouvelles technologies comme les détecteurs de mensonge, les caméras de surveillance, les techniques d'écoute téléphonique, et l'informatique. Son auteur fut invité à témoigner en 1966 devant le comité d'enquête parlementaire de la Chambre des représentants.

Dans ce contexte médiatique, l'annonce de la proposition de créer un centre de données national provoqua à son tour des réactions. En août 1966, le *Pittsburgh Post-Gazette* titre « *Computer as Big Brother* ». Le *Wall Street Journal* également s'inquiète des atteintes qu'un tel centre de données fait peser sur les libertés civiles, et toujours en août 1966, un éditorial du *New York Times* parle de « Orwellian nightmare » pour qualifier le projet (Kraus, 2013, p. 13-14).

C'est en raison de la même annonce, qui est en quelque sorte l'élément déclencheur de l'histoire narrée dans ce chapitre, que la Chambre des représentants se saisit à son tour de la question en mettant en place une commission d'enquête parlementaire. Celle-ci, le *Special Subcommittee on Invasion of Privacy* du *Committee on Government Operations*, procéda à des

auditions dès les 26, 27 et 28 juillet 1966, soit peu de temps avant la publication des articles de presse sur la proposition de centre national de données retrouvés par Rebecca Kraus au cours de son étude sur cette période. Son président était Cornelius Gallagher, un élu démocrate du New-Jersey, qui rappela dans un discours ouvrant les auditions parlementaires, le 26 juillet 1966, l'objectif des travaux de la commission[17] :

> « Le Comité spécial sur l'atteinte à la vie privée débute aujourd'hui son examen des propositions d'instauration d'un Centre National des Données ou d'une Banque Nationale des Données. Le sous-comité s'intéresse aux questions d'économie et d'efficience en tant qu'elles sont liées à des questions d'atteinte à la vie privée[18]. » (US House of Representatives, 1966, p. 1)

Si la médiatisation des questions de vie privée à la fois dans la littérature de science-fiction[19] et par le succès de l'essai *Naked Society*, dont l'auteur, Vance Packard, est longuement auditionné par la commission d'enquête, a joué un rôle dans la mise à l'agenda parlementaire et politique de la question du rapport entre informatique et vie privée, la presse quotidienne ne semble pas, étant donné la chronologie que nous venons de décrire, avoir joué de rôle déterminant. Cette mise à l'agenda doit donc plutôt s'interpréter comme une conjonction entre un contexte général d'affirmation constitutionnelle du droit à la vie privée (Cour Suprême des États-Unis, 1965, affaire Griswold c. Connecticut), de luttes pour les droits civils[20], de l'image de l'ordinateur dans l'imaginaire social et la fiction, et de l'adhésion d'un grand nombre d'acteurs du débat, parmi lesquels Vance Packard, Willis Ware, Alan Westin ou encore Cornelius Gallagher, à un paradigme libéral de la vie privée qu'ils ont contribué à former[21].

---

17 Ces auditions font suite à des travaux entamés dès 1965 (US Hous of Representatives, 1966, p. 1).

18 Traduction. Texte original : « The Special Committee on Invasion of Privacy today begins its investigation into proposals to establish a National Data Center or Data Bank. The subcommittee is interested in questions of economy and efficiency as they are related to problems of invasion of privacy ».

19 Une recherche dans le texte de la retranscription des auditions parlementaires du *Subcommittee on Invasion of Privacy* montre 3 occurrences du terme « Orwell », 9 occurrences du terme « 1984 », 6 occurrences du terme « Big Brother » et 1 occurrence du terme « Huxley ». Cela montre la présence de certaines œuvres de science-fiction dystopiques dans l'imaginaire des personnes qui ont participé aux auditions et aux travaux de cette commission d'enquête parlementaire. Notons que le nombre total d'occurrences de ces termes peut en réalité être encore plus grand, car le texte du document, obtenu au format PDF, a été généré par reconnaissance automatique de caractères (OCR) à partir d'images numérisées de copies du rapport imprimé. Cette méthode n'es pas parfaitement fiable. Par exemple, le terme « Westin », en référence à Alan Westin, juriste américain théoricien du droit à la vie privée, n'a pas été trouvé, bien qu'il soit fait plusieurs fois référence à ses travaux ; le logiciel de reconnaissance de caractères avait détecté la chaîne de caractères « Westm » au lieu de « Westin », ce qui explique l'erreur.

20 La marche de Martin Luther King, où il prononce le célèbre discours connu pour la phrase « I have a dream », à Washington, a lieu en 1963. Le Civil Rights Act, qui déclare illégale toute discrimination fondée sur la race, la couleur, la religion, le sexe ou l'origine nationale, est adopté en 1964. Le Voting Rights Act, qui interdit les discriminations raciales dans le vote, est adopté en 1965.

21 Cf. section 2.2.

Nous retrouvons bien dans les débats l'image inquiétante d'une informatique bureaucratique et déshumanisante, popularisée par les arts et de la science-fiction de l'époque. En parlant de la centralisation des données engendrée par la création du *National Data Center*, le président du sous-comité, Cornelius E. Gallagher, affirme :

> « L'une de ces tendances est la demande croissante d'une infrastructure centralisée au sein de la structure du gouvernement fédéral, qui serait alimentée par des informations recueillies au sein de différentes agences gouvernementales et dont des ordinateurs pourraient tirer des faits sélectionnés. Nous affirmons que l'absence de toute garantie au sein de cet organisme pourrait mener à la création de ce que j'appelle 'L'Homme Informatisé'. Cet Homme, tel que je le vois, serait déchu de son individualité et de sa vie privée. De par l'uniformisation entraînée par les progrès informatiques, son statut dans la société serait mesuré par l'ordinateur et cet être perdrait son identité personnelle. Sa vie, ses talents et ses capacités de générer des revenus seraient très largement réduits avec très peu d'alternatives à sa disposition[22]. » (US House of Representatives, 1966, p. 2)

Frank Horton, un député de l'État de New-York auditionné par la commission d'enquête, propose un parallèle entre l'informatique et l'âge nucléaire :

> « Je suis devenu convaincu que l'ampleur du problème auquel nous sommes aujourd'hui confrontés est semblable aux bouleversements forgés dans la vie de notre nation à l'aube de l'ère nucléaire[23]. » (US House of Representatives, 1966, p. 5)

Même s'il n'est pas cité dans les auditions de la Chambre des Représentants, de telles réflexions sur les effets politiques de l'informatisation (ou de l'automatisation) sont à rapprocher des travaux de l'historien et sociologue des techniques Lewis Mumford, qui eut une influence intellectuelle notable sur la pensée de la technique de son temps[24], et qui venait de publier deux ans plus tôt un article proposant une distinction entre techniques démocratiques et techniques

22 Traduit de l'anglais. Texte original : « One such trend is the increasing demand for a centralized facility, within the structure of the National Government, into which would be poured information collected from various Government agencies and from which computers could draw selected facts. It is our contention that if safeguards are not built into such a facility, it could lead to the creation of what I call the "Computerized Man". "The Computerized Man," as I see him, would be stripped of his individuality and privacy. Through the standardization ushered in by technological advance, his status in society would be measured by the computer, and he would lose his personal identity. His life, his talent and his earning capacity would be reduced to a tape with very few alternatives available »

23 Traduit de l'anglais. Texte original : « I have become convinced that the magnitude of the problem we now confront is akin to the changes wrought in our national life with the dawning of the nuclear age »

24 Il est par exemple cité par Stefano Rodotà lors d'un séminaire organisé à Paris par l'OCDE en 1974 sur la protection des données (Rodotà, 1974)

autoritaires. L'informatique, c'est-à-dire le gouvernement cybernétique (*cybernetic direction*) et l'automatisation (*automation*), y apparaissent clairement dans la catégorie des techniques autoritaires :

> « À travers les processus de mécanisation, d'automatisation et de direction cybernétique, cette technique autoritaire a enfin réussi à surmonter sa principale faiblesse : sa dépendance initiale aux mécanismes asservis résistants, parfois en désobéissance active, mais encore suffisamment humains pour abriter des objectifs qui ne correspondent pas toujours à ceux du système[25] » (Mumford, 1964, p. 5)

Mais l'existence d'une perception de l'informatique comme une technique autoritaire, liée au complexe militaro-industriel et assimilé à l'ère nucléaire, même partagée par des députés, ne permet pas d'expliquer pourquoi l'ordinateur poserait un problème précisément pour la protection de la vie privée. Cela permet encore moins de comprendre pourquoi l'éventuelle érosion de cette dernière serait un problème tout court. Il faut, pour le comprendre, en passer aussi par les conceptions sur la « vie privée » auxquelles adhéraient les participants aux travaux et auditions de cette commission d'enquête.

Pour commencer, le lien entre l'ordinateur et la vie privée venait, pour les participants aux auditions de la capacité, du premier à conserver longtemps des données, à les retrouver bien plus facilement qu'auparavant, et à les recouper, de sorte à grandement faciliter le fichage de la population. Paul Baran, qui venait d'inventer en 1964 le principe des réseaux de communication distribués (Baran, 1964) sur lequel repose aujourd'hui Internet, affirma ainsi devant le sous-comité :

> « Les problèmes liés à l'atteinte à la vie privée sont, à mon avis, significatifs […]. Les systèmes de données individuelles en cours d'élaboration, tant publics que privés, peuvent être reliés ensemble pour former un réseau qui soulèvera essentiellement les mêmes problèmes [qu'un centre national de données]. […] Comment contrôler le développement de l'automatisation de tous les fichiers d'informations sensibles afin de protéger au mieux

25 Traduit de l'anglais. Texte original : « Through mechanization, automation, cybernetic direction, this authoritarian technics has at last successfully overcome its most serious weakness: its original dependence upon resistant, sometime actively disobedient servo-mechanims, still human enough to harbord purposes that do not always coincide with those of the system. »

les droits de l'individu et d'éviter une nation "1984"[26] ? » (US House of Representatives, 1966, p. 120-121)

Cette citation témoigne du fait que les juristes ne soient pas les seuls à s'inquiéter des dangers qu'ils perçoivent dans l'informatique. Leur inquiétude est partagée par un certain nombre d'informaticiens. Un collègue de Paul Baran à la Rand Corporation, Willis Ware, futur co-fondateur de l'association militante *Electronic Privacy Information Center* (EPIC) (voir : Rotenberg, 2013), publia dès le milieu des années 1960 des rapports sur la question (Atten, 2013). En 1966, il explique aux responsables de la Rand Corporation, dans un rapport depuis déclassifié, commandé par l'armée de l'air des États-Unis :

« Parce que la capacité de l'ordinateur à accepter et à corréler de l'information issue de fichiers ou de banques de données très grandes existera, cela rendra possible une surveillance personnelle et sociale par une agence élue pour le faire. La profondeur de surveillance pourrait surpasser la seule intrusion dans la vie privée » (Ware, 1966 cité par Atten, 2013, p. 45)

Après avoir réfléchi de façon générale à l'impact futur de l'informatique sur la société (Ware, 1966), Willis Ware a présenté en avril 1967 un papier à une conférence à Atlantic City, qui fut ensuite publiée par son employeur (Ware, 1967), sous le titre : « *Security and Privacy in Computer Systems* ». Les problèmes de sécurité et de protection de la vie privée y sont présentés comme des problèmes « distincts mais reliés[27] » qui posent notamment le problème d'ingénierie suivant : comment éviter les fuites d'informations confidentielles, et l'accès par des personnes non-autorisées aux données ? Puis l'article définit les termes « *private* » et « *privacy* » comme : « normalement associés à un individu dans un sens personnel[28] ». S'il développe surtout des considérations techniques sur les modalités de piratage de données confidentielles, soit couvertes par un secret comme le secret militaire, soit relevant de la vie privée des personnes, certains passages montrent une certaine sensibilité de l'auteur de l'article à la question politique de la protection du droit à la vie privée, et à l'idée que l'informatique, de ce point de vue, représente une menace :

« D'immenses quantités d'informations personnelles sont accumulées dans des fichiers informatiques, et il ne fait aucun doute que les incitations à franchir les mesures de

26 Traduit de l'anglais. Texte original : « The problem of the invasion of privacy are, in my view, significant […]. Individual data systems, both public and private, now being developed, can be tied together eventually into a network that will present essentially the same problems [as a national data center]. […] How shall we control the development of the automation of all sensitive information files in order to best protect the rights of the individual and avoid a "1984" nation ? »

27 « distinct but related » (Ware, 1967, p. iii)

28 « normally associated with an individual in a personal sense » (Ware, 1967, p. 3)

protection de la vie privée augmenteront. Les lois existantes peuvent s'avérer inadéquates ou nécessiter une mise en œuvre plus rigoureuse. […] L'existence de gardes-fous juridiques et éthiques adéquats de protection des renseignements personnels ne peut être considérée comme acquise[29]. » (Ware, 1967, p. 14-15)

Plus loin encore, Willis Ware, dans son article, montre qu'il était au courant des auditions parlementaires de 1966, qu'il connaît la référence à « *Big Brother* », ce qui démontre que l'information circulait entre informaticiens d'un côté, juristes et personnel politique de l'autre, s'intéressant à ces questions de protection de la vie privée :

« Le spectre de "big brother" agité au cours des récentes auditions du Congrès sur "l'atteinte à la vie privée" par le biais de fichiers informatiques de masse est en effet étroitement lié au volume d'informations exposées[30]. » (Ware, 1967, p. 15-16)

Nous voyons bien, à travers tous ces exemples, le lien se faire entre imaginaire inquiétant de l'ordinateur relayé par la science fiction, et risques pour la protection de la « vie privée ». Mais pour quelle conception de la « vie privée » les protagonistes des discussions devant la commission d'enquête de la Chambre des représentants s'inquiètent-ils en 1966 ?

3.2.5. La montée en puissance du paradigme libéral de la vie privée dans le débat

Le « droit à l'oubli », en lien avec des informations personnelles sur format numérique, est un sujet qui fait encore couler beaucoup d'encre dans des controverses des années 2010, suite à la décision « Google contre Espagne » de la CJUE[31] consacrant un droit au déréférencement sur les moteurs de recherche, en application de la directive communautaire 95/46/CE. Or, c'est dans la retranscription des auditions parlementaires du *Subcommittee on the Invasion of Privacy* que nous avons trouvé la plus ancienne utilisation de cette formule. S'inquiétant comme Paul Baran de la facilité à recouper des informations sur des individus, stockées sur des supports inaltérables sans limite de durée de conservation, Cornelius Gallagher affirma :

29 Traduit de l'anglais. Texte original : « Great quantities of private information are being accumulated in computer files; and the incentives to penetrate the safeguards to privacy are bound to increase. Existing laws may prove inadequate, or may need more vigorous enforcement. […] It can not be taken for granted that there now exist adequate legal and ethical unbrellas [sic] for the protection of private information. »

30 Traduit de l'anglais. Texte original : « Certainly the "big brother" spectre raised by recent Congressional hearings on "invasion of privacy" via massive computer files is strongly related to the volume of information at risk. »

31 CJUE 8 avril 2014 « Google contre Espagne », Aff. C-131/12.

« The possible future storage and regrouping of such personal information also strikes at the core of our Judeo-Christian concept of “forgive and forget,” because the computer neither forgives nor forgets[32]. » (US House of Representatives, 1966, p. 4)

Cette conception judéo-chrétienne du pardon n’est pas la seule source d’inspiration permettant de comprendre l’engagement des acteurs impliqués dans cette commission d’enquête en faveur de la protection du droit à la vie privée. D’autres citations de la retranscription des auditions permettent de voir l’influence jouée par le paradigme libéral de la vie privée. Ainsi, Burton Squires, professeur d’informatique, entama son intervention par une référence au philosophe libéral utilitariste John Stuart Mill :

« En me préparant à cette audience, j'ai cru bon de relire l'essai de John Stuart Mill intitulé "De la liberté", dans lequel il écrit ceci :

“*Le seul objet qui autorise les hommes, individuellement ou collectivement, à troubler la liberté d’action d’aucun de leurs semblables, est la protection de soi-même. La seule raison légitime que puisse avoir une communauté pour user de force contre un de ses membres, est de l’empêcher de nuire aux autres. Elle n’en a pas une raison suffisante dans le bien de cet individu, soit physique, soit moral. Un homme ne peut pas, en bonne justice, être obligé d’agir ou de s’abstenir, parce que ce serait meilleur pour lui, parce que cela le rendrait plus heureux, ou parce que, dans l’opinion des autres, ce serait sage ou même juste. […] Sur lui-même, sur son corps et sur son esprit, l’individu est souverain.*”[33]

Ce comité a déjà entendu de nombreux témoignages à propos de la collecte de données concernant les pensées, les croyances, les émotions et les sensations d'une personne. […] De telles données peuvent restreindre l'exploration des idées, appauvrir la curiosité intellectuelle et restreindre la libre expression de la pensée. L'essai de M. Mill approfondit également davantage ces domaines. Je voudrais donc étendre la portée de ces concepts dans la mesure où ils sont liés au traitement automatique des données[34]. » (US House of

32 Traduction : « Les futures possibilités de stocker et de regrouper ces informations personnelles s’en prennent également au cœur de notre concept judéo-chrétien du "pardon et de l'oubli". En effet, l'ordinateur ne pardonne ni n'oublie. »
Le texte en anglais a été maintenu dans le corps du texte car ses effets de style ne sont pas bien rendus dans la traduction française.

33 NDT : Texte en italique extrait de *De la liberté* de John Stuart Mill issu de la traduction par Charles Brook Dupont-White publiée chez Guillaumin et Compagnie en 1860, et mise en ligne sur le site Wikimedia à l’adresse : https://fr.wikisource.org/wiki/De_la_libert%C3%A9/Texte_entier (page consultée le 24 septembre 2019)

34 Traduit de l’anglais. Texte original : « In preparing for this hearing, I felt it appropriate to read again John Stuart Mill’s essay “On Liberty”, in which he says:
“The sole end for which mankind are warranted, individually or collectively, interfering with the liberty of action of any of their number, is self-protection. That the only purpose for which power can be exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or

Representatives, 1966, p. 136)

Cette citation illustre la place du libéralisme utilitariste dans les réflexions sur la protection de la « vie privée » face au danger perçu de l'ordinateur électronique dès les années 1960. Alan Westin, l'un des auteurs les plus cités du paradigme libéral de la vie privée (voir : Bennett, 1992 ; Bennett et Raab, 2003), n'a pas participé aux auditions à la Chambre des représentants en 1966, mais cela n'a pas empêché ses travaux d'y être discutés.

Dans un de leurs échanges au cours des auditions de la commission d'enquête sur la vie privée de la Chambre des représentants en 1966, Vance Packard et Cornelius Gallagher firent en effet référence aux travaux d'Alan Westin :

> « M. Gallagher — Dr. Westin, spécialiste des question de protection de la vie privée, dit : "À moins que la question de la protection de la vie privée ne soit au cœur de la planification et de l'administration des futurs systèmes informatiques, les possibilités de surveillance des données sur l'individu en 1984 pourraient être terrifiantes". Avez-vous des commentaires à ce sujet ?
>
> M. Packard — Je suis tout à fait d'accord. […] Je pense qu'une menace, comme l'ont dit le Dr. Westin et beaucoup d'autres, plane au-dessus de nous : celle que la machine domine nos vies[35]. » (US House of Representatives, 1966, p. 15-16)

Comme nous l'avions vu dans le chapitre précédent, pour Alan Westin, dont les travaux précédant la publication de son ouvrage *Privacy and Freedom*, sont déjà évoqués ci-dessus par Vance Packard et Cornelius Gallagher, la vie privée protège l'autonomie individuelle, indispensable pour prendre les décisions qui ne concernent pas la sphère du politique et qui permettent à chaque personne d'être maître de son propre bonheur. Il assemble ainsi dans sa théorie les éléments principaux de ce qui constitue le paradigme libéral de la vie privée, fondé sur l'idée de contrôle individuel, par opposition aux théories qui prônent la protection par des

---

moral, is not a sufficient warrant. He cannot rightfully be compelled to do or forbear because it will be better for him to do so, because it will make him happier, because, in the opinion of others, to do so would be wise or even right. […] Over himself, over his own body and mind, the individual is sovereign"
This committee has already heard extensive testimony regarding the collection of data concerning a person's thoughts, beliefs, emotions and sensations. […] Such data can restrict the exploration of ideas, diminish the intellectual curiosity and restrain the free expression of thought. Mr. Mill's essay also develops these areas more fully. I would like, therefore, to extend these concepts as they relate to automatic data processing »

35 Traduit de l'anglais. Texte original : « Mr. Gallagher — Dr. Westin, an expert in the problems of privacy, says: "Unless the issue of privacy is in the forefront of planning and administration of future computer systems, the possibilities of data surveillance over the individual in 1984 could be chilling." Would you care to comment this?
Mr. Packard — I certainly would agree that is correct. […] I think we do have this threat, as Dr. Westin said and as many others have said, hanging over us that the machine can dominate our lives. »

moyens juridiques de frontières collectivement définies autour d'un espace physique et informationnel de l'intime.

Quelques années plus tard, au début des années 1970, Willis Ware se vit confier la présidence d'une commission chargée de remettre un rapport sur la protection de la vie privée au Département fédéral[36] de la Santé, de l'éducation et des services sociaux (*U.S. Department of Health, Education and Welfare*). Ce rapport, connu sous le nom de « rapport HEW », de l'acronyme des initiales du ministère fédéral qui l'avait commandé, fut rendu en juillet 1973. Il compta Arthur Miller parmi ses co-auteurs, professeur de droit à Harvard, et, à l'instar d'Alan Westin, l'un des juristes théoriciens du paradigme libéral de la vie privée (Miller, 1971).

Le rapport, qui comprenait notamment une synthèse des travaux internationaux sur le sujet, et une description comparative des évolutions juridiques dans différents pays du bloc de l'Ouest, préconisait l'adoption d'un « *Code of Fair Information Principles* » (Ware, 1973, p. xx) reposant sur cinq principes de base :

- « Il ne doit pas exister de système d'enregistrement de données personnelles dont l'existence même soit secrète[37] » (Ware, 1973, p. xx)
- « Il doit exister une façon pour un individu d'apprendre quelles informations le concernant sont stockées dans un fichier, et comment elles sont utilisées[38] » (Ware, 1973, p. xx)
- « Il doit exister une façon pour un individu d'empêcher qu'une information à son sujet soit obtenue pour une finalité donnée soit utilisée ou rendue disponible pour une autre finalité sans son consentement[39] » (Ware, 1973, p. xx)
- « Il doit exister une façon pour un individu de corriger ou amender un enregistrement d'information identifiable le concernant[40] » (Ware, 1973, p. xx)
- « Toute organisation créant, maintenant, utilisant ou disséminant des enregistrements de données personnelles identifiables doivent garantir la fiabilité de la donnée pour la finalité à laquelle elles sont destinées et doit prendre toutes précautions pour empêcher tout détournement d'usage frauduleux [*misuse*] de cette donnée[41] » (Ware, 1973, p. xxi)

36 Équivalent d'un ministère.

37 Traduction de l'auteur. Texte original : « There must be no personal data record-keeping systems whose very existence is secret »

38 Traduction de l'auteur. Texte original : « There must be a way for an individual to find out what information about him is in a record and how it used »

39 Traduction de l'auteur. Texte original : « There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent »

40 Traduction de l'auteur. Texte original : « There must be a way for an individual to correct or amend a record of identifiable information about him »

41 Traduction de l'auteur. Texte original : « Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data »

Le rapport HEW, et les principes ci-dessus, ont inspiré l'adoption d'une loi fédérale qui réglemente les traitements de données à caractère personnel par l'administration fédérale : le Privacy Act de 1974. Notons que cette façon de résumer le contenu du droit *de la* protection des données à caractère personnel sous forme de « principes » est similaire à ce qu'avait proposé la commission dirigée par Kenneth Younger au Royaume-Uni en 1972[42]. Elle en est d'ailleurs probablement inspirée, puisque le rapport de la commission Younger est cité et résumé en annexe du rapport HEW (Ware, 1973, p. 173).

Ainsi, à la fin des années 1960, il existait déjà aux États-Unis une expertise sur la relation entre informatique et protection de la vie privée. Les connaissances et les discours produits sur le sujet, tant par des informaticiens, des juristes, que du personnel politique, étaient fortement influencés par une image angoissante d'une informatique évoquant le roman *1984* de George Orwell, et motivés par le référentiel du paradigme libéral de la vie privée, que certains de ces acteurs, comme Vance Packard, Alan Westin ou encore Arthur Miller, ont contribué à théoriser. L'expertise accumulée fut lue en Europe par les acteurs impliqués dans les différents groupes de travail qui, dans les années 1970, au Conseil de l'Europe comme à l'OCDE, rédigèrent les premiers textes juridiques internationaux sur la protection de la vie privée vis-à-vis des banques de données électroniques, et inventèrent un « droit à la protection des données personnelles ». Nous verrons d'ailleurs que parmi les acteurs dont nous venons de décrire l'activité aux États-Unis, plusieurs – tant des juristes comme Alan Westin que des informaticiens comme Willis Ware – furent invités à des conférences eu Europe où ils purent rencontrer des acteurs européens du réseau transgouvernemental qui y rédigea les premières lois de protection des données au tout début des années 1970.

3.3. L'invention en Europe de la *Datenschutz* (protection des données)

3.3.1. Comment la controverse sur l'ordinateur et les fichiers de renseignements personnels a traversé l'Atlantique

Jusqu'à la fin des années 1960 et durant toutes premières années de la décennie suivante, divers acteurs ont accumulé de l'expertise, aux États-Unis, sur la question de la protection de la vie privée vis-à-vis de la menace représentée par l'ordinateur dans les perceptions de l'époque influencées notamment par la science-fiction et une prise de conscience du rôle sociopolitique de la technique dans une société marquée par l'époque McCarthy et des mouvements sociaux contre la ségrégation raciale, pour les libertés civiles, sans oublier les mobilisations contre la guerre du

42 Cf. section 6.6. et annexe 13.

Vietnam. Comme nous venons de le voir, l'expertise accumulée aux États-Unis a notamment consisté en des études détaillées de la façon dont les ordinateurs sont utilisés. Le rapport du sous-comité présidé par Cornelius Gallagher en 1966, ou encore les ouvrages de Vance Packard (1965), Alan Westin (1970), ou encore Arthur Miller (1971), sont des exemples de tels travaux.

Des études similaires furent menées en Europe au cours des années 1970 (Conseil d'Etat (France), 1970 ; Gallouedec Genuys et Maisl, 1976 ; Niblett, 1971 ; Younger, 1972), inspirées des travaux américains. Si dès 1969 une proposition de loi est rédigée au Royaume-Uni[43], elle n'aboutira pas, et c'est dans un Land de RFA qu'est adoptée en 1970 la première loi au niveau mondial portant sur les données à caractère personnel. Cette loi fut aussi la première loi à s'appeler loi de « protection des données », de l'allemand « *Datenschutz* », dont l'invention est généralement attribuée à Spiros Simitis, juriste hélleno-allemand de l'Université de Francfort, qui s'inquiétait du pouvoir que pourrait donner à l'État sur ses citoyens des bases de données personnelles informatisées :

> « Je m'intéressais beaucoup à l'influence de l'automatisation sur le droit […]. Une nouvelle ère avait commencé, une nouvelle ère permettant d'avoir des connaissances, de les utiliser de manière tout à fait objective, et justement pour cette raison, cette ère allait bouleverser la structure et l'importance du droit. C'est là que les discussions ont commencé, avec des doutes à ce sujet et la nécessité de poser des questions. Par exemple, si l'on dispose d'autant de données sur une personne précise, quelles seront les conséquences sur les relations entre cette personne et l'État, ou entre cette personne et une entreprise publique ou privée, et notamment quelles seront les possibilités d'influencer directement le comportement de cet individu[44] ? » (Entretien avec Spiros Simitis)

Comme il le rappela en entretien, ces travaux européens étaient grandement inspirés, à l'origine, par la lecture des travaux réalisés aux États-Unis dans la décennie des années 1960 :

> « Lorsque nous avons commencé à réfléchir au sujet, à discuter, et à voir comment réagir, l'une des principales sources d'inspiration pour notre propre réflexion et prospective était une étude continue sur les décisions judiciaires aux États-Unis concernant

43 Data Surveillance Bill 1969, proposition de loi déposée par le député conservateur Kenneth Baker

44 Traduit de l'anglais. Texte original : « I was very interested in the influence of automation on Law […]. A new era had started, a new era which would allow you to have a knowledge, to use that knowledge in an absolutely objective way and for precisely that reason would change the whole structure and importance of law. And that's where the discussions started, with the doubts about that, and with the need to ask questions to if you have all those data on a particular person, for instance what will be the implication of that on the relationship between that particular person and the state or private company, commercial company and both state and private company ; possibilities to influence directly so to say the comportment of the particular individuals »

l'automatisation. Les Américains eux-mêmes ne disposaient pas encore de loi, mais ils ont fourni la majeure partie des bases de réflexion étant donné que l'automatisation de leur industrie […] était beaucoup plus développée qu'en Europe[45]. » (Entretien avec Spiros Simitis)

Les premières réflexions structurées sur les risques de l'informatisation pour le droit à la vie privée provenaient donc des États-Unis, où le paradigme libéral de la vie privée a été théorisé. Mais en 1970, aucune loi n'avait encore été adoptée dans ce pays de *Common Law*. Lorsque la controverse sur le sujet a traversé l'Atlantique, elle s'est implantée en Europe, dans un continent où sont majoritaires des pays de droit continental. Dans ces derniers, la culture juridique est plus favorable au règlement des problèmes publics par l'outil législatif. S'y ouvre alors une demi-décennie où furent rédigées et adoptées les toutes premières lois nationales de protection des données a été résumé. Cette période a été résumée en 1974 par Hans Peter Gassman, alors en charge de ces sujets pour le secrétariat de l'OCDE, où il évoque la « littérature de mise en garde » venue des États-Unis :

« L'enjeu est la maîtrise par la société de la technologie moderne de l'information et, alors que dans la dernière décennie on a observé l'apparition d'une « littérature de mise en garde », les années 70 seront consacrées à la mise au point d'un « logiciel social », sous forme de lois, réglementations, codes déontologiques, etc., nécessaire pour réglementer la technologie de l'information et s'assurer que ses progrès auront, tout compte fait, un aspect positif pour l'humanité. » (Hans Peter Gassman et G. Russel Pipe, dans : OCDE, 1974, p. 13)

Nous verrons à travers les cas de la Hesse, de la Suède, des Pays-Bas et de la France quatre exemples de la façon dont la protection des données fut mise à l'agenda politique. La Hesse, la Suède, le Rhin-Palatinat et la France furent, dans cet ordre, les quatre premiers États en Europe à adopter une loi. Les Pays-Bas, comme d'ailleurs le Royaume-Uni, n'adoptèrent de lois qu'à la fin des années 1980[46].

Dans un premier temps, nous envisagions de nous concentrer uniquement sur la Hesse, où fut adoptée la première loi de protection des données et où le terme fut inventé, la Suède, où fut adoptée la première loi nationale, et la France, dont la loi fut rédigée par Louis Joinet, qui allait

45 Traduit de l'anglais. Texte original : « When we started thinking about that, and discussing it, and trying to react to it, one of the main sources of inspiration of our reflection and of our expectations, was a continuous study on decisions, court decisions, in the United States, that had to do with automation. The Americans themselves had not yet a law. But they offered most of the material, because the automation in their industry […] was by far more developed than in Europe »

46 Data Protection Act 1984 au Royame-Uni, et Wet persoonsregistraties van 1988 aux Pays-Bas.

ensuite jouer un rôle de premier plan au Conseil de l'Europe et à l'OCDE dans la rédaction de la Convention 108 et des Lignes directrices. Toutefois, l'exemple singulier des Pays-Bas méritait d'être développé. Il s'agit en effet d'un rare exemple de cas où la mise à l'agenda de la question fut la conséquence d'un mouvement social. Ces mobilisations, si elles n'aboutirent pas immédiatement à une loi – puisqu'il fallut y attendre la fin de la décennie suivante – débouchèrent sur l'abandon du modèle traditionnel de recensement décennal aux Pays-Bas, et, surtout, fournirent un argument empirique au discours des défenseurs de la vie privée sur la nécessité d'une loi pour garantir la confiance des citoyens en l'informatique[47].

Les réflexions sur l'informatique et la vie privée qui ont eu lieu au Royaume-Uni entre 1968 et 1975 méritent elles aussi un développement approfondi. En effet, c'est là qu'est née l'idée de formuler les règles à respecter en matière de protection des données sous forme de « principes ». Cette idée – reprise dans le rapport HEW aux États-Unis en 1973 – fut ensuite proposée par la délégation britannique au groupe d'experts du Conseil de l'Europe sur la protection de la vie privée vis-à-vis des banques de données électroniques (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 5 Rév.). Sous une forme révisée, elle intégra les deux résolutions du Conseil de l'Europe de 1973 et 1974, les Lignes directrices de l'OCDE, et la Convention 108. Ces principes sont aujourd'hui toujours en vigueur, et listés à l'article 5 du RGPD. Par souci de lisibilité, l'histoire de la mise à l'agenda et des premières réflexions institutionnelles sur la protection des données au Royaume-Uni ont toutefois été intégrées un peu plus loin dans la section sur l'origine des principes de protection des données[48].

3.3.2. L'invention de la « protection des données » dans le Land de Hesse puis du « droit à l'auto-détermination informationnelle » en République fédérale d'Allemagne

La loi de Hesse de protection des données de 1970[49] n'a pas été la première, en RFA, à imposer des règles sur la collecte et l'exploitation de données à caractère personnel. Lorsque le Schleswig-Holstein avait déjà adopté, dès 1968, une loi portant création de centres de traitement informatisé de données, et celle-ci contenait des dispositions dont s'inspire le texte de Hesse (González Fuster, 2014a, p. 69 ; Hondius, 1975, p. 35). La véritable innovation de ce dernier est que dans un contexte où, selon Gloria González Fuster, le gouvernement du Land avait été très actif dans la promotion du traitement automatisé de données à des fins administratives, la loi protégeant les citoyens, qui est la loi de protection des données, a été adoptée peu après et séparément de la loi du 16 décembre 1969 portant création de centres de traitement automatisé de données (González Fuster, 2014a, p. 69), qui elle-même n'avait été adoptée qu'après que le

47 Cf. section 3.8.
48 Cf. section 3.4.4.
49 Hessische Datenschutzgesetz, 7 octobre 1970 (GVBl. I S. 625).

gouvernement du Land eut déjà commencé à informatiser le traitement de ses fichiers d'informations personnelles. Cette innovation conféra une visibilité particulière à cette loi, et contribua à la diffusion de la formule de « protection des données » (*Datenschutz*), qu'elle inaugurait et qui, de l'aveu même de Spiros Simitis, « n'est pas un joli mot »[50] mais est néanmoins devenu « le mot qui a été employé dans les autres langues[51] ».

Dans son contenu, la loi du Land de Hesse, qui ne s'appliquait encore qu'aux personnes morales de droit public relevant du droit hessois, obligeait ces dernières à « protéger » les données personnelles sous leur responsabilité, c'est-à-dire à s'assurer que seules des personnes autorisées y aient accès et puissent les manipuler. La loi prévoyait également un droit d'accès pour les individus aux données les concernant, et le droit d'exiger la rectification de données erronées. Enfin, et il s'agit là encore d'une innovation contenue par cette loi, elle crée la première autorité de protection des données au monde : le *Datenschutzbeauftragter*, ou Commissaire à la protection des données, chargé de contrôler son application et de rédiger des rapports publics sur le développement de l'informatique dans l'administration d'État.

Quatre facteurs d'explication permettent de comprendre la rapidité de l'adoption de cette loi en Hesse.

Le premier élément est bien sûr le contexte d'automatisation du traitement de l'information sur les personnes par les administrations publiques, dans un souci de rationalisation des politiques publiques, et en application d'un référentiel global de « progrès », de « modernité » et de « scientificité » qui n'est autre que celui qui, dans un autre champ de l'action de publique, l'agriculture, a conduit en France à de profondes réformes de la politique agricole, en faveur d'une industrialisation croissante et de la fin de la doctrine de maintien des paysans sur leurs terres (Müller, 1984).

Le deuxième élément est l'existence d'un autre référentiel voyant en l'ordinateur une menace pour les libertés individuelles. Ces personnes, parmi lesquelles Spiros Simitis, se sont dès lors intéressées aux travaux publiés sur le sujet aux États-Unis. Mais la controverse sur les fichiers informatisés de données personnelles, née aux États-Unis, dans un pays de *Common Law*, allait être reconfigurée une fois importée dans un contexte de culture juridique de droit continental.

En effet, le troisième élément d'explication de l'adoption rapide d'une loi est que le land de Hesse est un État de droit continental, où contrairement aux États-Unis, le pouvoir judiciaire ne pouvant pas créer de droit nouveau, il est moins fréquent de s'en remettre à la jurisprudence

50 Traduction libre de : « is not a nice word » (entretien avec Spiros Simitis).

51 Traduction libre de : « it is the word which was used then in the other languages too » (entretien avec Spiros Simitis).

pour régler des problèmes publics émergents, et plus fréquent de s'en remettre à la loi. Ce point a été soulevé, comme nous le reverrons[52], dans plusieurs entretiens, dont celui avec Spiros Simitis :

> « Les Américains ne réagissent habituellement pas rapidement par une loi, et s'appuient d'abord et surtout sur les décisions des tribunaux. En Europe, c'est différent. Nous nous appuyons sur les décisions des tribunaux, dont l'une des plus importantes est celle de la cour constitutionnelle allemande, mais nous réfléchissons en même temps à la Loi[53]. » (Entretien avec Spiros Simitis)

Enfin, le quatrième élément, qui semble avoir fourni aux partisans de la *Datenschutz* en Hesse un argument juridique de poids, a été une décision de 1969 du Tribunal constitutionnel fédéral de RFA, qu'évoque Spiros Simitis dans l'extrait d'entretien ci-dessus : l'arrêt *Mikrozensus*[54].

Dans cet arrêt, le Tribunal constitutionnel fédéral a en effet considéré qu'il était irréconciliable avec le principe de dignité de la personne humaine (*Würde der Menschen*) que l'État force des personnes à dévoiler *tous*[55] les aspects de leur personnalité, pour être consignés dans un fichier de données, et ce, même à des finalités d'enquêtes statistiques anonymisées :

> « Il est incompatible avec la dignité humaine que l'État puisse revendiquer pour lui-même le droit d'enregistrer et de cataloguer de manière obligatoire l'être humain dans toute sa personnalité, même dans l'anonymat d'une enquête statistique, et de le traiter ainsi comme un objet accessible à tous égards à un inventaire[56]. » (BVerfG, 16 juillet 1969 – 1 BvL 19/63, « Mikrozensus »)

Les juges de Karlsruhe poursuivent dans leur arrêt en justifiant l'interdiction d'une telle intrusion par le droit au développement libre et à l'auto-détermination de la personne ; nous

52 Cf. section 3.7.

53 Traduit de l'anglais. Texte original : « The Americans do not usually quickly react with a law, and rely first and essentially upon the court decisions. We, in Europe, it's different. We rely on the court decisions, and one the most important decisions is the decision of the German constitutional court, but at the same time we're thinking of the law »

54 BVerfG, 16 juillet 1969 – 1 BvL 19/63, « Mikrozensus »

55 Cette précision est importante. En l'espèce, le Tribunal constitutionnel fédéral n'a en effet pas considéré que l'enquête contre laquelle était dirigée la requête ne constituait pas une intrusion dans la vie privée

56 Traduit de l'allemand par Nebiha Guiga. Texte original : « Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist »

retrouvons encore une fois l'inspiration libérale utilitariste décrite en détail par Colin Bennett (Bennett, 1992 ; Bennett et Raab, 2003), cette fois dans le cas de la jurisprudence allemande.

Cette décision du Tribunal constitutionnel fédéral a fourni un argument de poids à Spiros Simitis et aux défenseurs de la vie privée de Hesse. En effet, elle leur a permis d'avancer l'argument selon lequel leur projet de loi était indispensable pour que les projets d'informatique d'État soient conformes aux constitutions tant fédérale que hessoise[57].

En 1974, le land de Rhénanie-Palatinat adopta à son tour une loi « contre l'usage abusif de données[58] » dont l'abréviation officielle est « Loi du Land de protection des données » (*Landesdatenschutzgesetz*). Puis, au niveau fédéral, un projet de loi de protection des données vit le jour en 1972, mais il fallut attendre 1977 pour qu'une telle loi soit adoptée (Kilian, 2010, p. 83). Enfin, en 1983, la Cour constitutionnelle fédérale de RFA, amenée à se prononcer sur la constitutionnalité d'une loi sur le recensement de la population (arrêt *Volkszählungsurteil*), proclama l'existence d'un droit à « l'auto-détermination informationnelle » (*informationelle Selbstbestimmung*[59]).

Cet arrêt de 1983, bien qu'il paraisse *a priori* bien proche de l'arrêt *Mikrozensus* de 1969, marqua toutefois une évolution, car il amena les juges de Karlsruhe à proclamer un droit général à l'auto-détermination *informationnelle*. Là où, dans *Mikrozensus*, il n'était encore question que d'un droit général à l'auto-détermination qui devait protéger l'individu contre l'intrusion de l'État dans sa vie privée, le Tribunal constitutionnel de RFA inventa dans *Volkszählungsurteil* une nouvelle catégorie de droit spécifique aux données personnelles, que seul un intérêt public supérieur peut venir contredire :

> « Dans les conditions du traitement moderne des données, la protection de l'individu contre la collecte, le stockage, l'utilisation et la divulgation illimités de ses données personnelles est assurée dans le cadre du droit général de la personnalité, à savoir l'article 2 paragraphe 1 de la Loi fondamentale en relation avec l'article 1 paragraphe 1 de la Loi fondamentale. À cet égard, le droit fondamental garantit le droit de l'individu de décider lui-même de la divulgation et de l'utilisation de ses données personnelles.
>
> Les restrictions de ce droit à l'« autodétermination informationnelle » ne sont autorisées que pour garantir un intérêt général majeur. Elles nécessitent une base juridique conforme à la constitution, qui doit respecter l'exigence constitutionnelle de la clarté des normes.

57 La dignité de la personne humaine était, et est toujours, protégée à l'article 3 de la Constitution de 1946 du Land de Hesse

58 Landesgesetz gegen mißbräuchliche Datennutzung vom 24. Januar 1974, GVBl. S. 31

59 Décision du Tribunal constitutionnel fédéral allemand BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil)

> Dans les mesures qu'il adopte, le législateur doit aussi respecter le principe de proportionnalité. Il doit également prendre des précautions d'ordre organisationnel et procédural pour parer au risque de violation du droit des personnes[60]. » (extrait du dispositif de l'arrêt « Volkszählungsurteil » du 15 décembre 1983)

L'arrêt *Volkszählungsurteil* contribua de la sorte à détacher le droit *à la* protection des données de la notion de droit *à la* vie privée en la raccrochant à un autre principe fondamental, nouveau : l'« auto-détermination informationnelle », selon lequel la légitimité de traitements de données à caractère personnel doit être (en principe) fondée sur le consentement de la personne concernée. Bien que la protection de la sphère de la vie privée soit régulièrement citée dans l'arrêt pour justifier le droit à l'auto-détermination informationnelle, ce dernier ne porte pas que sur des données dont il serait *a priori* possible, comme dans *Mikrozensus*, de dire qu'elles n'appartiennent pas à cette sphère du privé. Il porte au contraire sur toutes les données à caractère personnel pouvant être rattachées à une personne physique ; à elle ensuite – sauf exception prévue par la loi – de décider souverainement si elle accepte ou non de la partager. Cette évolution est entre autres justifiée, selon les juges qui ont rédigé l'arrêt, par l'impossibilité de déterminer à l'avance si de telles données sont ou non des données sensibles étant donné les capacités de conservation et de croisement permises par l'informatique[61]. Mais surtout, à travers le mécanisme du consentement, une large marge de manœuvre est conférée à l'individu dans son choix de partager ou non une information à caractère personnel, ce qui est conforme aux conceptions libérales de la « vie privée ».

De nombreuses lignes de l'arrêt *Volkszählungsurteil* sont en effet dédiées à la justification de ce nouveau droit. Il y est expliqué que la collecte informatisée d'informations personnelles par l'État peut mettre en péril le droit général à l'auto-détermination fondé sur le principe de dignité de la personne humaine, en influençant les individus dans leurs comportements et en exerçant une pression psychologique sur eux. Nous retrouvons donc dans cet arrêt une trace de l'inspiration libérale utilitariste, puisque que, *in fine*, c'est bien la sphère de l'autonomie individuelle défendue par John Stuart Mill qu'il s'agit de protéger.

---

60 Traduit de l'allemand par Nebiha Guiga. Texte original : « Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. »

61 Voir notamment le paragraphe 159 de l'arrêt.

Notons enfin que le Tribunal de Karlsruhe imposa en 1983 le respect d'un certain nombre de règles, comme la limitation des finalités (point 162 de l'arrêt), qui sont identiques aux règles contenues dans la Convention 108 du Conseil de l'Europe, adoptée deux ans plus tôt, et qui allait être ratifiée par la RFA en 1985 (ce qui explique qu'en 1983, le Tribunal n'y fasse pas encore de référence directe). Ceci est une exemple supplémentaire allant dans le sens de ce qu'affirme Colin Bennett (Bennett, 1992) lorsqu'il écrit que les circonstances nationales d'adoption de règles juridiques nationales, qu'elles soient, d'ailleurs, de nature jurisprudentielle comme ici pour l'auto-détermination informationnelle, ou législatives comme dans ce sous-chapitre pour les lois de protection des données, n'ont eu que peu ou pas d'influence sur le contenu concret de celles-ci. Nous reviendrons dans le prochain sous-chapitre sur le rôle du Conseil de l'Europe et de l'OCDE dans cette harmonisation précoce des règles de protection des données.

3.3.3. Les Pays-Bas

Comme en Allemagne, le recensement, et son informatisation, ont provoqué aux Pays-Bas des réactions inquiètes pour la garantie du droit *à la* vie privée. La particularité de ce pays est la politisation précoce de la question dans l'espace public et les mouvements sociaux. Pour le comprendre, il faut revenir brièvement sur l'histoire du recensement dans ce pays.

Entre 1829 et 1971, les Pays-Bas ont connu quatorze recensements décennaux avant qu'en 1980, le dernier soit reporté puis finalement annulé au profit de méthodes alternatives d'enquêtes statistiques (Holvast, 2013, p. 12). Le tout premier recensement avait pour but de connaître le nombre d'habitants, au niveau du pays, mais également par province et par commune, ainsi que la répartition de la population entre hommes et femmes, la profession des habitants, et leur religion (Holvast, 2013, p. 34). Petit à petit, les informations demandées devinrent de plus en plus précises : si, au début, par exemple, seul l'âge de chaque habitant était demandé par les agents chargés du recensement, petit à petit, au cours du XX^{e} siècle, ces derniers ont demandé l'année de naissance, puis l'année et le jour. Alors qu'en 1829, le choix des religions était limité à catholique, protestant, juif ou autre, à la fin du XIX^{e} siècle, chaque habitant se vit présenter une liste de 19 religions parmi lesquelles il devait indiquer la sienne (Holvast, 2013, p. 34). Le Bureau central des statistiques (*Centraal Bureau voor Statistiek*) fut créé le 9 janvier 1899 pour être en charge du recensement décennal.

En 1960, pour la première fois, les cartes perforées représentant chacune un individu ne furent plus traitées avec des machines de Hollerith, mais avec un ordinateur électronique. Le fichier du recensement contenait cette année-là 11,5 millions de cartes perforées, et les cas de refus de répondre au questionnaire du recensement demeurèrent marginaux cette année-là (Holvast, 2013, p. 43).

Ce n'est que le 15 septembre 1970 que fut créée une association, le Comité de vigilance sur le recensement (*Comité Waakzaamheid Volkstelling* – CWV), pour protester contre l'organisation du recensement décennal prévu l'année suivante. Cette association était proche des milieux « *provo* », des groupes intellectuellement proches de ceux qui ont contribué en France à Mai 68. La motivation derrière la création de cette association fut expliquée par Peter Muijlwijk, l'initiateur du projet, dans une interview donnée le 27 octobre 1970 au quotidien *NRC Handelsblad* :

> « J'ai – par hasard – passé un an à retranscrire à la machine un manuscrit de Weinreb et fut de nouveau confronté au pouvoir des listes et des papiers, qui conduisirent des milliers de personnes en Allemagne pendant la guerre. J'ai été impressionné par la possibilité offerte à l'administration de tuer des gens[62]. » (Muijlwijk, 1970, cité par : Holvast, 2013, p. 94)

Selon Jan Holvast, l'informatisation du recensement ne semble donc pas avoir représenté d'élément déclencheur de la mobilisation contre le recensement, mais une circonstance aggravante qui l'a exacerbée, dont la réglementation de l'usage fut l'une des revendications centrales du CWV.

En entretien, Peter Hustinx souligna dès la première question le rôle de cette défiance de la population vis-à-vis du recensement, et le refus d'une proportion importante d'entre elle d'y participer, dans la mise à l'agenda de la question de la protection de la vie privée vis-à-vis des fichiers de personnes, au sein du gouvernement dirigé par Barend Biesheuvel, de tendance chrétien-démocrate, et du ministère de la justice, dirigé par Dries van Agt. Dans la préface qu'il rédigea au livre de Jan Holvast sur la réaction au recensement de 1971, Jacob Kohnstamm, qui fut de 2004 à 2016 président de l'autorité néerlandaise de protection des données, se souvint des événements en ces termes :

> « Au début de mes études, en 1971, je me suis interrogé sur la protection de la vie privée dans le cadre du recensement. Comme environ 250 000 autres personnes, j'ai répondu absent lorsque les formulaires distribués furent recueillis[63]. » (Jacob Kohnstamm, dans : Holvast, 2013, p. 9)

62 Traduction de l'auteur. Texte original : « Ik heb – toevallig – een jaar lang het met de hand geschreven manuscript van Weinreb uitgetypt en werd aldus geconfronteerd met de macht van lijsten en papieren, aan de hand waarvan duizenden in de oorlog naar Duitsland wereden gestuurd. Ik raakte onder de indruk van de mogelijkheden om mensen administratief te vermoorden. »

63 Texte d'origine : « Als beginnend student zette ik in 1971 ook mijn vraagtekens bij het waarborgen van de privacy rond de volkstelling. Net als zo'n 250 000 anderen gaf ik niet thuis toen de formulieren werden opgehaald. »

En définitive, seules 22 400 personnes ont refusé de remplir le formulaire de recensement, et environ 246 000 personnes auraient fourni de fausses informations (Holvast, 2013, p. 395), sur une population qui compte alors autour de 13 millions de personnes[64]. La médiatisation de l'affaire, et le fait que des manifestations aient eu lieu en soutien aux personnes qui ont refusé de prendre part au recensement, permettent aisément d'imaginer qu'un grand nombre de personnes aient donné des renseignements erronés. Cela a donné, nous le verrons, un argument empirique de poids à ceux qui, à partir de la fin des années 1960, mobilisèrent l'argument selon lequel des lois de protection des données étaient nécessaires pour que les citoyens prennent « confiance » en l'informatique.

En 1972, sur le modèle suédois, un comité fut mis en place par le gouvernement néerlandais pour formuler des propositions de réglementation de l'informatique afin de protéger la vie privée des citoyens ; il s'agit de la commission Koopmans (*Staatscommissie-Koopmans*), prévue par le décret royal n° 70 du 21 février 1972, et inaugurée le 16 mars de la même année. Elle fut assistée par un secrétariat dirigé par Michel Scheltema, et composé de Dirk Ravestijn, du ministère de l'Intérieur, Pieter Jan Hustinx (qui a choisi d'être connu sous le nom de Peter Hustinx), du ministère de la Justice, et Jan Niçaise, du ministère de l'Économie (Conseil de l'Europe, EXP/Prot.Priv. (74) 3). Michel Scheltema et Dirk Ravestijn furent envoyés dès la première réunion du Groupe d'experts du Conseil de l'Europe sur la protection de la vie privée dans les communications électroniques (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 5 Rév), et Peter Hustinx dès la troisième réunion, en novembre (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 17). En janvier 1974, le rapport de cette commission aboutit à la conclusion qu'il fallait légiférer (Conseil de l'Europe, EXP/Prot.Priv. (74) 3, p. 8). Malgré cela, il fallut cependant attendre le 28 décembre 1988 pour que soit promulguée au journal officiel du Royaume des Pays-Bas une loi de protection des données[65].

3.3.4. La Suède

Le point de départ de la réflexion institutionnelle sur la protection des données à caractère personnel fut différent en Suède.

Comme aux États-Unis, l'image ambivalente et angoissante de l'ordinateur a joué un rôle dans la façon dont fut problématisé le rapport entre informatique et vie privée en Suède. Lars Ilshammar a ainsi montré que progressivement, à partir du milieu des années 1960, alors que

64 Selon les chiffres d'Eurostat : jeu de données « Population change - Demographic balance and crude rates at national level (demo_gind) » disponible en ligne sur la page https://ec.europa.eu/eurostat/en/web/population-demography-migration-projections/data/database (page consultée le 20 décembre 2018).

65 Wet van 28 december 1988, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties. *Staatsblad van het Koninkrijk der Nederlanden*, n° 665, p. 1.

l'ordinateur devenait une machine utilisée par l'État, son image auprès des parlementaires passa d'un outil inoffensif au seul usage de calcul mathématique, à celle d'un machine bureaucratique au service du contrôle rationalisé de la population (Ilshammar, 2007). Mais un autre facteur, spécifique aux traditions constitutionnelles et administratives suédoises, contribua dans ce pays à la problématisation du rapport entre informatique, données et droit à la vie privée.

Le principe de libre-accès aux documents administratifs[66] remonte en effet en Suède à une loi sur la liberté de la presse de 1766[67]. L'introduction d'un numéro d'identification personnel en 1947, couplée à une informatisation des fichiers sur les individus détenus par l'État dès 1963 (Bennett, 1992, p. 47) ainsi qu'au principe de libre-accès à ces informations détenues par l'administration, a entraîné des craintes quant à la confidentialité de données pouvant contenir des informations sur la vie privée des personnes. Lors de son intervention au colloque sur la protection des données organisé en 1974 à Vienne par l'OCDE, Jan Freese, qui travaillait alors pour la *Datainspektionen*, l'autorité de protection des données, revint sur cet élément déterminant dans le contexte suédois :

> « La loi sur la liberté de la presse favorise l'ouverture et le libre-accès, alors que la loi suédoise sur la protection des données protège les libertés individuelles. » (Källner et Freese, 1974, p. 69)

Les données récoltées lors des recensements firent, comme aux Pays-Bas, l'objet d'une attention particulière. La commission parlementaire mise en place en 1969 sur le sujet rendit ses conclusions en 1972, et dès 1973, la Suède adopta la première loi *nationale* de protection des données à caractère personnel, évoquée par Jan Freese dans l'extrait ci-dessus (Flaherty, 1989, p. 94-98). La *Datalag* de 1973[68], qui a été essentiellement rédigée par Jan Freese (Gassman, 2010, p. 6 , cité par : González Fuster, 2014, p. 58), s'inspira de celle de Hesse pour la création d'une autorité en charge de veiller à son application, et surtout, chargée d'autoriser les nouveaux traitements de données à caractère personnel. Si le terme utilisé pour désigner le but de cette loi, qui est le mot suédois « *integritet* » (intégrité) au lieu d'une traduction du terme allemand « *Datenschutz* », au-delà de différences terminologiques, il est difficile trouver des différences de fond dans le contenu et les objectifs de cette loi de celui de la loi de Hesse (Bennett, 1992, p. 27).

L'adoption de cette loi est aussi à inscrire dans un contexte plus vaste de réforme constitutionnelle en cours, avec l'adoption d'une nouvelle constitution en 1974. Hans Corell, qui

66 En suédois : « *offentlighetsprincip* », ou principe d'ouverture
67 Tryckfrihetsförordning som utfärdades den 2 december 1766 (Suède)
68 Datalag (1973:289) (Suède)

participa à des négociations tant au Conseil de l'Europe qu'à l'OCDE, nous le rappela en entretien :

> « Vous voyez, nous élaborions également à cette époque une nouvelle constitution en Suède, qui est entrée en vigueur en 1974. Il y avait donc beaucoup d'activité dans ce domaine[69]. » (Entretien avec Hans Corell)

Ce contexte de développement du droit constitutionnel, notamment dans le domaine des droits et libertés fondamentales, n'est pas sans rappeler ce qui se passait ailleurs en Europe. L'année 1973 fut celle des accords d'Helsinki, un traité international signé par des pays des deux blocs, comportant notamment un chapitre sur les droits fondamentaux. En Allemagne de l'Ouest, en 1974, alors que la Suède adoptait une nouvelle constitution, le Tribunal constitutionnel fédéral entrait dans un bras de fer avec la CJCE en affirmant qu'il se permettrait de censurer toute mesure de droit communautaire contraire aux droits et libertés fondamentales tant que ce droit ne garantissait pas un niveau de protection similaire à celui offert par la Loi fondamentale de RFA[70]. Ce contexte de progression de la protection juridique des droits et libertés fondamentales s'étendit même à certains pays du bloc de l'Est. En Hongrie, la réforme du code civil de 1977 introduisit ainsi plusieurs nouveaux droits dans le Code civil hongrois[71].

Un contexte similaire s'observait alors en France pendant la décennie des années 1970, avec la réforme du Code civil de 1970, la ratification sous l'interim du président Alain Poher de la Convention européenne des droits de l'Homme en 1974[72], et surtout, l'affirmation du rôle du Conseil constitutionnel au début de cette décennie en matière de contrôle du respect des droits et libertés fondamentales[73].

---

69 Traduit de l'anglais. Texte original : « You see, we also elaborated a new constitution in Sweden in those days, which entered into force in 1974. So there was a lot of activity in this field. »

70 BVerfGE, 29 mai 1974, 37, 271 - « Solange I ».

71 Loi IV de 1977 amendant la loi IV de 1959 sur le Code civil de la République populaire de Hongrie (*1977. évi IV. törvény a Magyar Népköztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény módosításáról és egységes szövegéről*).

72 Pour être plus précis, cette ratification de la CEDH, vingt-deux ans après sa signature, est intervenue en deux temps. D'abord une loi autorisant la ratification fut adoptée le fin 1973 (loi 73-1227 du 31 décembre 1973), puis Alain Poher, président du Sénat, exerçant les fonctions de président de la République par interim suite au décès de Georges Pompidou, signa le 3 mai 1974 le décret n° 74-360 portant publication de la CEDH au Journal officiel (voir : JORF du 4 mai 1974, pages 4750 et suivantes).

73 Voir la décision n° 71-44 DC du 16 juillet 1971, dans laquelle, pour la première fois, le Conseil constitutionnel français opéra un contrôle du respect par le législateur de droits et libertés fondamentales.

3.3.5. La France

En France, le gouvernement commanda au Conseil d'État un rapport sur « les conséquences du développement de l'informatique sur les libertés publiques et sur les décisions administratives » dès 1969 (Conseil d'État (France), 1970). En 1970, la loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens créa un article 9 dans le code civil affirmant le droit des individus au respect de leur vie privée. Au cours de la première moitié de la décennie, une série de propositions de lois furent déposées par des députés français, dont, en octobre 1970, une proposition de Michel Poniatowski[74], député de la Fédération nationale des républicains indépendants, dirigée par le président Valéry Giscard d'Estaing. Sa proposition visait notamment à créer un « Comité de surveillance de l'informatique » (González Fuster, 2014a, p. 63).

Tant André Vitalis[75] que Marie Georges[76] ont en outre insisté en entretien sur l'absence de médiatisation et de politisation, à leurs yeux, de l'informatique et des fichiers de données à caractère personnel jusqu'au milieu des années 1970, soit après les premières propositions formulées entre autres par Michel Poniatowski, et après la rédaction du rapport, dans un premier temps confidentiel, que le Conseil d'État avait transmis au gouvernement en 1970 (Conseil d'État (France), 1970).

Ce n'est semble-t-il qu'en 1974, avec un article de Philippe Boucher (Boucher, 1974) dans *Le Monde* sur le projet de « Système automatisé pour les fichiers administratifs et le répertoire des individus » (ou projet SAFARI), que la question des conséquences de l'informatique sur les droits et libertés individuelles, dont le droit à la vie privée, furent mises à l'agenda médiatique. Cette affaire provoqua des réactions dans des milieux proches de la CFDT et du Syndicat de la Magistrature, puis dans la presse, dans un contexte politique encore proche des événements de Mai 68. Marie Georges raconta ainsi la façon dont elle s'intéressa au lien entre informatique et libertés, puis à la façon dont elle était entrée en contact avec Louis Joinet, du Syndicat de la Magistrature, et Philippe Lemoine de la CFDT :

> « Un, je suis une soixante-huitarde. Donc ça ça vous donne le lien avec les questions de libertés et de société […]. Quand fin 72 je rentre en France de Madagascar, je revois mes amis, et l'un d'eux est au CEPIA, qui est […] le premier centre de formation professionnelle créé dans le cadre du plan Calcul […], Philippe Lemoine […] me propose

74 Proposition de loi n° 1454 de la IVe législature de la Ve République de l'Assemblée nationale

75 Auteur d'une thèse sur l'informatique, le pouvoir et les libertés, André Vitalis (1988), l'un des co-fondateurs de la revue *Terminal*, fut consultant auprès de la CNIL à la fin des années 1980 et côtoya nombre de ses fondateurs.

76 Marie Georges fut longtemps cheffr de la division des affaires européennes, internationales et de la prospective de la CNIL. Avant cela, elle milita dans les mêmes réseaux qu'André Vitalis, Philippe Lemoine, Louis Joinet ou encore Philippe Bouchard en faveur de l'adoption d'une loi de protection des données en France. Elle fut une des négociatrices de la directive 95/46/CE au début des années 1990.

de venir travailler au CEPIA. […] Philippe, moi, et quelques autres, on concevait les formations […]. On devait recruter des gens et les transformer en formateurs. […] On a eu [comme formateurs] des chefs de projet de l'administration. Et c'est là qu'on a appris tous les projets d'informatisation, notamment SAFARI » (entretien avec Marie Georges)

« À l'INRIA, Philippe et moi, on apprend l'existence de tous ces fichiers, et c'est ça qui nous frappe : c'est que personne […] ne connaît l'existence de ces projets ou des fichiers qui existent déjà. […] On se dit : qui […] pourrait être un relais sur ces questions ? Nous on était scotchés. […] On a tout de suite compris le problème de démocratie. Si on est envahis à nouveau, ou qu'on a un régime autoritaire, qu'est-ce qu'ils vont faire de ces données ? […] La seule organisation qui s'y intéresse : il va y avoir un congrès du Syndicat de la magistrature qui parle de fichiers. Or, il se trouve que j'ai une amie, très proche, qui est en train de faire un stage de magistrate dans le bureau du fondateur, qui est Louis Joinet. Donc on fait venir Joinet, et c'est parti ! […] C'était en 73 » (entretien avec Marie Georges)

Puis, ce fut le projet de fichier GAMIN (Gestion automatisée de médecine infantile) qui suscita des mobilisations à son encontre au milieu des années 1970, notamment parmi les médecins et les assistants sociaux qui devaient alimenter le fichier en données de santé, en violation du traditionnel principe du secret médical (Vitalis, 1988, 2010) :

« Il y avait un collectif, pour GAMIN. Peut-être la seule manifestation centrée sur le fichage a eu lieu à Nantes à cette époque. On n'était pas nombreux. […] Là y avait un collectif extrêmement fort, parce que les assistants sociaux avaient eu une lutte très forte avec le Conseil général » (Entretien avec André Vitalis)

André Vitalis insista aussi sur le rôle de l'image qu'avaient les ordinateurs dans les années 1970. Cette image inquiétante de l'ordinateur, dont nous avons déjà vu le rôle qu'elle a joué dans les années 1960 aux États-Unis[77], est aussi reprise par la presse française, par exemple par Philippe Boucher dans son article de 1974 sur le projet SAFARI, ou encore Hélène Vida, présentatrice du Journal d'Antenne 2 en juillet 1976 :

« Puissant, cet Iris-80, une comparaison le démontre sans contestation. L'appareil employé pour engranger les données de l'opération Safari, qui concerne l'identification individuelle de l'ensemble des 52 millions de Français, a une contenance de 2 milliards

77 Cf. section 3.2.3.

d’octets. Celle de l’ordinateur du ministère de l’intérieur est de 3,2 milliards d’octets. » (Boucher, 1974)

« Dans l’absolu, on peut affirmer que la liberté naît de la connaissance. Mais quand il s’agit des ordinateurs, ces robots du renseignement, c’est l’inverse qui se produit et la liberté du citoyen est en péril » (Vida, 1976)

Reprenons notre chronologie. Le mois suivant la parution de l’article de Philippe Boucher sur l’affaire SAFARI, Alain Poher devint président de la République par intérim suite à la suite du décès de Georges Pompidou, avant que ne soit élu, le 19 mai, Valéry Giscard d’Estaing à la présidence de la République. Jacques Chirac fut nommé premier ministre, et Michel Poniatowski, dont nous avons vu qu’il avait déjà proposé quelques années plus tôt une loi pour réglementer l’usage de bases de données personnelles informatisées, devint ministre de l’Intérieur. Le 8 novembre, un décret[78] signé par Valéry Giscard d’Estaing créée, sous l’autorité de Jean Lecanuet, ministre de la Justice, une commission « Informatique et Libertés », présidée par Bernard Chenot, alors vice-président du Conseil d’État. L’IRIA, ancêtre de l’INRIA, est associée aux travaux, de même que Louis Joinet.

Le rapport de cette commission fut rédigé par Bernard Tricot, son rapporteur, et remis en juin 1975. Il se termine par une série de propositions, dont celle de créer, comme en Hesse et en Suède, une autorité indépendante capable d’exercer un contrôle sur l’utilisation de l’informatique, d’abord et surtout par des personnes morales de droit public, mais également, dans une certaine mesure, par le secteur privé (Tricot, 1975, p. 89). D’autres mesures proposées, comme celle d’imposer un « principe de finalité » (Tricot, 1975, p. 90), sont inspirées des « *Fair Information Principles* » et de ceux proposés au groupe d’expert du Conseil de l’Europe par la délégation britannique en 1972 (Conseil de l’Europe, EXP/Prot.Priv./EDB (72) 5).

Les conclusions du rapport furent reprises dans un projet de loi[79]. Louis Joinet, dans une audition par une mission d’information du Sénat le 18 mars 2014, rappela que c’est à lui que fut confié la rédaction du projet, à la Direction des affaires civiles du ministère de la Justice :

« Le début de ma carrière remonte à 1964. À l'époque, j'étais expert auprès du Conseil de l'Europe. J'ai consacré vingt ans de ma vie à la protection des données. J'étais chargé, à la Direction des affaires civiles, de rédiger techniquement la loi « Informatique et Libertés ». » (Joinet, 2014)

78 Il s’agit du Décret n° 74-938 du 8 novembre 1974 portant création de la commission informatique et libertés
79 Projet de loi n° 2516 de la Ve législature de la Ve République

Louis Joinet participait, pendant la même période, aux groupes d'experts de l'OCDE et du Conseil de l'Europe qui allaient rédiger des textes qui allaient devenir, en 1980 et 1981, les Lignes directrices régissant la protection de la vie privée, et la Convention 108. De fait, à part pour la loi de Hesse, les premières lois nationales de protection des données des années 1970 étaient très fortement inspirées par le contenu des discussions dans ces arènes intergouvernementales, faisant de ces dernières le centre de la prise de décisions. C'est en leur sein que se structura la « *privacy community* » qui joua un si grand rôle non seulement dans les années 1970, mais aussi dans l'adoption de la directive européenne de protection des données de 1995 et dans la structuration de la coalition de cause des défenseurs de la vie privée pendant la réforme de cette dernière entre 2009 et 2016[80].

3.4. Le rôle du Conseil de l'Europe et de l'OCDE

3.4.1. Rappels sur le choix des terrains

Comme nous l'avions vu dans le premier chapitre[81] et comme nous venons de le rappeler l'OCDE et le Conseil de l'Europe ont joué un rôle central dans la coordination de la rédaction des premières lois nationales de protection des données, par la constitution de « groupes d'experts » regroupant bon nombre des hauts fonctionnaires qui, dans leurs pays, ont œuvré à l'invention des principes que celles-ci contiennent. C'est ce qui explique la surprenante cohérence dans le contenu de différentes lois nationales adoptées apparemment indépendamment les unes des autres dans plusieurs pays de l'Ouest au cours de la décennie 1970.

Nous commencerons par présenter le groupe d'experts que nous avons étudié au niveau du Conseil de l'Europe : le groupe d'experts sur la protection de la vie privée vis-à-vis des banques de données électroniques, qui rédigea en 1973 et 1974 les deux premiers documents internationaux de référence en matière de protection des données sous forme de résolutions du Comité des ministres du Conseil de l'Europe. Ce même groupe fut chargé de la rédaction du brouillon de la Convention 108. Ensuite, nous présenterons les groupes de travail successifs qui, à l'OCDE, entre 1970 et 1980, ont étudié le rapport entre informatique et protection de la vie privée, en nous concentrant sur le groupe d'experts chargé entre 1978 et 1980 de proposer des lignes directrices qui furent finalement adoptées en 1980, l'année même où le Conseil de l'Europe acheva la rédaction de la Convention 108, signée par ses États Membres début 1981.

80 Cf. chapitre 4.
81 Cf. section 1.2.3.1.

Ajoutons avant de présenter ces arènes et leur chronologie, qu'en cours de recherche, les documents d'archives étudiés et les entretiens réalisés nous ont conduits à nous intéresser, en raison des nombreuses références que nous y avons trouvées, à des travaux et des publications réalisés aux États-Unis au cours de la décennie précédente. Si nous n'avons intégré ces sources et ces références à notre analyse que dans la mesure où elle nous ont permis d'éclairer les corpus correspondant à nos terrains de l'OCDE et du Conseil de l'Europe, leur importance, leur richesse et leur relative complexité expliquent pourquoi il leur a été accordées d'assez longs développements en section 3.2.

3.4.2. Le groupe d'experts sur la protection de la vie privée vis-à-vis des banques de données électroniques du Conseil de l'Europe

En 1967, la Commission internationale des juristes organisa à Stockholm la Conférence nordique sur le droit à la vie privée (« *Nordic Conference on the Right to Privacy* »). Cette conférence, régulièrement citée dans les travaux de l'époque, joua un rôle dans la mise à l'agenda, dans les milieux juridiques européens, de la réflexion sur le droit à la vie privée (González Fuster, 2014a, p. 39). Il n'y a toutefois pas été question d'informatique, ni d'ailleurs de technologie, ce qui fut d'ailleurs pointé du doigt dans des travaux postérieurs qui se sont inspirés des conclusions de la conférence (González Fuster, 2014a, p. 40).

Peu après, le 31 janvier 1968, l'Assemblée parlementaire du Conseil de l'Europe adopta une résolution[82] s'inquiétant des risques que certaines nouvelles techniques, comme les écoutes téléphoniques, faisaient peser sur le droit à la vie privée. Cette résolution ne mentionnait pas l'informatique, mais appelait néanmoins le Comité des ministres à charger un comité d'experts de « procéder à une étude et de faire rapport sur la question de savoir si, eu égard à l'article 8 de la Convention des Droits de l'Homme, la législation nationale des États membres protège suffisamment le droit au respect de la vie privée contre les violations qui peuvent être commises par l'emploi des méthodes scientifiques et techniques modernes » et, si besoin, à « formuler des recommandations tendant à une meilleure protection du droit au respect de la vie privée » (Recommandation 509 (68) de l'Assemblée parlementaire du Conseil de l'Europe). Cette résolution fut notamment inspirée par la lecture des travaux d'Alan Westin, cité dans les travaux parlementaires en ayant précédé l'adoption (González Fuster, 2014a, p. 83).

En mars, les délégués des ministres composant le Comité des ministres du Conseil de l'Europe décida de donner suite à cette résolution de l'Assemblée parlementaire. Le rapport, rédigé par le secrétariat du Conseil de l'Europe, note en effet que « la menace [à la vie privée]

82 Recommandation 509 (1968) de l'Assemblée parlementaire du Conseil de l'Europe : « Droits de l'Homme et réalisations scientifiques et technologiques modernes »

née des appareils techniques modernes est commune à la plupart, sinon tous les États membres[83] ».

La mission fut confiée au comité d'experts en matière de droits de l'Homme, qui remit son rapport le 18 novembre 1970 (Conseil de l'Europe, DH/Exp (70) 15[84]). Suite à cela, un sous-comité du Comité de coopération juridique (CCJ) fut mis en place, afin qu'il rédige des recommandations sur les actions à mener, sur la base de ce premier rapport.

Ce sous-comité tint une réunion à Strasbourg du 11 au 13 octobre 1971. Deux documents, figurent parmi ceux qui lui avaient été préalablement soumis en vue de préparer la réunion :

- Un projet de convention internationale rédigé par l'Union internationale des avocats (Conseil de l'Europe, CCJ/Prot.Priv. (71) 1) ;
- Le document d'information rédigé par la Direction des affaires juridiques du secrétariat du Conseil de l'Europe (Conseil de l'Europe, CCJ/Prot.Priv. (71) 6).

Le premier document, le projet de convention, couvre à la fois la protection de la vie privée des personnes physiques et celle des personnes morales, et une part non négligeable y est dédiée à la question de la protection de la vie privée vis-à-vis des banques de données électroniques.

Le second document est un point d'information rédigé par le secrétariat pour préparer la réunion du sous-comité du CCJ. Il y est recommandé au sous-comité du CCJ de se concentrer sur le problème causé par l'informatique, prioritaire par rapport à la protection de la vie privée vis-à-vis des médias de masse et des appareils techniques autres que les ordinateurs :

> « After a preleminary examination, and taking into account the activities already undertaken by other international organisations, the Secretariat has identified as one of the subjects which would lend themselves to such a treatment, the problem of "data privacy", i.e. the registration and utilisation of private data by ultra-modern means (computers, etc.) for various purposes, some of which interfere with privacy[85]. » (Conseil de l'Europe, CCJ/ Prot.Priv. (71) 6, p. 6)

83 Il s'agit d'une traduction à partir de la version anglaise du compte-rendu, la version française n'étant pas disponible dans les archives en ligne du Conseil de l'Europe : « the threat arising from modern technical devices is common to most if not all member states »

84 Ce document est cité par le document CCJ/Prot.Priv. (71) 6, page 2, mais nous ne sommes pas parvenu à y accéder.

85 Traduction de l'auteur : « Après examen préliminaire, et en tenant compte des activités déjà menées par d'autres organisations internationales, le Secrétariat a identifié comme sujet se prêtant à un tel traitement la question de la « vie privée des données », c'est-à-dire l'enregistrement et l'utilisation de données privées par des moyens ultra-modernes (ordinateurs, etc.) à différentes fins, dont certaines portent atteinte à la vie privée. »
Le texte original en anglais a été maintenu dans le corps du texte car la traduction apporte une perte de précision sémantique.

Cet avis fut suivi par le sous-comité du CCJ (Conseil de l'Europe, CCJ (71) 66, p. 4).

Un groupe d'experts fut alors mis en place : le groupe d'experts sur la protection de la vie privée vis-à-vis des banques de données électroniques, dont le nom fut plusieurs fois légèrement amendé entre 1973 et 1974[86], et dont la première réunion se tint du 13 au 15 mars 1972. Le secrétariat de ses réunions était assuré sous la direction de Frits Hondius. Ses travaux aboutirent en 1973 et 1974 à deux résolutions[87] du Conseil de l'Europe, adoptées en Comité des ministres :

- La résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé ;
- La résolution (74) 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public.

La première résolution, en 1973, contenait déjà les principes proposés un an plus tôt par la délégation britannique (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 5), et qui furent connus, sous une forme légèrement différente, comme les « *Fair Information Principles* » dans un rapport publié en 1973 aux États-Unis (Ware, 1973). Elle appelait au respect de ces principes pour toutes les « informations relatives aux personnes », puis précisait que ce terme de « personnes » était à entendre au sens de « personnes physiques », à l'exclusion, donc, des personnes morales comme les entreprises ou les associations. La seconde résolution, de 1974, et qui porte sur le secteur public, a mis plus de temps a être acceptée par le Comité des Ministres, mais toutes deux contiennent des principes et un champ d'application similaires.

Nous trouvons toutefois dans chacune la trace d'un débat autour du champ d'application de la protection des données : les principes de protection ne doivent-ils être respectés que lorsqu'un organisme public traite des données qui relèvent de la vie privée des personnes ? Ou bien quel que soit le contenu de la donnée, dès lors qu'il y a un lien entre cette donnée et une personne physique ? Ainsi, dans la résolution de 1973, nous pouvons lire que :

> « Les informations concernant l'intimité des personnes ou celles pouvant être à la source de discriminations ne doivent pas, en règle générale, être enregistrées, ou, du moins diffusées » (principe 1, résolution (73) 22 du Conseil de l'Europe)

86 Dans un document du 28 février 1973, nous pouvons ainsi lire qu'il s'agit d'un document destiné au « Sub-Committee of the CCJ charged with examining a draft resolution on the protection of privacy vis-à-vis electronic data banks in the private sector » (Conseil de l'Europe, CCJ/SC.Prot.Priv. (73) 2). Afin de rester succinct, et étant donné qu'il s'agit de changements lexicaux mineurs à chaque fois, qui n'affectent ni la composition, ni le fonctionnement du groupe d'experts, nous avons fait le choix de conserver, pour y faire référence, son nom initial de « groupe d'experts sur la protection de la vie privée vis-à-vis des banques de données électroniques », sur toute la période de 1972 à 1975.

87 Le terme de « résolution » indique que ces textes n'ont pas de valeur juridiquement contraignante. Leur incidence est donc plus politique que juridique.

Dans celle de 1974 :

> « Particulièrement lorsque des banques de données électroniques traitent des informations concernant l'intimité de la vie privée des personnes, ou lorsque le traitement des informations peut être à la source de discriminations,
>
> (a) leur création doit être prévue par la loi […] ;
>
> (b) ces lois […] doivent préciser leur finalité […] ;
>
> (c) les informations enregistrées ne doivent pas être utilisées à d'autres fins que celles qui ont été définies, à moins qu'une dérogation ne soit expressément autorisée par la loi, ou accordée par une autorité compétente [...] » (principe 3, résolution (74) 29 du Conseil de l'Europe)

Ces formulations semblent le fruit d'un compromis. L'extrait cité ci-dessus de la résolution de 1974 est d'ailleurs contredit par un autre extrait, qui impose le principe de limitation des finalités quelle que soit la nature des données en question :

> « Les informations enregistrées doivent être :
>
> *a.* obtenues par des moyens licites et loyaux ;
>
> *b.* exactes et tenues à jour ;
>
> *c.* adéquates et pertinentes par rapport à la finalité recherchée […] » (principe 2 de la résolution (74) 29 du Conseil de l'Europe)

Nonobstant ces menues incohérences dans les textes, nous voyons peu à peu prendre forme, dans des textes qui n'ont pas encore de valeur juridique contraignante mais qui sont déjà rédigés au niveau européen, un nouveau droit spécifique : le droit *de* la protection des données à caractère personnel, qui se constitutionnalisa par la suite pour devenir un droit *à la* protection des données à caractère personnel, et qui s'émancipe du strict cadre des données qui relèvent *a priori* de l'intime, de la « sphère privée ». Dès le moment où il fut décidé de définir le champ d'application des principes de la protection des données comme *toute* donnée à caractère personnel, et que le syntagme de « donnée à caractère personnel » fut délié de la notion de vie privée ou d'intimité, les bases de ce qu'Yves Poullet et Antoinette Rouvroy ont appelé une nouvelle génération de droit *à la* vie privée sont déjà fixées, près de dix ans avant la décision *Volkszählungsurteil* qu'ils prennent comme repère (Poullet, 2010 ; Rouvroy et Poullet, 2009). Nous aurons l'occasion d'y revenir dans le dernier chapitre de cette thèse en étudiant les controverses autour de la notion de « donnée à caractère personnel ».

Confirmant les intuitions que Frits Hondius exprima dans un livre qu'il publia sur l'avènement du droit à la protection des données en 1975 (Hondius, 1975), tous les enquêtés interrogés à ce sujet ont insisté sur le fait qu'à cette date, c'est-à-dire une fois adoptées ces deux résolutions du Conseil de l'Europe, l'essentiel des débats sur les grandes définitions et les principes fondamentaux du droit des données personnelles furent clos[88].

Sur la base de ces acquis, le Conseil de l'Europe poursuivit son travail en créant en 1976 un Comité d'experts sur la protection des données (González Fuster, 2014a, p. 86). Si le nom du groupe est changé, et fait désormais directement référence au droit à la protection des données et non plus au droit à la vie privée, il se place dans la continuité parfaite du groupe d'experts sur la protection de la vie privée vis-à-vis des banques de données électroniques dont le nom, en 1975, s'était d'ailleurs raccourci en un « groupe d'experts sur la vie privée » (Conseil de l'Europe, EXP/Prot.Priv. (75) 6).

Ce groupe d'experts sur la protection des données fut chargé dès sa création en 1976 (OCDE[89], DSTI/ICCP/77.47, p. 42) de rédiger un projet de convention pour la protection des personnes à l'égard des fichiers automatisés, achevé en 1979 (Conseil de l'Europe, CJ-PD-GTI (79) 1). Ce document fut élaboré en étroite coopération avec un groupe équivalent de l'OCDE (González Fuster, 2014a, p. 87), Frits Hondius, du Conseil de l'Europe, et Hans Peter Gassman, entretenant d'étroites relations professionnelles. Il devint, après modifications, la Convention 108 du Conseil de l'Europe, et fut adopté formellement par le Comité des ministres en septembre 1980, puis signé en janvier 1981. Louis Joinet, qui a rédigé le projet de loi Informatique et Libertés en France[90], fut le président de ce groupe d'experts chargé de la rédaction de la convention[91].

La Convention 108, qui n'a été actualisée qu'en 2018, marqua une étape supplémentaire dans l'histoire du droit *des* données à caractère personnel. En effet, contrairement aux précédentes résolutions du Conseil de l'Europe, mais aussi contrairement aux lignes directrices adoptées par l'OCDE en 1980, il s'agit de la première convention internationale juridiquement contraignante dont l'objet est la défense du droit fondamental à la protection des données à caractère personnel. L'enjeu des discussions au Conseil de l'Europe de 1976 à 1981 était donc moins de débattre du contenu essentiel du texte de la convention, mais de faire accepter le

88 Entretiens avec Hans Corell, Peter Hustinx, Marie Georges, Michael Kirby, Alice Frank, et Henri Delahaie

89 Dans ce document, le Secrétariat de l'OCDE rapporte les propos de Frits Hondius indiquant que c'est pour cette raison que fut créé en 1976 le nouveau comité d'experts sur la protection des données, qui prit la place du groupe d'experts précédent.

90 Cf. 3.3.5.

91 Ce fait est mentionné dans la retranscription de son audition au Sénat en date du 17 mars 2014 (Joinet, 2014).

principe d'une telle norme juridique par des États, et de s'assurer de sa compatibilité avec les différents droits nationaux auxquels elle avait vocation à s'appliquer.

Contrairement au groupe d'experts de l'OCDE, nous n'avons pas pu obtenir beaucoup d'informations sur le fonctionnement du groupe d'experts du Conseil de l'Europe. Les archives consultées montrent qu'il y avait en général deux experts envoyés par État membre, certains États, n'envoyant cependant pas systématiquement de délégué[92]. Ces experts étaient, pour l'essentiel d'entre eux, des magistrats ou des fonctionnaires de ministères de la Justice, ayant pour certains participé à des travaux de groupes de réflexion nationaux chargés de réfléchir à une réforme du droit *de la* vie privée. Le secrétariat dirigé par Frits Hondius était chargé de préparer les réunions en amont, et de rédiger des comptes-rendus en aval. Des documents, souvent des projets de lois nationaux ou des rapports rédigés par des groupes d'experts nationaux, étaient traduits par le secrétariat et transmis à l'avance à l'ensemble des participants afin qu'ils en prennent connaissance.

Le groupe d'experts n'a fait que rédiger des propositions, qui ont ensuite, *in fine*, été transmis par le secrétariat au Comité des Ministres pour une adoption formelle. Ce processus, dont les archives disponibles n'ont malheureusement pas permis de retracer le cheminement dans le détail, a certes transformé et reformulé le texte de la proposition rédigée par le groupe d'experts, mais sans en modifier l'esprit, et finalement assez peu la forme. Les personnes composant le groupe d'experts sur la protection de la vie privée vis-à-vis des banques de données électroniques peuvent donc bel et bien être considérées comme les auteurs, à titre collectif, des résolutions de 1973 et 1974 précitées, puis de la Convention 108.

Il semble que ce groupe d'experts ait fonctionné en relative autonomie. En effet, la question de la protection des données à caractère personnel ne bénéficiait pas d'une grande couverture médiatique en Europe, et n'étant pas perçu comme fortement politique par les gouvernements nationaux, nous n'avons trouvé la trace ni dans les archives ni en entretien de directives dictées par des ministres. Les membres du groupe d'experts ont donc, semble-t-il, disposé d'une relative autonomie pour y exprimer leurs positions et se mettre d'accord sur des principes communs en accord avec leurs propres principes personnels. Pour Peter Hustinx, en entretien, cette relative autonomie par rapport aux gouvernements aurait été la conséquence de la nouveauté du sujet, qui leur aurait laissé une forte marge de manœuvre pour que les participants, dont il décrivit certains, notamment Louis Joinet, comme « passionnés », puissent trouver un consensus cadrant avec leurs convictions personnelles. Cela ne veut pas dire pour autant, bien sûr, que toute différence nationale et désaccords personnels sur le fond disparussent. Mais les désaccords dont nous avons retrouvé la trace semblent avoir plutôt porté sur des différences conceptuelles ou sur des différences de façon de faire selon les traditions juridiques nationales, plutôt que sur des questions politiques fondamentales affectant le cœur des convictions de ces

92 Par exemple, à la deuxième réunion du groupe d'experts, en juin 1972, Chypre, l'Irlande, l'Islande, le Luxembourg, Malte et la Finlande (pays observateur), n'envoyèrent pas de délégué.

experts ou des politiques des gouvernements qui les ont envoyés à ces réunions à Strasbourg[93]. Comme l'exprima Hans Corell en entretien, sur la période du milieu des années 1970 à l'adoption de la Convention 108 en 1981 :

> « À ma connaissance, notre tâche était, pour ainsi dire, de nature technique et consistait à traduire des travaux déjà effectués sous une forme appropriée, comme par exemple une convention internationale[94]. » (Entretien avec Hans Corell)

Dans la citation ci-dessus, Hans Corell, qui à l'époque était un haut-fonctionnaire du ministère de la Justice suédois, évoquait son passage au groupe d'experts du Conseil de l'Europe, mais aussi à celui de l'OCDE, sur lequel s'était d'ailleurs concentré lors de notre entretien avec lui. Nous verrons que le groupe d'experts de l'OCDE qui a travaillé à la rédaction des Lignes directrices de 1980 a entretenu des liens étroits avec son homologue du Conseil de l'Europe.

3.4.3. Les groupes informatiques successifs de l'OCDE

Hans-Peter Gassman, en charge du secrétariat de ces groupes, assista à des réunions au Conseil de l'Europe, et Frits Hondius, en charge du secrétariat des groupes successifs du Conseil de l'Europe, assista à des réunions à l'OCDE. Plusieurs de ses membres avaient assisté aux réunions des deux groupes, comme Louis Joinet, ou encore Hans Corell, qui se rappelait en entretien :

> « Il m'a été demandé de travailler à la fois au Conseil de l'Europe et à l'OCDE sur des questions en discussion. Parce que le Conseil de l'Europe souhaitait proposer une convention sur la protection des données. J'étais donc le délégué suédois à ces négociations. Peu après, l'OCDE a souhaité mettre en place des lignes directrices et il m'a également été demandé de faire ce travail[95]. » (Entretien avec Hans Corell)

Malgré leur étroite coopération, il existait une forme de rivalité entre l'OCDE et le Conseil de l'Europe en matière de développement de règles de protection des données, pour

93 Cf. section 3.7.

94 Traduction. Texte original : « As I recall it, our task was more, shall we say, over technical matters, that we had to translate work that had already been done into a proper form, as a convention »

95 Traduction. Texte original : « I was asked to work both in the Council of Europe and in the OECD on issues that were discussed. Because in the Council of Europe, they wanted to draft a convention on data protection. So I was the Swedish delegate in those negociations. And then soon after came the OECD who wanted to elaborate guidelines. And then I was asked to do this work as well. »

savoir qui allait parvenir en premier à fixer un corpus de règles, que le deuxième arrivé se devait de prendre en compte. Les pays de l'OCDE non-membres du Conseil de l'Europe, en particulier, étaient inquiets de voir se développer ces règles sans qu'ils puissent prendre part à leur élaboration :

> « Cette décision a été prise en partie […] en raison du sentiment que les pays intercontinentaux de l'OCDE pourraient être délaissés, tandis que l'Europe prenait de l'avance et mettait en place son propre régime juridique face à ce qui constituait effectivement une technologie de portée mondiale et en forte croissance. L'OCDE a ainsi décidé de mettre en place un groupe d'experts […][96]. » (Entretien avec Michael Kirby)

Le périmètre du groupe de l'OCDE n'est donc pas identique à celui du Conseil de l'Europe. Alors que ce dernier s'est spécialisé depuis l'adoption de la Convention européenne des droits de l'Homme dans des questions relatives aux libertés fondamentales, et n'a pour membres que des pays européens, l'OCDE compte depuis 1961 des membres non-européens. En effet, suite à la création de la Communauté économique européenne (CEE) en 1957, l'Organisation européenne de coopération économique (OECE), qui avait notamment été en charge de la gestion du plan Marshall, devient l'Organisation de coopération et de développement économique (OCDE) pour permettre à des membres non-européens du bloc de l'Ouest d'adhérer. Ainsi, les pays européens de l'OCDE sont rejoints dès 1961 par le Canada et les Etats-Unis, le Japon en 1964, l'Australie en 1971 et la Nouvelle-Zélande en 1973[97].

La mise à l'agenda de la protection des données à l'OCDE n'a pas suivi exactement le même processus intellectuel qu'au Conseil de l'Europe. La question de la protection de la vie privée vis-à-vis de la numérisation de données à caractère personnel s'est faite non pas à partir d'une mise à l'agenda de la problématique de la « vie privée », comme au Conseil de l'Europe, mais en raison de l'intérêt que l'OCDE portait aux échanges scientifiques et technologiques entre États membres, notamment dans le domaine de l'informatique.

En janvier 1968, le Groupe d'experts pour les instruments scientifiques de la Direction des affaires scientifiques rédigea un rapport à diffusion restreinte sur les écarts technologiques entre pays membres (OCDE, DAS/SPR/68.1). Ce rapport fut suivi par une conférence sur le sujet le même mois (OCDE, DAS/SPR/68.8), et, sur la base des discussions qui y eurent lieu, le Comité de la politique scientifique proposa dans un document préparant la troisième Conférence

96 Traduction. Texte original : « That decision was made in part […] by feeling that the OECD intercontinental countries might be left in the cold whilst Europe went ahead and developed its own legal regime for what was effectively a global and fast-growing technology. And so the OECD decided to set up an expert group […]. »

97 Dates d'adhésion provenant du site web de l'OCDE : http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm (page consultée le 9 décembre 2019).

ministérielle de la science de février de se pencher sur les échanges transfrontières de données électroniques, dans le but de mener des travaux afin de les faciliter (OCDE, DAS/SPR/68.10). L'ordre du jour de cette conférence ministérielle évoqua ainsi les problèmes de compatibilité entre systèmes informatiques qui pourraient gêner la création d'une « bibliothèque mondiale » (OCDE, CMS (68) 18, p. 8) dans un contexte de Guerre froide où l'organisation concurrente à l'OCDE dans le bloc de l'Est, le Conseil d'assistance économique mutuelle (CAEM), avait aussi entamé des travaux dans ce sens (OCDE, CMS (68) 18, p. 11). Il fut alors décidé de créer un groupe d'experts sur l'utilisation des ordinateurs (*Computer Utilization Group*) (CUG) pour mener des études sur l'informatique et formuler des propositions (Niblett, 1971, p. 5).

Nous n'avons pas trouvé dans les archives de documents portant sur les données électroniques ou sur les flux transfrontières de données datant entre 1969 et 1971. L'enchaînement exact des événements ayant conduit à la mise à l'agenda de la protection de la vie privée à l'OCDE ne nous est donc pas connu. Toutefois, dès 1971, le CUG publia un rapport commandé à G.B.F Niblett[98] intitulé *L'information numérique et le problème de la vie privée* (*Digital Information and the Privacy Problem*), dans une série d'ouvrages appelée « Études d'informatique » (« *Informatics Studies* »).

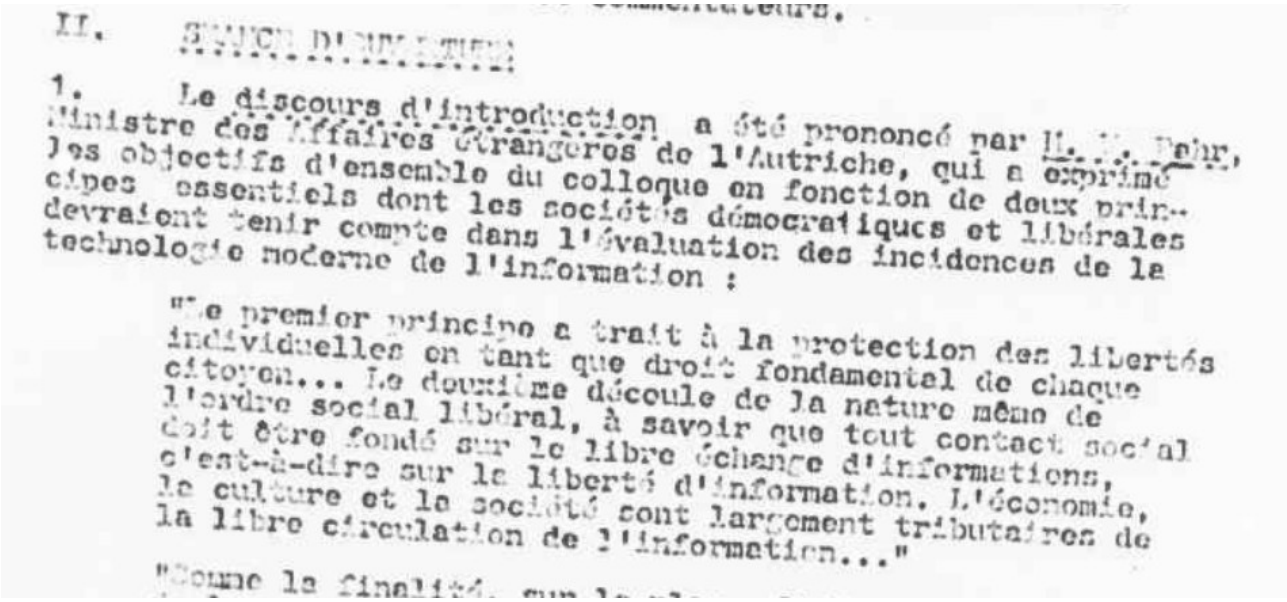
Le CUG s'inquiéta de l'adoption par le Land ouest-allemand de Hesse d'une loi de protection des données, et de l'émergence de propositions similaires dans d'autres juridictions (González Fuster, 2014a, p. 77). Ses membres craignaient qu'une adoption de lois divergentes, en ordre dispersé, créent des obstacles à la libre-circulation des données numériques. Le but de l'étude commandée à G.B.F Niblett fut donc de rédiger un état de l'art sur les réflexions en cours dans les États membres de l'OCDE, d'analyser le rapport entre informatique et droit *à la* vie privée, et de rédiger des propositions qui puissent aider les États membres à adopter un droit *de la* protection des données à caractère personnel le plus harmonisé possible, qui n'entrave pas les flux transfrontières de données.

À la suite de la la publication de ce rapport, un nouveau groupe d'experts fut créé : le *Data Bank Panel*, présidé par le suédois Per Svenonius (González Fuster, 2014a, p. 76). Ce groupe d'experts organisa à Paris, en 1974, un séminaire sur la protection des données : « Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives ». Ce séminaire fut suivi par un autre, organisé à Vienne en 1977, sur le même thème, intitulé : « Les flux de données transfrontières et la protection des libertés individuelles : effets et tendances » (OCDE, DSTI/ICCP/77.47).

Les compte-rendus de ces conférences (OCDE, 1974 et OCDE, DSTI/ICCP/77.47) sont des documents précieux qui ont été intégrés dans le corpus d'analyse de la présente recherche. En

98 G.B.F. Niblett était membre au Royaume-Uni d'une commission sur la vie privée de la *British Computer Society*. Nous ne sommes pas parvenu à retrouver son prénom, mais seulement ses initiales.

effet, les interventions du séminaire de 1974 ont fait l'objet d'une retranscription et d'une publication dans un livre publié dans la collection des « Études d'informatique » de l'OCDE. Elles permettent d'avoir une liste de personnes impliquées dans les discussions au niveau de l'OCDE, et de lire et analyser leurs discours sur la protection des données. Nous avons pu consulter ce livre, en français, à la Bibliothèque Sainte-Geneviève à Paris, et le retrouver sous format PDF mais en anglais en effectuant des recherches sur le web. Quant à la conférence de 1977, le compte-rendu que nous avons trouvé sur des microfilms des archives de l'OCDE à Paris n'est pas une retranscription intégrale des discours des intervenants. Certains propos sont rapportés entre guillemets, et d'autres à la voix indirecte. Il s'agit d'une synthèse plutôt que d'une retranscription, mais elle nous a également permis de nous faire une idée des positions des uns et des autres, de leurs arguments, et des éventuels débats :



II. [illegible]

1. Le discours d'introduction a été prononcé par M. [illegible], Ministre des Affaires étrangères de l'Autriche, qui a exprimé les objectifs d'ensemble du colloque en fonction de deux principes essentiels dont les sociétés démocratiques et libérales devraient tenir compte dans l'évaluation des incidences de la technologie moderne de l'information :

"Le premier principe a trait à la protection des libertés individuelles en tant que droit fondamental de chaque citoyen... Le deuxième découle de la nature même de l'ordre social libéral, à savoir que tout contact social doit être fondé sur le libre échange d'informations, c'est-à-dire sur la liberté d'information. L'économie, la culture et la société sont largement tributaires de la libre circulation de l'information..."

"Comme la finalité, sur le [illegible]

Figure 11 : *Extrait du compte-rendu du séminaire sur la protection des données de 1977 à Vienne, rédigé par le secrétariat de l'OCDE (DSTI/ICCP/77.47)*

Alors que les travaux au Conseil de l'Europe s'acheminaient vers la rédaction d'un projet de convention internationale juridiquement contraignante, la décision fut prise à l'OCDE, après la conférence de Vienne de 1977, de lancer la rédaction d'un document normatif (mais de droit souple) propre à cette organisation, sur la protection de la vie privée vis-à-vis des informations informatisées. Un nouveau groupe d'experts fut créé pour prendre la suite du *Data Bank Panel* : le « Groupe sur les obstacles au mouvement transfrontière des données et la protection des libertés fondamentales ». Son mandat, daté du 17 mars 1978, précisait bien à son premier point qu'il excluait à ce stade tout projet de traité international contraignant au niveau de l'OCDE, contrairement à ce qui était le dessein au Conseil de l'Europe des rédacteurs de ce qui allait devenir la Convention 108. Il indiquait en effet que le groupe devait :

« (1) Élaborer des lignes directrices relatives aux règles fondamentales régissant le mouvement transfrontière des données de caractère personnel et la protection des libertés individuelles, en vue de favoriser l'harmonisation des législations nationales, sans que cela exclue l'établissement ultérieur d'une Convention internationale ;

(2) Étudier les problèmes juridiques et économiques soulevés par le mouvement transfrontière de données sans caractère personnel, afin de servir de base à l'élaboration en ce domaine de lignes directrices qui s'inspireraient du principe de la libre-circulation de l'information » (OCDE, DSTI/ICCP/78.6 FR, pp. 2-3)

La question se posa alors d'élire quelqu'un pour prendre la présidence du groupe. Les Européens de droit continental étaient menés par Louis Joinet, délégué français. Les pays de *Common Law* comme le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande voyaient d'un mauvais œil ce qu'ils percevaient comme une tentative de leur imposer des règles inspirées par des traditions de droit continental[99]. La délégation états-unienne formée par Bill Fishman et Lucy Hummer ne souhaita donc pas voir d'Européen continental élu à la tête du groupe d'experts. C'est ainsi qu'un compromis fut trouvé, en la personne de Michael Kirby, qui avait pour qualité de n'être ni Européen, ni Américain (Kirby, 2017).

Les discussions aboutirent au bout de quatre réunions, en mai 1979 à la rédaction d'un brouillon qui fut d'abord soumis au Groupe de travail sur la politique de l'information, de l'information et des communications, puis au Comité de la politique scientifique et technologique (OCDE, DSTI/ICCP/79.40), puis au Conseil, composé des représentants nationaux auprès de l'OCDE. Suivirent des échanges, et deux réunions supplémentaires du groupe dirigé par Michael Kirby, avant qu'une nouvelle version de brouillon de lignes directrices ne soit adoptée en novembre 1979 (OCDE, SPT/M(79)3, p. 5). Il fallut encore plusieurs va-et-vient entre ces différents niveaux hiérarchiques entre mars 1980 et le 23 septembre 1980, date à laquelle le Conseil de l'OCDE décida d'adopter officiellement les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.

Le fait que des délégations non-membres du Conseil de l'Europe aient pris part aux discussions à l'OCDE a permis d'élargir les sujets de discussion[100]. Malgré tout, en pratique, nombre de décisions avaient déjà été prises dès le début des années 1970 par le groupe d'experts

99 Cf. section 3.7.
100 Entretiens avec Michael Kirby et Hans Corell

du Conseil de l'Europe. Comme le fit alors remarquer Michael Kirby en entretien, il ne pouvait plus être question de « réinventer la roue[101] », c'est-à-dire de remettre en cause les principes sur lesquels les délégations nationales au Conseil de l'Europe étaient tombées d'accord[102].

Comme Alice Frank et Hans Corell, Michael Kirby a décrit en entretien le mode de fonctionnement du groupe d'experts entre 1978 et 1979, ce qui permet de comprendre la façon dont les versions successives du texte furent rédigées :

> « Le Secrétariat était dirigé par Hans-Peter Gassman, un expert allemand travaillant pour l'OCDE. Le Secrétariat avait embauché un consultant […] : Peter Seipel, de l'Université de Stockholm. […] Dans mes souvenirs, je prenais un vol pour Paris et travaillais pendant les 24 heures du vol depuis l'Australie, sur de la documentation, parce que j'étais très occupé par mon travail à la *Law Reform Commission* (Commission de réforme du droit). Ensuite, j'ai travaillé de manière très intense pendant une semaine entière ; je ne pense pas que cela ait duré plus d'une semaine. Nous travaillions dans un nouveau bâtiment à Paris, où se trouvent la majorité des services de l'OCDE. De temps en temps, […] nous nous rendions au Château de la Muette pour une réception, parfois même avec champagne si notre travail avançait bien. La plupart du temps, nous travaillions dans un bureau isolé du Nouveau Bâtiment, […] et le groupe d'experts de l'OCDE travaillait très dur. […] Un problème qui est survenu très rapidement est que les participants français avaient reçu l'ordre du gouvernement français de ne pas rester aux réunions lorsqu'il n'y avait pas, ou plus, d'interprétation en anglais, en signe de protestation contre une anglicisation croissante des réunions de l'ONU […]. Ainsi, pour protester contre la volonté du président de continuer le travail après le départ des interprètes, à 18 heures, la délégation française quittait la réunion[103]. » (Entretien avec Michael Kirby)

101 Traduction libre de : « […] we didn't have to reinvent the wheel, we didn't want to reinvent the wheel […] » (entretien avec Michael Kirby).

102 Cf. section 3.4.4.

103 Traduction. Texte original : « The Secretariate was headed by dr. Hans-Peter Gassman, a German expert working for the OECD. They had a consultant who had been hired […] : Peter Seipel, at the University of Stockholm. […] My recollection is that I would fly to Paris, I worked the whole way on the plane, which is 24 hours of flight from Australia, on documentation, because I was very busy in my job in the Law Reform Commission. And then I would work with great intensity during an entire week. I don't think it ever stretched over more than a week. We worked in a new building, in Paris, where the OECD is, for the most part. Occasionally […] we were allowed into the Château de la Muette, and we were given a cocktail party, or if we worked very hard and made good progress, champagne might even be served. But on the whole we were in a dungeon of the Nouveau Bâtiment and that is where we worked. […] I worked the OECD expert group very hard. […] One problem which was presented quite early was that French participants were under instructions from the government of France not to remain in meetings when the French translation ran out, as a protest against the growing anglicisation of language in UN meetings […]. So that in protest to the chairman's endeavour to get people to work after the interpreters had departed, which was 6 PM, the French delegation would simply pack its bags and leave. »

Chaque réunion durait ainsi plusieurs jours.

Michael Kirby décrivit également les moyens techniques à sa disposition et l'usage de la photocopieuse pour produire rapidement pour chaque matin des comptes-rendus des discussions de la veille, qui lui permettaient de fixer sur papier les points de consensus au fur et à mesure qu'ils se formaient, pour éviter que des délégations revinssent dessus :

> « Je devais essayer de faire en sorte que la réunion reste dynamique, et nous parlons d'une époque où les logiciels de traitement de texte n'existaient pas. Je faisais cela en préparant à la fin de chaque journée un résumé écrit à la main des points sur lesquels un accord avait été trouvé, de ceux sur lesquels aucun accord n'avait été trouvé, et des points qui restaient à débattre. C'était fait sur un document dactylographié, contrairement au style que les gens de mon âge s'étaient vus enseigner à l'école ; c'était plus facile à lire. Je déposais ensuite le document le lendemain matin au secrétariat de l'OCDE, où il était photocopié, puis mis à disposition des participants. Je pense que cela aidait réellement à maintenir le dynamisme des échanges. Au départ, certains, surtout ceux qui ne travaillaient pas en anglais, étaient réticents à cette tentative de compte-rendu de la réunion. Mais je pense que tout le monde a fini par devenir enthousiaste en voyant l'effort majeur que fournissait une communauté internationale […] unie[104]. » (Entretien avec Michael Kirby)

Nous n'avons hélas pas retrouvé ces papiers dans la semaine que nous avons passée aux archives de l'OCDE. Toutefois, la méthode employée par Michael Kirby et le rôle de la fixation à l'écrit du consensus au fur et à mesure de sa formation dans l'adoption rapide d'un document prêt à être soumis à l'approbation du Conseil de l'OCDE fut souligné tant par Hans Corell, que par Alice Frank.

3.4.4. L'invention des principes de la protection des données

Que ce soient les résolutions de 1973 et de 1974 du Conseil de l'Europe, les Lignes directrices de l'OCDE de 1980, la Convention 108, ou, aujourd'hui, le RGPD à son article 5, ces

104 Traduit de l'anglais. Texte original : « I had to try and keep the momentum going. These are days before word processors. And the way I did that was by preparing at the end of each day a hand-written summary of the points that appeared to have been agreed, and the points that had not been agreed, and the points that remained to be discussed. And I would prepare those in hand-written printed format, I didn't write it in a copperplate style people of my age were taught at school, I printed it to make it easier for people who were getting the next best thing to a typed document. And that would be delivered to the OECD secretariate the next morning, and would be photocopied, and would be made available to the participants. I think that really kept the momentum, and at first, especially those who were not working in English, were resistant to this attempt to provide a kind of minutes of the meeting. But I think everybody got caught up with the enthusiasm of seeing a major effort of the international community […] coming together. »

instruments juridiques ont en commun le fait de dresser une liste de principes qui doivent être respectés par les personnes physiques ou morales qui traitent des données à caractère personnel.

La terminologie et la typologie de ces principes varie d'un texte juridique, ou d'un texte de doctrine, à l'autre. Ainsi, l'article 5 du RGPD parle des principes de « licéité, loyauté, transparence », puis de « limitation des finalités », de « minimisation des données », d'« exactitude », de « limitation de la conservation », d'« intégrité et confidentialité » et « responsabilité ». Le manuel sur la protection des données publié en 2014 par l'Agence des droits fondamentaux de l'Union européenne (Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, 2014) consacre l'intégralité de son chapitre 3 à ces principes, et liste les principes de « licéité » (p. 69), « spécification et limitation des finalités » (p. 74), « qualité des données » (p. 77), « loyauté » (p. 81) et « responsabilité » (p. 83). Quant à la convention 108, elle dispose à son article 5 que :

> « Les données à caractère personnel faisant l'objet d'un traitement automatisé sont :
>
> a) obtenues et traitées loyalement et licitement ;
>
> b) enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités ;
>
> c) adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ;
>
> d) exactes et si nécessaire mises à jour ;
>
> e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. » (art. 5 de la Convention 108 du Conseil de l'Europe)

Ainsi, nous pouvons voir que l'article 5 du RGPD regroupe « licéité », « loyauté » et « transparence » sous une même catégorie, mais distingue « limitation des finalités » et « limitation de la conservation ». Mais cette différence n'est qu'une différence dans la façon de présenter des principes auxquels chaque texte consacre ensuite des développements plus détaillés quant aux modalités de respect de ces principes.

Il arrive également qu'un principe soit évoqué dans un texte, mais pas dans l'autre, alors même que des obligations visant à mettre en œuvre le respect de ce principe y sont bien présentes. Ainsi, l'article 5 paragraphe 1 sous f) du RGPD évoque un principe d'« intégrité et confidentialité », qui impose que les données personnelles soient traitées « de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées » (art. 5 paragraphe 1 sous f) du RGPD). Les articles 32 à 34 sont ensuite consacrées spécifiquement à des obligations

relatives à la sécurité et à la confidentialité des données. Or, si la Convention 108 du Conseil de l'Europe n'évoque pas la sécurité et la confidentialité au rang des principes généraux et fondamentaux du droit *de la* protection des données à caractère personnelle, elle comprend bien un article 7, intitulé « Sécurité des données », qui dispose :

> « Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés. » (art. 7 de la Convention 108 du Conseil de l'Europe)

De la même façon, l'article 13 des Lignes directrices de l'OCDE de 1980 évoque un « principe de la participation individuelle » :

> « Principe de la participation individuelle
>
> 13. Toute personne physique devrait avoir le droit :
>
> a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant ;
>
> b) de se faire communiquer les données la concernant ;
>
> i) dans un délai raisonnable ;
>
> ii) moyennant, éventuellement, une redevance modérée ;
>
> iii) selon des modalités raisonnables ; et
>
> iv) sous une forme qui lui soit aisément intelligible ;
>
> c) d'être informée des raisons pour lesquelles une demande quelle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet ; et
>
> d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger. »

Si ce principe n'est pas évoqué sous cette formulation par le RGPD, il n'en demeure pas moins que son contenu est présent à travers l'ensemble du chapitre III sur les droits des personnes concernées, qui comprend des articles sur l'obligation d'information des personnes concernées (art. 13 et 14 du RGPD), le droit d'accès (art. 15), le droit à la rectification (art. 16), à l'effacement (art. 17), à la limitation (art. 18), à la portabilité (art. 20) ou encore d'opposition (art. 21).

Notons d'ailleurs que le principe de portabilité, qui permet à chaque personne concernée de demander à ce que lui soient communiquées les données qui la concernent dans un format numérique standard, est un droit nouveau qui n'existait pas avant le RGPD. Mais ce droit nouveau découle de la logique de ce principe de la participation individuelle évoqué dans les Lignes directrices de l'OCDE, c'est-à-dire de l'existence de droits des personnes sur les données les concernant ; il ne fait qu'y apporter une précision, et non amender le contenu essentiel de ce principe.

D'où viennent ces principes ? Quand ont-ils été inventés, et par qui ? Quels arguments, et quels référentiels, les ont portés ? Quelles transformations ont-ils subies de la formulation initiale à leur intégration aux Lignes directrices de l'OCDE et à la Convention 108 du Conseil de l'Europe ?

La confusion terminologique que nous venons d'exposer complique bien entendu le travail de recherche généalogique sur l'origine des principes de la protection des données, souvent désignée sous le terme de « *Fair Information Principles* ». Elle ne le rend toutefois pas impossible, à condition d'analyser non seulement le nom, la forme et le nombre de ces principes mais aussi leur contenu, avec les convergences, différences et nuances des propositions qui ont été faites à partir de la fin des années 1960 pour dessiner et rédiger peu à peu les dispositions concrètes d'un droit *de la* protection des données à caractère personnel.

Le rapport HEW publié en 1973 a popularisé la notion de « *Fair Information Principles* ». Selon Colin Bennett, il s'agirait d'ailleurs de la première « énumération explicite de 'certains principes fondamentaux de pratiques informationnelles loyales'[105] » (Bennett, 1992, p. 97). Grâce à l'accès que nous avons eu aux archives du Conseil de l'Europe, nous avons pu déterminer que ce n'est pourtant pas le premier document qui présenta sous cette forme les obligations à imposer aux traitements de données à caractère personnel.

La première réunion du groupe d'experts du Conseil de l'Europe sur la protection de la vie privée vis-à-vis des banques de données électroniques s'est déroulée à Strasbourg du 13 au 15 mars 1972. Le compte-rendu rédigé par le secrétariat et daté du 16 juin 1972 (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 5 REV) est structuré en suivant les points de l'ordre du jour. Après l'élection des président et vice-président du groupe d'experts, et la présentation par Hans Peter Gassman des travaux de l'OCDE, chaque délégation avait été invitée à faire une présentation.

105 Traduction de l'auteur. Texte original : « the first explicit enumeration of 'certain fundamental principles of fair information practice' ».

La délégation d'Allemagne de l'Ouest fit une présentation d'un projet de loi fédérale sur la protection des données, et sur les réflexions du gouvernement fédéral à ce sujet. Elle indiqua que les réflexions en cours étaient fondées sur un certain nombre de « principes » :

> « Le gouvernement fédéral, pour sa part, envisage aussi de rédiger un projet de loi à soumettre au Parlement fédéral, fondé sur les principes suivants : […][106] » (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 5 REV, p. 7)

La suite du texte ne comprend toutefois pas encore de liste de principes désignés chacun comme étant une catégorie de sens à part. Il s'agit plutôt d'une facilité de rédaction pour présenter les principaux points auxquels la réflexion en cours au sein du gouvernement fédéral d'Allemagne de l'Ouest s'attachait, à savoir que :

> « - La législation fédérale sur la protection des données complétera les autres lois existantes dans le domaine de la protection des données ;
>
> - la vie privée doit être protégée contre les dangers du traitement à la fois public et privé des données ;
>
> - les mesures législatives à adopter s'appliqueront au traitement électronique, mécanique et manuel des données ;
>
> - elles devront également fournir un cadre technique ou organisationnel minimum de protection des données ;
>
> - de manière générale, cette législation doit respecter le besoin d'équilibre entre le droit de l'individu à la protection des données le concernant, et le droit à l'information d'autres individus, de la société, et de l'État[107]. » (Conseil de l'Europe, EXP. Prot.Priv. (72) 5 REV, p. 7)

106 Traduit de l'anglais. Texte original : « The Federal Government, fot its part, is also considering the draft of such a law chich will be submitted to the Federal Parliament and is based, among others, on the following principles : […] ».

107 Traduit de l'anglais. Texte original : « - Federal legislation on data protection will be supplementary in character to other laws already existing in the field of data privacy;
- privacy should be protected against dangers caused by both public and private data processing;
- the legislative measures to be adopted will deal with electronic, mechanical and manual data processing;
- they should also provide for the minimum technical or organisational conditions with a view to protect data privacy;
- in general, this legislation should observe the necessity of maintaining a balance between the right of the individual to secrecy of data concerning him and the right to information of other individuals, society and the State. »

La présentation de la délégation britannique, composée d'un certain A. M. Greenwood[108], fonctionnaire du *Foreign et Commonwealth Office*, et de G.P. Pratt, secrétaire au *Home Office*, l'équivalent britannique du Ministère de l'Intérieur, évoqua de façon beaucoup plus précise une liste de « principes » qui, même si leur contenu a été fortement modifié dans l'intervalle, correspondait déjà dans la forme à ce qui est entendu aujourd'hui par : « principes de la protection des données » ou « *Fair Information Principles* » :

> « Une liste de principes applicables au traitement des informations personnelles dans les banques de données électroniques dans le secteur privé a été soumise par les experts du Royaume-Uni. Sur le fondement de cette liste, le Comité a élaboré le projet préliminaire suivant de règles minimales pouvant être intégrées à une recommandation[109]. » (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 5 REV, p. 12)

La liste des principes rédigés en commun par le groupe d'experts du Conseil de l'Europe en 1972 sur la base de ces propositions britanniques est disponible en annexe 12.

Au Royaume-Uni, le comité Younger sur la protection de la vie privée fut désigné en mai 1970 par le gouvernement travailliste, puis confirmé dans ses fonctions par le gouvernement conservateur élu en juin de la même année. Sa mission, si elle se limitait au secteur privé, dépassait par contre le cadre de la protection des données ou de la vie privée *informationnelle*, c'est-à-dire la simple question de l'informatique et de l'emploi d'ordinateurs pour stocker des données personnelles. Une section entière du rapport de ce comité, remis en 1972, y est tout de même consacré, rédigée par un groupe de travail organisé en son sein, le groupe de travail sur les ordinateurs (*Working Group on Computers*) (Younger, 1972).

G.P. Pratt, l'un des membres de ce groupe de travail, présent lors de la première réunion du groupe d'experts du Conseil de l'Europe où furent présentées les idées de la délégation britannique, avec les autres membres du groupe de travail sur les ordinateurs du comité Younger, ont sollicité l'expertise de la *British Computer Society* (BCS), une organisation professionnelle britannique regroupant des informaticiens. Cette dernière constitua également un groupe de réflexion sur la protection de la vie privée, qui remit un rapport au comité Younger en mars 1971 (British Computer Society, 1971). Comme nous le verrons dans le dernier chapitre, c'est de l'interaction entre les membres du comité Younger et ceux du groupe de réflexion sur la vie privée de la BCS, entre 1970 et 1972, qu'est née l'idée de formaliser un certain nombre de

108 La liste des participants annexée en fin de compte-rendu ne comportait que les initiales des prénoms et nous ne sommes pas parvenu à retrouver tous les prénoms.

109 Traduit de l'anglais. Texte original : « A list of principles on the processing of personal information by electronic data banks in the private sector was submitted by the United Kingdom experts. On the basis of this list, the Committee worked out the following preleminary draft of minimum rules which might be incorporated into a recommendation »

« principes » de la protection des données, dont, en particulier, le principe de limitation des finalités.

Après les résolutions non-contraignantes de 1973 et 1974 du Conseil de l'Europe sur la protection des données à caractère personnel, ce fut au tour de la Convention 108 de 1981 d'affirmer ces principes. Son article 10 rappelle que « chaque Partie s'engage à établir des sanctions et recours appropriés visant les violations aux dispositions du droit interne **donnant effet aux principes de base pour la protection des données**[110] énoncés dans le présent chapitre ». Ces principes sont rédigés sous forme de phrases décrivant des obligations, aux articles 5, 7 et 8 du traité.

Les Lignes directrices de l'OCDE adoptées 1980 proposent elles aussi une liste de principes, très similaires à ceux du Conseil de l'Europe[111].

Il existe toutefois quelques différences entre les deux textes. Par exemple le principe de responsabilité est absent de la Convention 108 car celle-ci ne peut être invoquée par des parties au cours d'un litige devant une juridiction nationale, et n'oblige que les États. Elle laisse donc le soin aux États ayant ratifié ce traité d'adopter eux-mêmes les modalités d'un régime de responsabilité des personnes physiques ou morales qui collectent des données à caractère personnel. Toutefois, les similitudes sont bien plus nombreuses que les différences. Il n'est donc pas très surprenant de les voir repris dans la directive sur la protection des données adoptée en 1995 par l'Union européenne[112], dans un article 6 qui, reprenant le titre de l'article 5 de la Convention 108 du Conseil de l'Europe, s'intitule « principes relatifs à la qualité des données », et contient cette fois au paragraphe 2 une obligation découlant implicitement de ce que le texte des Lignes directrices de l'OCDE appelle le principe de responsabilité :

> « 1. Les États membres prévoient que les données à caractère personnel doivent être :
>
> a) traitées loyalement et licitement ;
>
> b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées ;
>
> c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;

110 Texte mis en gras par l'auteur.
111 Cf. tableau en annexe 1.
112 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Journal officiel des Communautés européennes du 23 novembre 1995, N° L 281, p. 31 à 50.

d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1. »

Nous voyons ainsi se dessiner une forte convergence entre le résultat des travaux du Conseil de l'Europe et de l'OCDE, qui ont influencé les contenus des lois nationales, la directive adopté par la Communauté économique européenne (CEE) en 1995, et sont encore présents dans le RGPD.

3.5. La formation de la *privacy community*

La particularité des diverses loi nationales adoptées entre 1970 et 1995, et *a fortiori* en Europe à partir de 1995, lorsque la directive européenne adoptée impose une harmonisation assez détaillée du droit *de la* protection des données[113], est que malgré des différences sur des points de procédure, sur les institutions mises en place, pour l'essentiel, affichent un niveau élevé de convergence en termes de contenu, et reprennent les principes que nous venons de décrire (Bennett, 1992, p. 111-115). Cette convergence s'explique par les contacts noués entre des hauts fonctionnaires de plusieurs pays du bloc de l'Ouest, qui se sont notamment retrouvés ou rencontrés dans des réunions des deux groupes de travail, l'un à l'OCDE, l'autre au Conseil de l'Europe, que nous avons étudiés.

113 La CJCE rappela ainsi dans l'arrêt « Lindqvist » du 6 novembre 2003 que « l'harmonisation [des] législations nationales [sur la protection des données] ne se limite donc pas à une harmonisation minimale, mais aboutit à une harmonisation qui est, en principe, complète. C'est dans cette optique que la directive 95/46 entend assurer la libre-circulation des données à caractère personnel, tout en garantissant un haut niveau de protection des droits et des intérêts des personnes visées par ces données » (CJCE 6 novembre 2003 « Bodil Lindqvist », aff. C-101/01, pt. 96).

Les personnes qui ont formé ce groupe sont[114], selon le terme utilisé entre autres par Colin Bennett, des « défenseurs de la vie privée » (« *privacy advocates* ») (Bennett, 2008, p. ix). Ensemble, ils forment une « communauté de la vie privée » (« *privacy community* »). Le terme peut parfois être entendu dans la bouche des acteurs eux mêmes, et nous l'avons rencontré lors de déplacements sur le terrain, notamment dans les diverses conférences sur la vie privée que nous avons fréquentées et dont Colin Bennett rappelle dans l'un de ses livres consacrés au sujet qu'il s'agit de lieux essentiels de socialisation pour ce groupe d'acteurs (Bennett, 2008, p. xix). Il est également utilisé dans certaines publications scientifiques (Bennett, 2008 ; Regan, 1995).

Lors des différents entretiens réalisés, plusieurs enquêtés, comme par exemple Peter Hustinx, ont insisté sur le caractère « familial » de cette communauté. D'autres, comme Marie Georges, ont insisté sur le rôle que ces contacts à l'international ont eu pour se tenir informé des études, réflexions et évolutions législatives en cours à l'étranger, et pouvoir s'en inspirer dans la rédaction de textes législatifs nationaux.

Cette « *privacy community* » s'est structurée au tout début des années 1970. Comme l'écrit Priscilla Regan :

> « Au moment où les questions de protection de la vie privée ont été mises à l'agenda public dans les années 1960, aucune communauté dédiée à la protection de la vie privée [*privacy community*] impliquée dans le travail législatif ne s'était encore formée. Cependant, avant la fin des années 1970, un noyau de communauté politique [*policy community*] s'était mis en place et s'intéressait à la question générale de la vie privée, aux côtés d'autres communautés spécialisées ou coalitions de cause s'intéressant à des aspects précis de la protection de la vie privée, notamment la protection des informations personnelles, la protection de la vie privée communicationnelle et la protection de la vie privée sur le lieu de travail[115]. » (Regan, 1995, p. 20-21)

« Un groupe soudé d'experts de différents pays s'est rassemblé, a échangé des idées, et a

114 Nous utilisons le passé pour désigner ces personnes, car une partie non négligeable d'entre elles sont encore vivantes voire actives. Peter Hustinx, par exemple, a joué un rôle actif dans l'organisation de la 41e édition de l'ICDPPC, la réunion annuelle mondiale des autorités de protection des données, à Tirana, en 2019.

115 Traduit de l'anglais. Texte original : « At the time privacy issues were added to the public agenda in the 1960s, a privacy community interested in legislation had not yet formed. By the late 1970's, however, a core policy community interested in general privacy existed along with specialized privacy communities, or advocacy coalitions, concerned with specific aspects privacy, including information privacy, communication privacy and workplace privacy »

trouvé un consensus général sur le meilleur moyen de résoudre le problème[116]. » (Bennett et Raab, 2003, p. 16)

La communauté de la vie privée n'est pas tout à fait une communauté épistémique au sens strict (Adler et Haas, 1992) bien qu'elle s'en rapproche : elle dispose d'une expertise reconnue, elle a démontré sa capacité à influencer des *outputs* de politique publique, mais son ciment n'est pas tant le partage d'une épistémologie commune, c'est-à-dire d'une façon de produire des connaissances valides, mais un système de convictions qui, dès les années 1970, est le paradigme libéral de la vie privée.

Progressivement, à partir des années 1970, la création d'autorités administratives indépendantes chargées de superviser la mise en œuvre du tout nouveau droit *des* données à caractère personnel a facilité la création d'un réseau d'entrepreneurs transgouvernementaux (Newman, 2008) comprenant les membres de ces autorités. Ce réseau s'est rapidement formalisé autour de plusieurs conférences, dont la plus ancienne, et la plus importante, était l'*International Conference of Data Protection and Privacy Commissioners*[117] (ICDPPC), dont la première édition s'est tenue à Bonn en 1979. Ce réseau forme, historiquement, l'épine dorsale de la communauté de la vie privée.

Comment cette communauté s'est-elle constituée ? Qui en furent les membres ?

Charles Raab et Colin Bennett ont déterminé à partir de leurs recherches que les groupes d'experts du Conseil de l'Europe et l'OCDE ont fourni l'occasion à ceux qui allaient former le premier noyau de cette communauté transnationale de se rencontrer lors des réunions à Strasbourg et Paris, à partir du début des années 1970 (Bennett, 1992, 2008 ; Bennett et Raab, 2003). Nos recherches ont permis de le confirmer.

Les personnes qui constituèrent peu à peu la communauté de la vie privée à partir du début des années 1970 sont celles dont nous avons déjà évoqué les noms dans les sous-chapitres précédents : Louis Joinet, Hans Peter Gassman, Spiros Simitis, Jan Freese, Peter Seipel, Frits Hondius, Peter Hustinx, Alan Westin, Stefano Rodotà, puis Philippe Lemoine, Michael Kirby… Ces personnes, pour la plupart des hauts fonctionnaires, dont beaucoup n'en étaient qu'au début de leur carrière, se rencontraient régulièrement à Strasbourg et à Paris et dans certaines conférences. Le faible nombre de spécialistes disponibles parmi les hauts fonctionnaires des différents États qui ont délégué des experts à l'OCDE et au Conseil de l'Europe pour étudier les questions politiques soulevées par le développement de l'informatique explique le fait que les mêmes personnes, en nombre limitées, se soient retrouvées dans la majorité de ces réunions, et

116 Traduit de l'anglais. Texte original : « A closely-knit group of experts in different countries coalesced, shared ideas and generated a general consensus about the best way to solve the problem. »

117 Cette conférence a changé de nom pour devenir la *Global Privacy Assembly* (GPA) à partir de 2020

aient ainsi pu faire connaissance, voire nouer des amitiés. Ce sont aussi soit des personnes qui ont été envoyées à l'OCDE et au Conseil de l'Europe en raison du rôle qu'elles jouaient déjà sur le plan national, soit qui ont joué un rôle important dans l'adoption de lois nationales de protection des données parce qu'elles avaient assisté à ces réunions des groupes d'experts.

Par exemple, le même G.B.F Niblett qui rédigea le premier rapport de l'OCDE sur la protection de la vie privée vis-à-vis des banques de données électroniques (Niblett, 1971) avait aussi participé aux travaux du comité sur la vie privée de la British Computer Society en 1971 (British Computer Society, 1971). Peter Hustinx et Dirk Ravestijn, qui avaient fait partie du secrétariat de la commission Koopmans aux Pays-Bas (Conseil de l'Europe, EXP/Prot.Priv. (74) 3, p. 1), furent choisis par leur gouvernement pour être envoyés à Strasbourg participer aux travaux du groupe d'experts sur la protection de la vie privée vis-à-vis des banques de données électroniques (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 17, p. 7). Spiros Simitis et Louis Joinet, co-auteurs des lois de leurs pays[118] en matière de protection des données, ont tous deux participé au groupe d'experts de l'OCDE présidé par Michael Kirby entre 1978 et 1980. Et Michael Kirby lui-même était en charge en Australie de travailler à l'Australian Law Reform Commission sur des projets en rapport avec la protection de la vie privée (Greenleaf, 2008 ; Kirby, 2017). Nous pourrions encore multiplier de tels exemples.

Les membres de cette communauté sont restés longtemps en contact, souvent amical, les uns avec les autres. Entre 2016 et 2018, pendant la campagne d'entretiens avec un certain nombre d'entre eux, nous avons ainsi pu constater que bon nombre d'entre eux s'écrivaient, se téléphonaient voire se voyaient encore régulièrement. Dans d'autre cas, il nous a été demandé de retrouver les coordonnées de tel ou tel ami de longue date perdu de vue, mais rencontré dans un des groupes d'experts sur la protection de la vie privée de l'époque. Il est également arrivé que nous ayons été interrogé, informellement, en marge de l'entretien, sur la santé de l'un ou de l'autre. Les nouvelles des décès de certains d'entre eux, hélas survenus pendant la période d'enquête, suscitaient l'expression d'un fort émoi, qui ont pu donner lieu à des échanges d'e-mails spécifiques avec certains enquêtés, parfois plusieurs années après la réalisation de l'entretien.

Parmi les personnes dont nous avons retrouvé les noms, certains sont restés actifs jusque dans les années 2000 voire 2010. Ainsi, à l'heure de l'écriture de ces lignes, Philippe Lemoine était encore nommé commissaire à la CNIL en 2014, alors que nous le retrouvions déjà à la réunion des 9 et 10 novembre 1977 du sous-groupe sur les banques de données du Groupe de travail sur la politique de l'information, de l'informatique et des communications à l'OCDE, aux côtés de Louis Joinet, Stefano Rodotà, Jan Freese, Hans Peter Gassman ou encore Alice Frank (OCDE, DSTI/ICCP/77.48). Peter Hustinx, présent à des réunions du Conseil de l'Europe dès 1972 (Conseil de l'Europe, EXP/ProtPriv/EDB (72) 17), fut jusque fin 2014 le Contrôleur

118 En tout cas du Land de Hesse pour Spiros Simitis.

européen de la protection des données, et fut un des protagonistes de l'adoption du RGPD, et était responsable d'une partie du programme de l'ICDPPC de 2019 à Tirana.

En entretien, Peter Hustinx s'est souvenu en ces termes de ces liens noués avec les autres membres de la communauté de la vie privée :

> « Les représentants de certains États membres étaient des gens qui dans leurs fonctions s'occupaient en fait du sujet [de la protection des données]. Le représentant britannique pendant les années 80 était le *deputy*[119] de ce qui est devenu l'*Information Commissioner*. Dans les années 70, 80 … Quoi qu'il en soit, OCDE, Conseil de l'Europe, il y avait quelques personnes que j'ai beaucoup croisées. Un nom que tu as certainement croisé, qui n'a pas pris part à la discussion, mais qui a eu énormément d'influence, était Spiros Simitis, un professeur allemand, qui fut le premier, qui fut celui qui en Hesse s'intéressa au sujet, qui a été pendant des années *Datenschutzbeauftragter* en Hesse, qui a écrit des manuels, des manuels épais, à qui la Commission européenne avait à l'époque commandé un projet pour ce qui est devenu la directive. Et qui est devenu aussi, je crois que c'était autour de 1982, président du comité d'experts. Je lui ai succédé en 85. Mais il y a eu un certain renouveau. Un type comme… qui est aujourd'hui une *éminence grise*[120] à Strasbourg, Jean-Philippe Walter, je pense que je l'ai rencontré dès les années 80 à Strasbourg. […] Bien sûr, avec le temps, cette *community*[121] s'est élargie [...]. Et désormais, cette communauté est devenue vraiment grande, car… Pour que tu comprennes, je me suis impliqué, après ma retraite il y a six mois, en tant qu'administrateur de l'*International Association of Privacy Professionals*, l'IAPP. Ils organisent beaucoup de congrès. Et on y voit le même phénomène : il y a une sorte de famille, de communauté, qui peut parfois avoir des divergences d'opinion, mais… c'est juste. Les *data protection commissions*[122] se sont entre temps organisées, elles ont aussi leur propre *community*[123]. C'était d'abord très informel, puis à partir des années 1990 il y a eu régulièrement… j'y ai moi-même participé ; je suis devenu président en 1991 de l'autorité néerlandaise de supervision. […] Et j'ai pris l'initiative de monter un club

119 En anglais dans le verbatim d'entretien
120 En français dans le verbatim d'entretien
121 En anglais dans le verbatim d'entretien
122 En anglais dans le verbatim d'entretien.
123 En anglais dans le verbatim d'entretien.

européen. Donc depuis 1991 nous nous rencontrons [régulièrement][124]. » (Entretien avec Peter Hustinx)

Pour Spiros Simitis :

« Je dois vous dire, et vous devez garder à l'esprit, que je dialoguais en permanence par exemple avec les créateurs de la CNIL ou qui ont travaillé dans ce domaine. Nous nous sommes rencontrés, nous avons réfléchi et discuté ensemble. Il est ainsi devenu très clair que nous avions bien sûr besoin de règles à l'échelle nationale, mais également d'une réflexion internationale sur la protection des données[125]. » (Entretien avec Spiros Simitis)

Leur action ne fut pas seulement une action de réflexion. Si Abraham Newman (2008) qualifie les membres de la « *privacy community* » d'« *entrepreneurs* transgouvernementaux » c'est bien parce qu'ils ont développé une stratégie afin d'imposer leur agenda politique d'adoption de lois de protection des données.

124 Verbatim original : « de vertegenwoordigers van een aantal lidstaten, waren mensen die inmiddels misschien in functie met het onderwerp bezig waren. De engelse vertegenwoordige vanaf, vanuit de jaren 80, was de deputy wat nu Information Commissioner is. In de jaren 70, naar 80, ... Hoe dan ook, OECD, Raad van Europa, daar speelden een aantal mensen die ik heel veel ben tegen gekomen. Eh ... een naam die je zeker bent tegen gekomen, die niet aan de discussie deel nam, maar wel heel veel invloed had, was Spiros Simitis, de duitse professor, die was de eerste, was degene die in Hesse met het onderwerp bezig was geweest, die jarenlang Datenschutzbeauftr‰gte is geweest in Hesse, die handboeken geschreven heeft, dikke handboeken, die door de Europese Commissie destijds gevraagd is een eerste ontwerp te maken voor de richtlijn. [inaudible] althans. En die werd ook, geloof ik in 82 of zoiets, voorzitter van het committee of experts. Ik heb hem daarna opgevolgd in 85. Maar, er is een zekere vernieuwing ontstaan. Een vent als eh... die nu, Èminence grise is in de, in Straatsburg, Jean-Philippe Walter, ik denk dat ik die in Straatsburg al van de jaren 80 heb meegemaakt. […] Nu, gaandeweg, is natuurlijk die community groter geworden [inaudible]. En nu wordt de community helemaal groot, omdat men, voor jou begrip, ik ben na mijn pensioen een half jaar geleden betrokken geraakt, als bestuurslid, bij de International Association of Privacy Professionals, de IAPP. Nou, die organiseert een hele reeks van die congressen. En, eh, ja daar zie dezelfde verschijnsel: er is een soort van familie, is er een community, die ook soms met elkaar van mening kan verschillen, maar eh, dat klopt. De data protection commissions hebben zich ook gaandeweg georganiseerd, die heeft ook een community. Eerst was het heel informeel, en vanaf het begin van de jaren 90 waren er regelmatig - en ik heb er zelf aan meegedaan, ik werd in 91 voorzitter van de nederlandse toezichthouder, voor die tijd was ik ambtenaar, weliswaar was dit een onderwerp die mijn portefeuille, maar ik deed ook veel meer. Maar toen, eh, was er een vacature in de nederlandse toezichthouder, en toen zeiden ze: nou, je schijnt ervan te weten. Omdat ik zo druk bezig was geweest in het Raad van Europa, was ik gevoellig voor dat perspectief, he, wat we nu bespreken. En ik heb toen het initiatief genomen om, om een europese club op te richten. Dus we zijn vanaf 91 stelselmatig. »

125 Traduit de l'anglais. Texte original : « I must tell you, you must have in mind, that for instance those who created the CNIL or worked in that field, and myself, were in constant discussion. So we met, we thought and we discussed together. And that is why at the same time it became very clear that we need rules, national rules of course, but also an international reflection on data protection. »

Un premier facteur d'influence de ce réseau, souligné par Abraham Newman (2008), est d'être parvenu à être identifié comme un lieu de ressource crédible d'expertise[126]. Ainsi, même hors de l'Europe de l'Ouest, et dès les années 1970, le réseau de défenseurs européens de la vie privée a attiré l'attention de personnes qui, dans d'autres pays, sur d'autres continents, ont cherché à développer des lois pour protéger la vie privée face à ce qui était perçu comme une menace des bases de données électroniques. Michael Kirby a raconté en entretien sa propre rencontre avec les défenseurs européens de la vie privée, alors qu'il venait de recevoir pour mission de travailler à un rapport sur ce sujet par l'équivalent australien du ministre fédéral de la justice :

> « Bon, la question de la protection de la vie privée avait été largement étudiée avant que nous ne recevions la requête du Procureur Général. Il y avait eu une enquête majeure au Royaume-Uni ainsi qu'une enquête majeure en France, le rapport Tricot. […] Et à l'époque, une conférence s'était tenue à propos de la législation de la Communauté économique européenne sur la protection de la vie privée. Cette conférence avait eu lieu à Vienne et il nous avait paru utile d'y envoyer le secrétaire et le président de la Commission australienne de réforme du droit, George Brouwer. […] Nous avons été ainsi reliés à la communauté internationale [127][...] » (Entretien avec Michael Kirby)

En entretien, Spiros Simitis évoqua quant à lui longuement le rôle des autorités de protection des données dans les années 1970, et l'importance de les doter d'une indépendance vis-à-vis des gouvernements pour renforcer leur crédibilité et imposer l'adoption des principes et définitions de la protection des données dans le droit positif aux parlements nationaux :

> « Une fois la quête pour la protection des données clairement [...] définie et le besoin d'une structure juridique également accepté, le premier principe mis en lumière a été la nécessité absolue [...] d'un contrôle. Ensuite, la nécessité absolue d'une institution qui assure [...] le contrôle de l'utilisation des données et qui en parallèle [...] collabore [...] étroitement avec le Parlement. Ainsi, un garant de la protection des données était déjà envisagé dans la première loi. [...] Le protecteur des données en Allemagne, en France, et ainsi de suite, doivent soumettre un rapport sur leurs expériences, qui doit ensuite [...] être débattu au Parlement. Il s'agit là de ce que nous avons construit, et en raison de cette construction, le contrôleur est un élément très spécifique. Il ne fait pas partie de

126 Pour une définition de l'expertise, voir : Delmas, 2011.

127 Traduit de l'anglais. Texte original : « Well there had been a lot of investigations on privacy before we received the reference from the Attorney-General. There had been a major investigation in the United Kingdom, and there had also been a major investigation in France, the Tricot report. […] And at the time, a conference was held on European Economic Community law on privacy protection. That conference was held in Vienna, and it was considered useful for us to send the secretary and the director of the ALRC, George Brouwer, to the conference in Vienna. […] So it was in that way that we were linked to the international community [...] »

l'administration. [...] Nous avions créé quelque chose de tout à fait nouveau : du fait de son indépendance et de ses relations avec le Parlement, le commissaire à la protection des données était perçu comme une institution très particulière[128]. » (Entretien avec Spiros Simitis)

Cette création d'agences indépendantes, dotées parfois de compétences réglementaires – c'est le cas dès 1978 de la CNIL en France – s'inscrit dans l'amorce d'un mouvement d'agencéification de l'État caractéristique du Nouveau management public (Rossi, 2013). Elle aboutit à ce que certaines compétences exécutives se voient retirées au gouvernement par le législateur, qui les confie à ces autorités administratives indépendantes. Leur autonomie vis-à-vis de l'exécutif leur permet alors bien plus qu'une simple démarche de construction de crédibilité : en se mettant en réseau, et en utilisant leurs compétences de concert, les défenseurs de la vie privée qui les dirigent parviennent peu à peu à imposer leur agenda politique. Spiros Simitis a répondu sans ambigüité par l'affirmative, lorsqu'en entretien, nous lui avons posé la question de savoir s'il avait effectivement menacé l'Union européenne d'user de ses pouvoirs pour saboter le projet d'espace Schengen en interdisant des transferts de données vers le Système d'information Schengen, à la fin des années 1980, comme le suggérait Abraham Newman (2008) dans son ouvrage sur le sujet :

« Oui. C'est absolument correct. Cela a été vu comme un cas particulier dans lequel une coopération des commissaires à la protection des données était nécessaire pour dire clairement que cela ne pouvait pas se faire. […] Nous avons dit : vous ne pouvez rien faire sans nous.[129] » (Entretien avec Spiros Simitis)

Cette première génération de défenseurs de la vie privée noua des relations avec des acteurs de la génération suivante, dont certains ont occupé des positions de pouvoir leur permettant de peser sur la production de politique publique en matière de protection des données. Par exemple, László Sólyom, qui avait été l'élève de Spiros Simitis, et avait publié plusieurs articles sur le sujet dans les années 1980 (Sólyom, 1988a, 1988b), devint en 1990 le tout premier

128 Traduit de l'anglais. Texte original : « When the quest for data protection was clearly […] defined, and the need for a legal structure was also accepted, the first principle that was underlined was the absolute necessity […] for control. And secondly, the absolute need for an institution that guaranteed […] the control of the use of data, and that at the same time […] was […] in close coordination with the Parliament. And therefore the protector of data protection was foreseen already in the first law. […] The data protector in Germany, France and so on, have to submit yearly a report on their experiences. And that report […] has to be discussed in Parliament. That's the construction, you see. And because of that construction, the controler is a very particular thing. He is not part of the administration. […] So it was something absolutely new we created, and in that independence, and in that particular relationship to the Parliament, the data protection commissioner was perceived as a very particular institution. »

129 Traduit de l'anglais. Texte original : « Yes. That is absolutely correct. Yes, that was seen as a specific case in which a cooperation also of the data protection commissioners was necessary in order to say clearly that that cannot be done. […] We said: you can do nothing without us. »

président de la Cour constitutionnelle hongroise, d'où il importa en droit hongrois les concepts de droit à l'auto-détermination informationnelle et de protection des données[130], avant de devenir président de la République de 2005 à 2010. Dans l'un de ses articles sur la protection des données de 1988, outre Stefano Rodotà et bien entendu Spiros Simitis, il citait un article de Masao Horibe (Horibe, 1984), qui avait été membre de la délégation japonaise dans le groupe d'experts préparant les Lignes directrices de l'OCDE (Kirby, 2017, p. 11), bien avant de devenir en 2016 le premier président de la Commission de protection des informations personnelles au Japon lors de sa création en 2016 (Sólyom, 1988a, p. 33-34). Nous pouvons aussi évoquer l'exemple de Marie Georges, qui travailla en France dans les années 1970 avec Louis Joinet et Philippe Lemoine, et fut très tôt embauchée par la CNIL ; elle fut un des principaux protagonistes de la négociation de la directive européenne de 1995, et son nom a été évoqué à plusieurs reprise dans des discussions informelles avec des représentants de groupes d'intérêt que nous avons rencontrés lors de déplacements à Bruxelles.

3.6. Le rôle du « paradigme de la vie privée » dans la *privacy community*

Comme le rappelle Colin Bennett (1992, p. 127), une *policy community* comme la *privacy community* est cimentée par un système de convictions partagé :

> « La convergence résulte de l'interaction au sein d'une communauté politique [*policy community*] disposant d'une expertise et une motivation partagées, et qui opère au-dessus du cadre de la politique nationale. Un consensus qu'une motivation cristallise au niveau transnational[131]. » (Bennett, 1992, p. 127)

Quel est le système de convictions qui cimente les motivations de cette communauté ?

Pour répondre à cette question, nous avons étudié à la fois des rapports et articles publiés par les défenseurs de la vie privée pendant la période allant de 1965 à 1980, et nous en avons interrogé certains en entretien sur leurs sources d'inspiration et de motivation dans leur engagement en faveur de la protection de la vie privée, et en particulier de la vie privée informationnelle. En menant cette enquête, nous avions une hypothèse, empruntée aux conclusions des travaux de Colin Bennett et Charles Raab : le fait que ces acteurs adhéraient au

130 Cour constitutionnelle de la République hongroise, décision 15/1991. (IV. 13.) AB.

131 Traduit de l'anglais. Texte original : « Convergence results from the interaction within a policy community which is bound by a shared expertise and motivation and which operates initially above the fray of national politics. A consensus a motivation crystallizes at the transnational level. »

paradigme libéral de la vie privée (Bennett et Raab, 2003). Cette hypothèse s'est pour l'essentiel vérifiée.

Le constitutionnaliste italien Stefano Rodotà, proche du parti communiste italien, qui le fera élire député en 1979, qui participa aux travaux de la *privacy community* et fut président de l'autorité italienne de protection des données bien des années plus tard, pourrait sembler ne pas partager cette adhésion au paradigme libéral de la vie privée, et se rapprocher d'une approche marxiste[132]. Son intervention à la conférence organisée en 1974 par l'OCDE à Vienne sur la protection des données se distingue en effet des autres par ses références marxistes, et par sa critique de la vie privée comme étant matériellement et historiquement un privilège de la bourgeoisie. Dans cette même intervention, il aborda la question de la protection de la vie privée à l'échelle non de l'individu, mais des collectifs :

> « L'homme de la rue n'est pas toujours en mesure de saisir toute l'importance que peuvent avoir certaines informations pour des organismes complexes, nantis d'un pouvoir élaboré de traitement des données. […] En outre, l'énorme différence de poids qui existe entre l'individu isolé et les grands organismes qui recueillent les données est parfaitement évidente. Dans ces conditions, parler de « contrôle » est purement illusoire. […] En conséquence, il importe de renverser la tendance et de passer des moyens de défense individuels aux mécanismes de contrôle sociaux. En suivant cette voie, certains moyens dont l'individu disposait jusqu'à présent risquent bien de se perdre, mais cette perte sera largement compensée par la création, au niveau collectif, d'un système de contrôle plus attentif et plus efficace que tout ce qui existait auparavant. » (Rodotà, 1974, p. 159-160)

Mais, même si cela semble contradictoire, il mentionna aussi à plusieurs reprises l'impossibilité de définir un noyau d'informations ne devant sortir de la sphère privée, déterminé à l'avance et pour tous, ontologiquement opposé à un ensemble informationnel qui peut ou doit (selon les cas) relever de la sphère publique. Dans l'extrait ci-dessous, il appelle ainsi à l'établissement de mécanismes de « contrôle », qu'il oppose, à la façon d'Edward Shils ou d'Alan Westin, au « secret » :

> « […] il ne suffit pas de définir, d'une part, un « noyau individuel » de la vie privée dont la protection absolue doit être garantie et, d'autre part, un domaine d'information qui intéresse le public en général et qui doit bénéficier d'autorisations modulées de circulation et de diffusion. Compte tenu des modifications qui sont intervenues dans la définition même de la notion de vie privée, c'est au contrôle et non plus au secret qu'il faut donner la place. » (Rodotà, 1974, p. 158)

132 Cf. section 2.3.3.

Lui aussi citait, dès le début de son intervention à ce colloque, les travaux d'Alan Westin et d'Arthur Miller, qui comptent parmi les principaux théoriciens du paradigme libéral de la vie privée. Il partagea le constat d'une perte de terrain d'une définition consistant à protéger la sphère prédéfinie de l'intime au profit d'une définition centrée sur le contrôle qu'exerce l'individu sur les informations qui le concernent :

> « Il faut souligner que le droit à une certaine intimité perd constamment du terrain dans les définitions du droit à la vie privée au profit de la possibilité donnée à l'individu d'exercer un contrôle sur la communication des informations qui le concernent. » (Rodotà, 1974, p. 149)

Nous retrouvons donc cette idée de « contrôle » qui est au cœur du paradigme libéral même dans une intervention de Stefano Rodotà.

En France, nous avons vu le rôle qu'ont joué Mai 68 et ses idéaux dans la mobilisation de personnes comme Marie Georges, Philippe Lemoine, ou encore Louis Joinet. Aux Pays-Bas, les organisations qui se sont mobilisées étaient proches du mouvement « provo », lui-même proche des mouvements soixante-huitards français qui se sont révoltés entre autres contre le conservatisme religieux. En même temps, comme nous l'avions vu, la première argumentation que nous avons trouvée en faveur d'un « droit à l'oubli » numérique, à la Chambre des représentants des États-Unis d'Amérique en 1966, s'était appuyée sur des arguments religieux judéo-chrétiens.

Toujours sur le registre des contrastes, en France, en 1977, Philippe Lemoine avait publié, sous le pseudonyme de Jean-Philippe Faivret, avec Dominique Wolton et Jean-Louis Missika, en collaboration avec la CFDT, un ouvrage intitulé *Les dégâts du progrès* qui s'inquiète notamment du développement de l'informatique (Faivret, Missika et Wolton, 1977). L'image qu'ils se font de l'informatique n'est évidemment pas la même que celle d'ingénieurs comme Paul Baran, Willis Ware, ou les membres de la *British Computer Society* (BCS). Ces derniers ont écrit qu'un de leurs objectifs prioritaires était de lutter contre ce qu'ils considéraient comme des craintes sur l'informatique alimentées par des mythes. Mais, comme nous l'avons vu, cela n'empêcha pas une partie au moins de ces mêmes informaticiens de s'inquiéter eux aussi des conséquences de la numérisation d'informations sur des personnes sur les conditions de possibilité d'exercice du droit *à la* vie privée. La BCS elle-même s'affirma favorable à l'adoption de lois contraignantes en la matière (British Computer Society, 1972).

Ainsi, quelles que soient par ailleurs les convictions personnelles des défenseurs de la vie privée qui ont constitué le noyau de la « *privacy community* » au début des années 1970, et les nuances entre eux dans leurs conceptions de la « vie privée », les théories d'Alan Westin et d'Arthur Miller et des autres théoriciens libéraux constituèrent un socle de références partagées. Le schéma ci-dessous, dans lequel chaque nœud est soit un auteur soit un rapport étudié, *illustre* quels rapports citent quels auteurs et rapports. Il n'est pas exhaustif ; en effet, il n'a pas été possible de numériser le texte de tous les documents et d'opérer un traitement automatisé sur l'ensemble des citations. Nous insistons donc sur le fait qu'il n'est qu'une illustration, et qu'il n'a pas servi à l'analyse elle-même. Mais il reste suffisant pour visualiser la place que George Orwell, Alan Westin et Arthur Miller ont eu dans les travaux sur la protection des données, sélectionnés sur la période allant de 1965 à 1980.

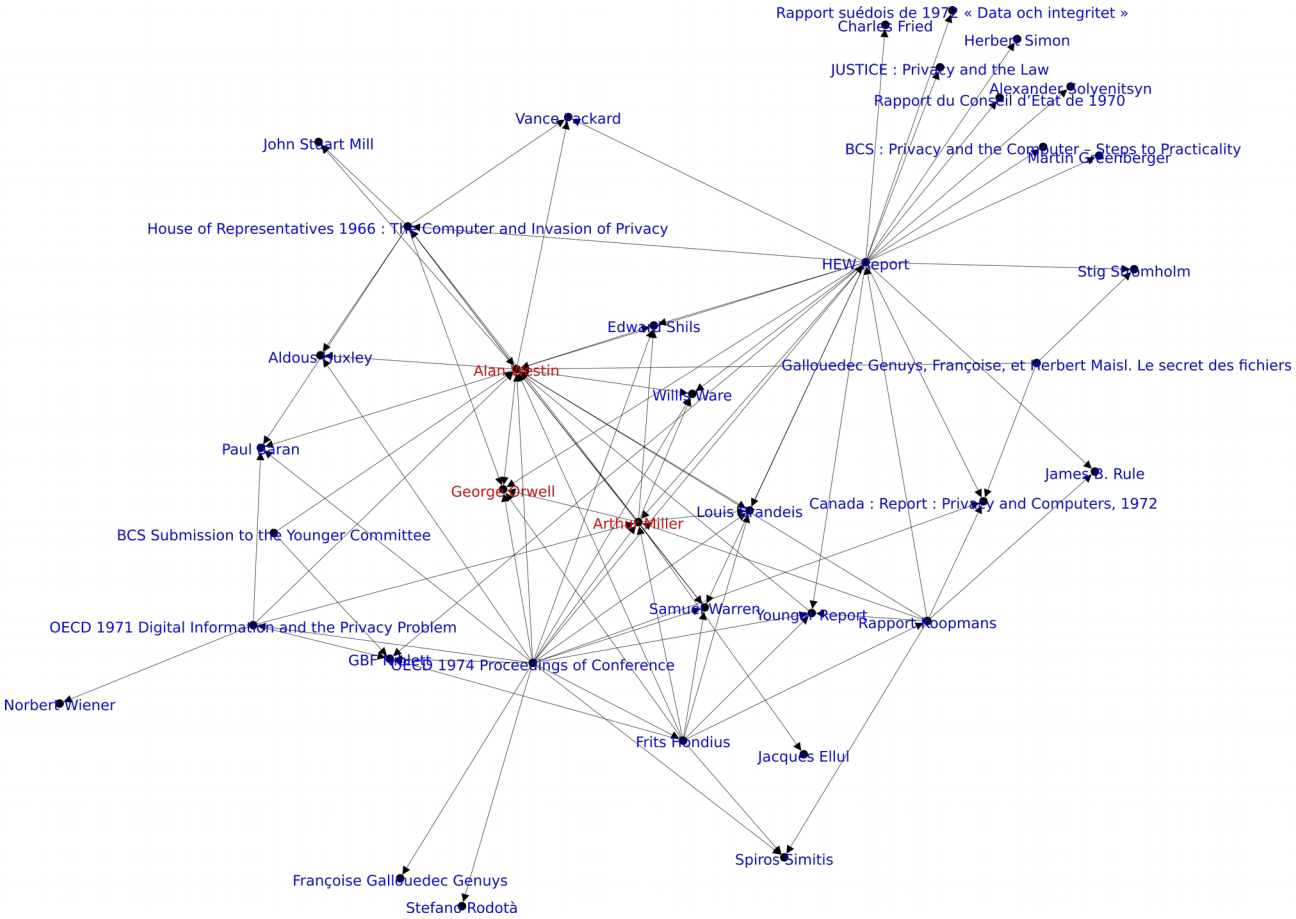


Figure 12 : *Schéma* illustratif[133] *montrant une sélection d'auteurs et de rapports et une sélection d'autres auteurs et rapports auxquels ils font référence. Alan Westin, George Orwell et Arthur Miller sont en rouge.*

133 Nous insistons sur le fait que ce schéma n'est pas conçu comme ayant une valeur *démonstrative*.

Notons au passage la centralité de la référence à George Orwell et son roman *1984*. Parvenir à l'an 1984 sans que ne se soit mis en place une société dystopique de surveillance généralisée assistée par ordinateur était, dans les mots d'un discours prononcé par Alan Westin en 1974 à un colloque de l'OCDE, un objectif essentiel à atteindre :

> « Dans dix ans environ, 1984, la date que George Orwell a rendue célèbre, apparaître sur nos calendriers. Si nous progressons avec vigueur et perspicacité dans l'élaboration des réglementations dans tous les pays avancés, nous devrions pouvoir, lorsque 1984 arrivera, non pas dire combien Orwell, à notre grand regret, a été terriblement prophétique, mais constater avec satisfaction que les sociétés occidentales ont été assez sages et assez résolues pour éviter l'abîme qu'il avait dénoncé. » (Westin, 1974, p. 120)

Rappelons que le paradigme de la vie privée est fondé sur l'idée que l'être humain est autonome, et doit pouvoir bénéficier de certaines libertés individuelles qui, suivant l'argument de John Stuart Mill, doivent lui garantir la poursuite de sa propre utilité, nul ne pouvant mieux que lui être en mesure de définir ses propres intérêts en la matière. Construit à partir de la définition de la vie privée comme un « droit à être laissé tranquille », selon l'expression de Samuel Warren et Louis Brandeis (Warren et Brandeis, 1890), il a été fortement influencé par Alan Westin et Arthur Miller, qui ont insisté dans leurs travaux sur deux aspects complémentaires. Le premier est que le droit à la vie privée est un droit *individuel*, qui doit laisser l'individu souverain dans sa décision de partager ou non une information personnelle, ou de donner ou non l'accès à soi. Le second est que la garantie de ce droit individuel est nécessaire au maintien d'un bien collectif : les institutions démocratiques de la société[134].

L'objectif d'éviter que « 1984 soit *1984* » s'est traduit donc pour les acteurs de la *privacy community* par un programme de mesures concrètes à adopter qui étaient les suivantes :

- Un champ d'application matériel du droit *de la* protection des données s'étendant – à l'exception notable des Lignes directrices de l'OCDE – à toutes les données relatives à des individus, que ces données relèvent du domaine de l'intime aux yeux des auteurs de la loi ou pas[135] ;
- Les principes de la protection des données, ou « *Fair Information Principles*[136] » ;
- L'octroi de droits aux personnes physiques sur lesquelles des données sont collectées.
- La création, dans la plupart des pays où des lois ont été adoptées, d'agences autonomes du pouvoir exécutif chargées de veiller au respect de ces principes, comme la CNIL en France.

134 Cf. section 2.2.
135 Cf. section 6.2.
136 Cf. section 3.4.4.

Le droit *individuel* à la « vie privée » fut rattaché au droit de la personnalité[137]. Après des débats initiaux sur le point de savoir s'il fallait accorder un droit *à la* protection des données aux personnes morales, comme les entreprises ou les associations, il fut décidé d'y renoncer pour ancrer ce droit fermement dans le domaine juridique des droits de la personnalité[138]. Comme le rappela le secrétariat du Conseil de l'Europe, réagissant à la demande d'une délégation nationale qui n'est toutefois pas clairement identifiée dans le document :

> « […] le souhait exprimé par une délégation que la protection fournie par la résolution soit limitée à des personnes privées et ne bénéficie pas à des personnes morales, semble raisonnable étant donné que les dangers liés au stockage des informations sont moins importants pour ces dernières[139]. » (Conseil de l'Europe, CCJ/SC.Prot.Priv. (73) 2, p. 3)

Tous ces éléments tendent à démontrer que c'est bien autour du paradigme libéral de la vie privée que se structura la « *privacy community* » en tant que *policy community* et réseau d'entrepreneurs transgouvernementaux, autour desquels allait se structurer une coalition de cause que nous retrouvons entre 2009 et 2016, pendant les négociations sur le projet de Règlement général de protection des données[140].

3.7. Le clivage entre *Common Law* et droit continental dans les arènes étudiées

La communauté de défenseurs de la vie privée qui s'est structurée entre 1965 et 1975 était donc soudée par le partage d'un système de convictions : le paradigme libéral de la vie privée. Est-ce à dire qu'il n'existait absolument pas de débats entre eux sur les mesures à adopter ?

Avant d'évoquer le principal point de clivage observé dans les débats, nous devons d'abord faire le constat que nous n'avons trouvé la trace d'aucun argument tendant à délégitimer le droit *à la* vie privée, ou à nier son existence, comme l'a fait Judith Thomson (1975) au prétexte qu'il serait un regroupement éclectique et incohérent d'une collection de droits épars déjà protégés par des règles de droit positif comme le droit à l'image, à la propriété privée, ou encore

137 Cf. section 6.2.1.

138 Ce point a été évoqué assez longuement par Spiros Simitis en entretien.

139 Traduit de l'anglais. Texte original : « […] the wish expressed by one delegation that the protection provided by the resolution should be limited to private individuals and not enjoyed by corporate bodies, seems reasonable in that the dangers from stored information are greater in the case of the former than the latter. »

140 Cf. chapitre 4.

le droit à ne pas faire l'objet d'atteintes à sa réputation. Nous n'avons pas non plus trouvé la trace d'arguments qui disqualifieraient le droit à la vie privée, ou bien sa valeur, face des impératifs économiques, comme cela a pu être le cas pendant le processus d'élaboration du RGPD[141], ou de la part de quelques acteurs issus de l'industrie de la publicité en ligne, pendant le débat sur la définition de la notion de « *tracking* » au sein du W3C[142]. Nous n'avons pas non plus la trace d'arguments qui, reprenant les théories en économie néoclassique de Richard Posner (Posner, 1977, 1981) et George Stigler (Stigler, 1980), affirment que le droit à la vie privée introduit dans le fonctionnement des marchés une opacité créant un obstacle à leur efficacité allocative[143]. La prise en compte d'arguments économiques n'a en réalité joué de rôle qu'en favorisant la mise à l'agenda de la protection des données au niveau de l'OCDE, où s'est construit le discours selon lequel des règles communes pour la protection des libertés individuelles étaient nécessaires pour garantir une libre-circulation perçue comme économiquement utile de données personnelles[144].

Nous n'avons pas non plus d'arguments fondés sur des nécessités techniques réelles ou supposées de l'informatique pour délégitimer le droit à la protection des données à caractère personnel. Les documents de la *British Computer Society*, produits en 1971 et 1972, que nous avons pu consulter, soutiennent explicitement l'adoption de lois contraignantes protégeant les données à caractère personnel (British Computer Society, 1971, 1972). Tout au plus, nous avons pu voir que des informaticiens de la BCS et de son équivalent états-unien, l'*Association for Computer Machinery* (ACM) se sont donnés pour mission de dénoncer publiquement des « mythes infondés » dont la démystification permettrait un débat plus « raisonnable » sur le sujet (British Computer Society, 1972 ; Parker, 1968).

En définitive, le principal clivage, tant aux dires des personnes interrogées qu'à la lecture des documents d'archives de notre corpus, a été celui qui recoupa une ligne de clivage traditionnelle entre des cultures juridiques de droit continental romano-germanique et des cultures juridiques de *Common Law*. Ce sont les débats suscités autour de ce point de clivage qui expliquent la bifurcation qui s'est opérée au milieu des années 1970 entre un régime de co-régulation fondé sur la jurisprudence, le marché et quelques lois sectorielles aux États-Unis d'Amérique, et un régime de réglementation contraignante et globale (« *comprehensive* ») en Europe[145].

Les pays d'Europe continentale sont des pays de droit continental, ou civiliste, c'est-à-dire des pays où « les règles de droit sont conçues […] comme étant des règles de conduite »

141 Cf. section 4.4.
142 Cf. section 5.5.4.
143 Cf. section 2.3.1.
144 Cf. section 3.4.3.
145 Le concept de « réglementation globale » (« *comprehensive regulation* » de la protection des données, a été emprunté à Colin Bennett et Charles Raab (2003) et à Fabrice Rochelandet (2010).

(David, Jauffret-Spinosi et Goré, 2016, p. 17) fixées par le législateur, et fondant une société. La culture juridique de ces pays accordait traditionnellement moins de poids aux lois qu'à la jurisprudence, c'est-à-dire aux solutions adoptées dans des cas concrets par des juges afin de trancher des litiges. À l'inverse, des pays comme l'Angleterre et le Pays de Galles[146], mais aussi les États-Unis, et de façon générale la plupart des juridictions du Commonwealth[147], sont des pays dits de *Common Law*. Cette « loi commune » y est fondée sur la règle du précédent, qui veut que la règle de droit se forme au fur et à mesure de jugements formulés dans des litiges particuliers. Ainsi, « la règle de droit de la *Common Law* […] est une règle qui vise à donner sa solution à un procès, non à formuler une règle générale de conduite pour l'avenir » (David, Jauffret-Spinosi et Goré, 2016, p. 18). Le pouvoir judiciaire est donc plus fort dans les pays de *Common Law* que dans ceux de tradition civiliste, puisque la jurisprudence est directement et explicitement source de droit positif[148]. Une autre caractéristique des pays de *Common Law* est qu'il existe entre eux une certaine forme d'unité dans les sources du droit, bien qu'elle se soit estompée à travers le temps. Cela explique les nombreuses références à des précédents britanniques dans l'article de Samuel Warren et Louis Brandeis (1890) qui cherchent pourtant à convaincre leurs lecteurs d'un droit *à la* vie privée en droit états-unien, et non anglo-gallois.

Spiros Simitis expliqua en entretien les conséquences pratiques de telles différences de culture juridique au moment de décider de ce qu'il fallait faire :

> « La question a toujours été d'abord de décrire et de définir les problèmes, ce que nous pouvions faire tous ensemble très bien. Ensuite se posait la question de savoir comment réagir. Lorsque l'on s'intéresse au continent, pour ainsi dire, c'est-à-dire à la France, il nous paraît évident de considérer que la prochaine étape est une loi. Les Britanniques ne voient pas vraiment les choses ainsi et se demandent plutôt comment réagir avec de la jurisprudence, ou bien se demandent si une loi est réellement nécessaire et dans quelle mesure[149]. » (Entretien avec Spiros Simitis)

De fait, Alan Westin, juriste d'un pays de *Common Law*, ne partageait pas l'avis de personnes comme Spiros Simitis ou Louis Joinet qui souhaitaient voir la création d'autorités de protection des données compétentes pour la supervision tant du secteur public que du secteur

146 Le droit écossais est différent du droit anglo-gallois.

147 Là encore nous noterons que la situation n'est pas uniforme dans toutes les juridictions du Commonwealth. Ainsi, au Québec et en Louisiane, il existe une influence certaine du droit romano-continental.

148 Chose interdite en France par l'article 5 du Code civil : « Il est défendu aux juges de prononcer par voie de disposition générale et réglementaire sur les causes qui leur sont soumises. »

149 Traduit de l'anglais. Texte original : « The question was always first to describe and define the problems. There we could work very well together, all of us. Then came the question: how do we react? And when you take the continental, or the continent so to say in France, it is for us normal, normal to perceive the next step as a law. For the British it is not exactly the same. For the British it was: can you do that through jurisdiction? Or do you need really a law and to what extent? »

privé. En juin 1974, il recommanda d'ailleurs au Congrès de limiter le Privacy Act qu'il allait adopter aux seules agences fédérales (Westin, 1974, p. 117). Cette voie était pour lui une voie médiane entre le choix de l'auto-régulation qui était alors celui du Royaume-Uni, et le choix « bureaucratique » de la Hesse et de la Suède :

> « Comme on pouvait s'y attendre, les différences importantes existant entre les systèmes constitutionnels et juridiques, les traditions politiques et les systèmes économiques ont produit d'importantes variations dans les formes administratives de la réglementation :
>
> a) L'approche suédo-allemande est marquée par la confiance dans des agences administratives puissantes, l'archivage et l'enregistrement ainsi que l'octroi d'autorisations par les pouvoirs publics, les codes détaillés de procédure et l'analyse administrative plutôt que juridique ;
>
> b) Le Royaume-Uni a énoncé des codes de bonne conduite que les fonctionnaires et les responsables privés doivent observer et n'interviendra en matière de législation que si ce système d'autorégulation se révèle inadéquat ;
>
> c) Les États-Unis adopteront un système définissant les normes législatives générales à suivre par les agences, les droits des individus et comptent sur les tribunaux et les contestations introduites par les citoyens pour remédier à la mauvaise gestion des agences » (Westin, 1974, p. 119-120)

Si, au Conseil de l'Europe, le Royaume-Uni était isolé face à la masse d'États de droit continental, il reçut dans les discussions dans le groupe d'experts dirigé par Michael Kirby à l'OCDE entre 1978 et 1979 un appui de poids : les États-Unis d'Amérique, auxquels s'opposait une délégation française soucieuse de voir adoptés au niveau international les principes développés au Conseil de l'Europe. Michael Kirby parla longuement de cette opposition, à la fois dans un article qu'il fit paraître en 2017, et en entretien :

> « Le chef de la délégation des États-Unis était M. William Fishman. […] Alors que Fishman réfléchissait en s'aidant d'une profonde connaissance de la technologie à laquelle nous nous intéressions, Hummer ne s'éloignait jamais trop du script écrit par le département d'État. Sans surprise, cela était conçu pour éviter que l'on impose aux États-Unis ou à ses alliés ce qui était perçu comme une approche lourde, très bureaucratique, à l'européenne, de la supervision du secteur informatique. […] Les principaux adversaires de cette formidable équipe des États-Unis étaient des fonctionnaires tout aussi brillants de la République Française, menés par M. Louis Joinet. […] Il était à l'époque responsable du développement de la législation française sur la protection de la vie privée : la *vie*

privée[150]. […] Joinet était assisté dans le groupe d'experts par un collègue : Philippe Lemoine. Dans mes souvenirs, ce dernier travaillait aux services diplomatiques français, au Quai d'Orsay. Il faisait ressortir l'excellence de Joinet. Chacun d'eux pouvait défendre longuement et avec passion ce qui était habituellement une posture pan-européenne au sujet de la cause commune qu'étaient la Convention du Conseil de l'Europe et les principes directeurs de l'OCDE[151]. » (Kirby, 2017, p. 10)

« […] les Européens réunis autour de la table, qui représentaient à l'époque la majorité des membres de l'OCDE, désiraient ardemment que l'OCDE accueille, soutienne et applique les conventions du Conseil de l'Europe. À l'inverse, les Américains souhaitaient mettre en place des principes moins bureaucratiques dans leurs modalités, qui laisseraient de la marge au pouvoir judiciaire, qui bénéficient d'une plus grande confiance dans les pays de Common Law que les bureaucrates[152]. » (Entretien avec Michael Kirby)

La création d'autorités de contrôle, chargées notamment de la mise en œuvre, comme en France, de mécanismes de déclaration préalables voire de demandes d'autorisation des traitements de données à caractère personnel, semblait trop bureaucratique pour les experts de tradition de *Common Law*, bien qu'ils adhérassent à la *privacy community*. Cela tendrait d'ailleurs à expliquer le fait que ni les Lignes directrices de l'OCDE, ni d'ailleurs la Convention 108, n'imposent l'adoption de tels mécanismes par les États membres.

Le clivage entre pays de *Common law* et pays de droit continental se doubla d'un débat sur l'importance relative entre deux droits fondamentaux : le droit à la liberté d'expression et le droit à la vie privée. Leur importance relative n'était en effet pas la même aux États-Unis et en Europe[153]. Là où le Premier amendement à la Constitution des États-Unis d'Amérique interdit absolument au législateur d'adopter des lois pouvant restreindre l'étendue de la liberté

150 NDT : en français dans le texte.

151 Traduit de l'anglais. Texte original :« The leader of the United States delegation was Mr. William Fishman. […] Whereas Fishman brought to his thinking a deep knowledge of the technology we were dealing with, Hummer never strayed far from the script written by the State Department. Unsurprisingly, this was designed to prevent the imposition on the United States or its allies of what was seen as a heavy handed European-style bureaucratic supervision of the informatics industry. […] The leading antagonists for this formidable United States team were equally briliant officials of the French Republic. Dominant amongst these was Mr. Louis Joinet. […] He was serving at the time on the development of the French laws for the protection of privacy: *La vie privée*. […] Joinet was supported in the expert group by a colleague, Philippe Lemoine. My recollection was that he was an officer of the French Diplomatic Service at the Quai d'Orsay. He was a foil to Joinet's brilliance. Each of them could speak long and passionately in defence in what was usually a pan-European posture, concerning the common cause of the emerging CE Convention and OECD Guidelines. »

152 Traduit de l'anglais. Texte original : « […] the Europeans that were sitting around the table, who were most of the members of the OECD at that time, were keen to get the OECD to embrace, endorse, and apply the Council of Europe conventions. And on the other hand, the Americans were keen to develop principles that would be less bureaucratic in their arrangements, that would preserve proper room for the judiciary, who were more trusted in the Common Law countries than bureaucrats are. »

d’expression, l’article 10 de la CEDH s’attarde longuement sur les conditions selon lesquelles il est possible de la restreindre :

Premier amendement à la Constitution des États-Unis d’Amérique	Article 10 de la CEDH
« Le Congrès ne fera aucune loi qui touche l'établissement ou interdise le libre exercice d'une religion, ni qui restreigne la liberté de la parole ou de la presse, ou le droit qu'a le peuple de s'assembler paisiblement et d'adresser des pétitions au gouvernement pour la réparation des torts dont il a à se plaindre[154]. »	« 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations. 2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. »

Tableau 8 : *Comparaison entre le Premier amendement à la constitution des États-Unis d’Amérique et l’article 10 de la Convention EDH.*

Peter Hustinx se rappela en entretien du fait que des diplomates américains soient venus parler à des membres du groupe d’experts du Conseil de l’Europe, aux alentours de la période où furent signés les Accords d’Helsinki. Ces derniers étaient inquiets de l’adoption dans plusieurs

153 Les différences entre le droits états-unien et droit européen en matière de liberté d’expression restent aujourd’hui importantes, et sources de conflit de droit dans la régulation des contenus en-ligne (voir : Bird, 2001 ; François, 2014 ; Weiss, 2014).

154 Traduit de l’anglais par l’équipe de la Digithèque de matériaux juridiques et politiques de l’Université de Perpignan, à l’URL : https://mjp.univ-perp.fr/constit/us1787a.htm (page consultée le 11 mars 2020). Texte original : « Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. »

pays européens de lois de protection des données dont il leur semblait qu'elles pouvaient aboutir à restreindre la liberté d'expression. Michael Kirby se souvint lui aussi de l'emploi par la délégation américaine d'arguments reposant sur la prééminence de la liberté d'expression durant les discussions, cette fois-ci à l'OCDE :

> « […]Les délégations américaines, en particulier celle des États-Unis, étaient très sceptiques quant au système des commissaires à la protection des données, qu'elles considéraient comme trop lourd et fastidieux, et comme un système bureaucratique potentiellement intrusif. Elles ont affirmé que ce système ne serait d'aucune manière adopté aux États-Unis, tout en suggérant qu'il pourrait même être inconstitutionnel dans leur pays en raison du premier amendement à la Constitution, qui garantit la liberté d'expression et la liberté d'expression des idées, et qui les protègent de toute intrusion législative[155]. » (Entretien avec Michael Kirby)

Nous avons retrouvé une trace des craintes évoquées par des juristes de *Common Law* que la consécration d'un droit général *à la* protection des données à caractère personnel empiète sur le terrain de la liberté d'expression et de la presse, dans l'annexe d'une proposition de convention internationale sur la protection de la vie privée rédigée par l'Union internationale des avocats en 1971, et transmise au Comité de coopération juridique du Conseil de l'Europe :

> « Les experts anglo-saxons souhaitaient inclure les textes suivants comme paragraphes finaux respectivement des Articles 14 et 15 :
>
> > « Le fait que les données aient uniquement été acquises à des fins de publication ou qu'elles aient été ainsi publiées, et que cette publication soit dans l'intérêt public, constitue un moyen de défense contre une action intentée en vertu de l'article suivant. »
> >
> > « Le fait qu'une telle publication soit dans l'intérêt public constitue un moyen de défense contre une action intentée à la suite des actions illégales définies ci-dessus. »
>
> Les arguments avancés par les experts anglo-saxons étaient les suivants :
>
> > « Puisque la principale justification de la liberté de la presse est que celle-ci sert

155 Traduit de l'anglais. Texte original : « […] The American delegations, in particular the United States delegation, were very skeptical towards the very heavy handed, labour intensive, and potentially intrusive bureaucratic system of the data protectison commissioners. And they made it plain that there was no way that that would be adopted in the United States of America, and indeed they suggested that it might be unconstitutional to have such a system in the United States, because of the provisions of the First Amendment to the United States constitution, guaranteeing free expression and free flow of ideas and protecting that from legislative intrusion. »

l'intérêt du public, notamment en lui révélant des informations que celui-ci devrait connaître, il peut exister des situations dans lesquelles même les types de publications énoncés dans le présent article peuvent être dans l'intérêt du public. […]. »

Les autres membres du Comité de rédaction […] s'étaient exprimés unanimement contre l'inclusion de toute exonération de responsabilité. [156] […] » (Conseil de l'Europe, CCJ/Prot.Priv. (71) 1, p. 20)

Il est vrai que les entreprises de presse sont consommatrices d'informations sur des individus. Le droit à la vie privée peut entrer en conflit avec le principe de la liberté d'expression s'il aboutit à ce que par exemple des personnalités publiques, par exemple des élus, puissent s'en servir pour empêcher des journalistes d'enquêter sur des activités qu'elles mènent dans le cadre de leur mandat public. C'est pour cela que selon Peter Hustinx, le droit *de la* protection des données à caractère personnel a émergé de l'espace entre le droit *à la* vie privée et le droit *à la* liberté d'expression, protégés respectivement par les articles 8 et 10 de la CEDH. Ce nouveau domaine du droit, devenu depuis une nouvelle catégorie de droit fondamental en tant que droit *à la* protection des données à caractère personnel, devait permettre de résoudre des arbitrages en cas de conflit entre droit *à la* vie privée et droit *à la* liberté d'expression (Hustinx, 2013 ; entretien avec Peter Hustinx). Une analyse similaire avait été faite en Hongrie par László Sólyom, un proche de Spiros Simitis (Sólyom, 1988a, 1988b).

Face à ces objections, l'argument de l'obstacle potentiel aux flux de données transfrontière dû à des conflits de droit fut régulièrement avancé au sein de l'OCDE pour justifier le rapprochement des législations nationales. Par exemple, le compte-rendu d'un colloque organisé à Vienne en 1977 juste avant la création du groupe d'experts en charge de la rédaction de Lignes directrices à l'OCDE mentionne Paul Sieghart, l'auteur de *Privacy and Computers*, publié en 1976 (Sieghart, 1976), affirmant que :

156 Traduit de l'anglais. Texte original : « The Anglo-Saxon experts wanted to include the following texts as the final paragraphs of Articles 14 and 15 respectively:

« It shall be a defence to an action brought under the following article that the data was acquired solely for the pruposes of publication or that it was so published, and that such publication was in the public's interest. »

« It shall be a defence to an action brought as a result of the illicit acts defined above that such publication was in the public's interest. »

The explanation advanced by the Anglo-Saxon experts was as follows:

« Since the prime reason for the freedom of the press is that it furthers the public's interest, in particular by revealing to the public information which it should know, there may be instances when even the forms of publication referred to in this article may be in the public's interest. […] »

The other members of the Drafting Committee […] were unanimously against including exemption from liability. [...] »

« […] les différences existant entre lois sur la protection des données montrent bien l'utilité d'une convention internationale qui permettrait de se prémunir contre deux maux différents engendrés par les phénomènes suivants : d'une part le phénomène des lacunes[157] fait que différentes réglementations s'appliquent dans différents pays ; les exploitants seront alors incités à traiter les données d'ordre individuel dans un pays doté d'un régime plus laxiste […] ; d'autre part, le phénomène des chevauchements[158] tient à ce qu'une seule opération de traitement des données peut être soumise à deux ou plusieurs réglementations susceptibles d'être incompatibles, peut-être au point d'empêcher que l'opération puisse être exécutée […] » (OCDE, DSTI/ICCP/77.47, p. 38)

L'argument économique, sous la forme du spectre du protectionnisme en matière de données, fut également repris par Louis Joinet lors de la même conférence à Vienne, comme le montrent ses propos rapportés dans le rapport qu'en a fait le secrétariat de l'OCDE :

« Les technologies nouvelles engendrent une circulation non plus strictement internationale mais « supranationale » qui risque d'échapper de plus en plus à la souveraineté des États. De l'avis de M. Joinet, si nous devions retarder indéfiniment d'éventuelles initiatives en vue d'une réglementation internationale, nous risquons de laisser se développer certaines politiques protectionnistes. » (OCDE, DSTI/ICCP/77.47, p. 37)

Frits Hondius dressa un parallèle entre « paradis de données » et « paradis fiscaux », notant que les premiers risquaient de se développer, avec les mêmes conséquences néfastes que les seconds, si aucun traité international ne venait fixer un niveau de réglementation minimum applicable partout :

« La fonction d'un traité international dans ce domaine serait comparable à celle des traités d'ordre fiscal qui doivent permettre aux particuliers d'éviter une double imposition. De même, si un système d'information fonctionne simultanément dans plusieurs pays, il convient d'éviter de multiples réglementations et autorisations là où une seule suffirait. En revanche, les paradis de données peuvent s'avérer aussi, sinon plus, néfastes que les paradis fiscaux » (DSTI/ICCP/77.47, p. 45)

157 Souligné dans le texte
158 Souligné dans le texte.

Ces arguments ont pu servir pour convaincre les gouvernements nationaux à endosser les Lignes directrices de l'OCDE, et à signer, puis ratifier, la Convention 108 du Conseil de l'Europe. Mais ils ont également été mobilisés pour convaincre de l'utilité d'un accord sur des principes généraux communs y compris au sein même de la communauté des défenseurs de la vie privée ceux qui craignaient que des lois trop générales protégeant les données à caractère personnel même dans le secteur privé empiéteraient sur les compétences des juges et sur le droit à la liberté d'expression.

Finalement, la création d'autorités de contrôle en charge de donner leur avis sur des traitements de données à caractère personnel n'est rendue obligatoire ni par les Lignes directrices, ni par la Convention 108 de 1981. L'article 13 de cette dernière impose certes aux États l'ayant ratifiée de désigner une autorité chargée de servir de point de contact national dans le cadre d'une coopération entre autorités nationales ayant des compétences en matière de protection des données. Mais il n'y est pas précisé qu'elle doive être créée spécialement dans un but de contrôle de l'application de la convention, ni qu'elle doive disposer de pouvoirs particuliers en la matière. Les articles 20 à 22, sur la coopération internationale, des Lignes directrices de l'OCDE ne mentionnent même pas l'existence d'autorités de contrôle.

Les États signataires sont ainsi laissés libres par ces textes de décider de définir les institutions, procédures et sanctions que leurs législateurs jugent adéquates[159] pour faire appliquer les principes de la protection des données.

La formulation de ces principes en des termes généraux perçus comme « peu bureaucratiques », technologiquement neutres, et qu'ils aient été inventés au Royaume-Uni et aux États-Unis, les rendait acceptables aux yeux des juristes de *Common Law*. Le fait qu'ils soient contraignants dans la Convention 108, puis repris dans les Lignes directrices de l'OCDE, les rendait acceptables aux juristes de droit continental :

> « Les Européens, en particulier, se réjouissaient de voir à quel point les Principes directeurs de l'OCDE avaient été inspirés en substance à l'identique des principes utilisés par le Conseil de l'Europe. […] Et le représentant du Conseil de l'Europe, dr. Frits Hondius, des Pays-Bas, était un homme poli, doux, et expert dans le domaine de la vie privée. Il était d'une très grande aide sans être agressif ; s'il l'avait été, il aurait suscité le mécontentement des Américains. Il était coopératif. Il n'insistait pas sur le fait que les pratiques européennes étaient les seules possibles mais il tentait d'assurer au mieux

159 Voir notamment l'article 19 des Lignes directrices, et l'article 4 de la Convention 108. Ce dernier dispose ainsi : « Chaque Partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés dans le présent chapitre. » L'article 19 des Lignes directrices exprime la même chose, dans une formulation beaucoup plus longue.

l'influence des deux conventions de protection des données[160] dans l'élaboration des principes de l'OCDE, afin d'éviter le plus possible les dangers et le manque d'efficacité qui découleraient du développement de deux systèmes internationaux, du moins d'un système régional et d'un système international, qui soient incompatibles[161]. » (entretien avec Michael Kirby)

Le soutien de la délégation états-unienne à ces principes débloqua la possibilité d'un accord entre celle-ci et la délégation française, ce qui de fait engendra un consensus général au sein de l'ensemble du groupe d'experts :

« L'entente entre Américains et Français sur un accord de base, réunissant les deux principaux antagonistes à la table du groupe d'experts, fut une étape très importante car les autres participants purent alors respirer librement. Les Anglo-saxons étaient rassurés car les Américains étaient prêts à suivre les Principes directeurs tels qu'ils avaient été élaborés. Les Européens étaient également prêts à les suivre, car la France, le plus vigoureux défenseur des efforts du Conseil de l'Europe, de la protection des données et d'une structure bureaucratique de protection de celles-ci, était prête à suivre la manière dont les Lignes directrices avaient été élaborés[162]. » (Entretien avec Michael Kirby)

« Les Lignes directrices de l'OCDE, telles que finalisés, n'avaient pas la force juridique d'un traité contraignant qui aurait potentiellement soulevé des problèmes par rapport au premier amendement à la Constitution des États-Unis[163]. » (Kirby, 2017, p. 11)

160 NDA : il s'agit ici d'une référence aux recommandations du Conseil de l'Europe de 1973 et 1974, et non à la Convention 108.

161 Traduit de l'anglais. Texte original : « Particularly the Europeans were pleased to see the extent to which the principles which had been used by the Council of Europe were being adopted as substantially the same principles in the OECD Guidelines. […] And the representative of the Council of Europe, dr. Frits Hondius, from the Netherlands, was a very polite and gentle and expert man in the field of privacy. And he was a great help, but without being aggressive. If he had been aggressive he would have had a bad reaction from the Americans. But he was supportive, he was not insistent that the European way was the only way, but he was trying to ensure as far as possible that the principles of the two automated data conventions would be influential in the design of the OECD principles so that to the greatest extent possible we would at least avoid the inefficiencies and dangers of developing two global, or least a regional and an international system, that would be incompatible. »

162 Traduit de l'anglais. Texte original : « When the Americans and the French reached a basic agreement, that resolved the two chief antagonists at the table of the expert group, that was a very important development, because it meant that the other participants could breathe easily. The Anglo-Saxons could breathe easily, because the Americans were willing to go along with the Guidelines as prepared. The Europeans were willing to go along with it, because France, which had been the most vigorous defender of the Council of Europe's efforts and of data protection and of a bureaucratic structure to protect data, was willing to go along with the way the Guidelines had been drafted. »

163 Traduit de l'anglais. Texte original : « The OECD Guidelines, as finalised, fell short of a binding treaty that would have potentially presented problems with the First Amendment of the U.S. Contistution. »

Une fois qu'un consensus entre les acteurs de la *privacy community* sur les mesures concrètes à rédiger dans les textes normatifs visant à garantir la protection des données à caractère personnel fut trouvé, quelles sont les stratégies argumentatives qu'ils ont déployé pour légitimer et faire accepter leurs revendications ? Ont-ils eu à articuler leur référentiel du paradigme libéral de la vie privée à un référentiel global[164], et si oui, quelle fut leur stratégie pour y parvenir ?

3.8. Le rôle de l'argument de la confiance sur la période 1966 – 1981

Parvenir à un consensus en interne était une chose. Mais les défenseurs de la vie privée présents dans les deux arènes étudiées n'étaient pas, surtout au début des années 1970, dans des positions de pouvoir décisionnel. Or, pour devenir loi, les mesures de protection des données à caractère personnel proposées devaient être approuvées tant au niveau des organisations intergouvernementales comme l'OCDE et le Conseil de l'Europe par les ministres compétents, que, au niveau national, par des majorités de parlementaires. Il fallait donc que cette coalition d'acteurs parvienne à convaincre des acteurs extérieur à leur groupe du bien-fondé de leurs idées. Quelles furent leurs stratégies argumentatives ?

En empruntant aux approches cognitives des politiques publiques, nous avons vu que pour convaincre, il était essentiel qu'un groupe d'acteurs soit capable d'articuler son référentiel, ou système de convictions, à un référentiel de niveau supérieur (sectoriel ou global). Ici, nous avons vu comment s'est formé un système de convictions, la conception libérale de la vie privée, qui, couplé à une certaine perception du développement de l'informatique, a construit un nouveau problème public auquel une nouvelle catégorie de droit, le droit *de la* « protection des données » devait offrir des solutions. Comment les défenseurs de la vie privée sont-ils parvenus à articuler leur référentiel au référentiel global, de sorte à en faire le référentiel sectoriel du nouveau domaine d'action publique qu'ils ont contribué à créer, et quel était ce référentiel global ?

Avant les années 1980, le référentiel global partagé au moins dans les pays du bloc de l'Ouest peut être décrit comme un paradigme de « modernisation » (Müller, 1984), positiviste, et conforme aux théories de l'économiste John Maynard Keynes (Keynes, 1977 [1936]). Ce paradigme est favorable à une intervention de l'État dans l'économie de marché capitaliste en raison de l'instabilité structurelle de celle-ci. S'inscrivant dans une logique productiviste, la théorie keynésienne est favorable à la dépense publique, y compris rendue possible par la dette, en particulier lorsque celle-ci peut servir à financer des mesures contra-cycliques de relance de la

164 Voir la définition de ce terme en section 1.1.

demande en réaction à des crises économiques ou des projets d'investissement (Hall, 1986, 1993).

En France, par exemple, la *Théorie générale* de Keynes (Keynes, 1977 [1936]) fut traduite en 1942, mais ne commença à toucher son public qu'après la fin de la guerre. Dans le contexte d'un pays ruiné par la guerre, les théories de Keynes, qui offrent une légitimité à l'intervention de la puissance publique dans la sphère de l'économie privée, trouvèrent un écho favorable. La nouvelle génération de hauts fonctionnaires qui parvenait alors au pouvoir se mit à considérer la modernisation et la croissance économique, aidée par des politiques de dépense publique, comme un objectif, une priorité politique en soi (Rosanvallon, 1989).

Nous trouvons par exemple la trace de ce changement de « climat idéologique » (Müller, 1984, p. 21) en matière de politique agricole. Dans *Le technocrate et le paysan*, Pierre Müller (1984) a montré que l'État, qui jusqu'alors menait une politique de maintenance des paysans sur leurs terres (Müller, 1984, p. 11), se mit à mener, après la Seconde guerre mondiale, une politique visant à industrialiser un secteur agricole demeuré « traditionnel » et « en surnombre » (Müller, 1984, p. 11). La réforme des politiques agricoles dans les années 1950 et 1960 passa notamment par la suppression de la fonction de « directeur des services agricoles » qui, jusqu'alors, jouaient dans les départements un rôle important dans l'animation de la société rurale agricole traditionnelle (Müller, 1984, p. 15-16). Pierre Müller l'explique par le fait que le référentiel sectoriel de ce corps de fonctionnaire était tourné vers une vulgarisation de savoirs scientifiques qui visait à aider des paysans à maintenir une production permettant leur auto-suffisance et leur maintien sur le territoire ; l'inadaptation de leur référentiel sectoriel au nouveau référentiel global entraîna leur disparation (Müller, 1984, p. 108).

Le référentiel global keynésien et de modernisation a été dominant dans l'ensemble des pays du bloc de l'Ouest jusqu'au tournant néolibéral des années 1980 (Hall, 1986 ; Jobert, 1994). La volonté de moderniser les économies et de soumettre les marchés à l'intervention planifiée de l'État accéléra la création d'indicateurs économiques, et d'institutions chargées de les produire. La comptabilité nationale se développa beaucoup à cette époque. Le Produit Intérieur Brut (PIB), inventé par Simon Kuznets aux États-Unis au début des années 1930, devint assez rapidement l'indicateur par excellent du développement économique. En France, la loi de finances du 27 avril 1946 acta la création l'Institut national de la statistique et des études économiques (INSEE), très peu de temps après celle d'un Commissariat général au Plan, chargé de produire des plans d'action économique quinquennaux[165]. Des institutions similaires furent créées ou bien renforcées dans d'autres pays. La collecte de l'information et son traitement efficace devinrent une des « fonctions principales » de la puissance publique, dans les mots de G.B.F. Niblett, dans son rapport livré en 1971 à l'OCDE :

165 Décret n° 46-2 du 3 janvier 1946 portant création à la présidence du Gouvernement d'un conseil du plan de modernisation et d'équipement et fixant les attributions du commissaire général du plan.

> « L'une des fonctions principales du secteur public, des ministères et des autorités centrales et locales est de recueillir, d'évaluer et de transmettre des informations, le tout de manière efficace et économique[166]. » (Niblett, 1971, p. 10)

Disposer de données précises et exhaustives, ainsi que d'une capacité de calcul efficace et rapide, parut, dans un tel contexte, très utile. La comptabilité nationale, et la statistique publique, furent identifiés très tôt comme des domaines d'application de l'informatique. C'est dans ce contexte qu'émergèrent les projets de « centres de calcul » nationaux, par exemple aux États-Unis (Atten, 2013 ; Kraus, 2013). C'est également dans ce contexte que le traitement des réponses aux questionnaires du recensement décennal, qui s'appuyait déjà sur des cartes perforées, a été informatisé dès la fin des années 1950 aux Pays-Bas (Holvast, 2013). Petit à petit, divers fichiers manuels gérés par l'État furent informatisés : permis de conduire, cadastre, fichiers de police, sécurité sociale…

Le lien entre développement des activités de l'État, et notamment de l'État-providence, et celui de l'informatique, fut fait par R.D. Blekeli, un universitaire osloïte présent au séminaire organisé en 1974 par l'OCDE à Paris :

> « Il semble se dégager de la société une tendance générale à réglementer davantage les questions d'ordre individuel. Cette tendance se vérifie aussi bien dans le secteur public que dans le secteur privé. La notion clé, en l'espèce, est celle de l'« État-Providence » (Welfare State) qui entretient avec l'individu des relations analogues à celles qui existent entre un employé et son entreprise. La société – ou l'entreprise – offre des bénéfices sociaux, des facilités de logement, des soins médicaux, etc. ; en échange, elle demande des taxes ou autres compensations et surtout le droit d'exercer un contrôle accru sur l'activité de l'individu. […] Les fonctionnaires de tout rang sont cependant constamment incités à réduire les coûts et les ressources absorbées par le processus administratif. Le traitement électronique de l'information […] constitue à cet égard un instrument de travail unique en son genre. » (Blekeli, 1974, p. 75)

L'extrait ci-dessus illustre comment, bien qu'au milieu des années 1970, le reflux de l'État caractéristique du tournant néolibéral des années 1980 n'était pas encore intervenu, l'informatique jouait déjà un rôle dans des politiques de réduction des coûts administratifs

166 Traduit de l'anglais. Texte original : « A principal function of the public sector, of government departments and central and local authorities, is the collection, evaluation and transmission of information and the carrying of this function in an efficient and economic manner. »

Les fabricants d'ordinateurs vantaient la capacité de calcul jamais égalée de leurs machines, capables de traiter un grand volume de données en un temps record, et de les croiser[167]. En 1954, une publicité de Remington Rand pour son ordinateur, l'UNIVAC, vantait ainsi l'infaillibilité de sa machine[168], puis, en 1956, la vitesse « phénoménale » de calcul[169].

En entretien, Spiros Simitis a rappelé que l'informatique était perçue dans les années 1960, par de nombreux hauts-fonctionnaires autour de lui, comme un outil porteur de la promesse de politiques publiques plus « rationnelles », plus « scientifiques » :

> « […] à l'époque, lorsque vous étudiiez cela, il fallait toujours se rendre compte que pour la société, quel que soit le pays, une nouvelle ère avait débuté, une nouvelle ère qui allait permettre de disposer de connaissances et de les exploiter de manière absolument objective [170][…] » (Entretien avec Spiros Simitis)

En Suède aussi, les années 1960 furent marquées par le développement de nombreuses applications de gestion administrative pour le compte de l'État, au nom de la modernisation et de la rationalité (Ilshammar, 2007). Hans Corell, qui a participé au groupe d'experts de l'OCDE qui a rédigé les Lignes directrices, avait par exemple été en charge de l'informatisation du cadastre suédois avant de rejoindre ce groupe[171].

Le référentiel global de modernisation, qui intègre cette vision d'une informatique au service de décisions publiques rationnelles, s'opposait donc logiquement à l'adoption de mesures comme des lois de protection des données personnelles, pouvant restreindre l'usage de l'informatique décisionnelle :

> « Il y avait une opposition évidente. Parce que les gouvernements, les parlements, étaient persuadés que l'on entrait dans un nouvel état dans la façon de prendre des décisions et

167 Le discours sur le « Big Data », défini comme la rencontre entre la vitesse de traitement, la variété et le volume des données (Laney, 2001), est donc au moins aussi ancien que l'informatique électronique.

168 Voir la publicité de Remington Rand archivée sur le site archive.org, et disponible en-ligne à l'adresse : https://archive.org/details/univac1954

169 Voir la publicité de Remington Rand archivée sur le site archive.org, et disponible en-ligne à l'adresse : https://archive.org/details/UNIVAC-AD-2

170 Traduit de l'anglais. Texte original : « […] at the time, when you study that, you always have to realise that for society at the time, irrespective of whether it was Germany, France, Italy, or whatever, a new era had started, a new era which would allow you to have a knowledge, to use that knowledge in an absolutely objective way […] »

171 Source : entretien avec Hans Corell

que ce nouvel élément permettrait d'avoir, je dirais, l'objectivité ultime[172]. » (Entretien avec Spiros Simitis)

« Lorsque les débats sur l'automatisation […] ont commencé, ils employaient […] les mots « données à caractère personnel ». Et les données personnelles étaient utilisées parce qu'elles étaient considérées comme un objet permettant […] d'élaborer certaines politiques publiques, de leur servir de fondement, d'expliquer pour qui ces politiques seraient pertinentes[173]. » (Entretien avec Spiros Simitis)

Le souvenir d'avoir été confronté à ces arguments est confirmé par le texte de son intervention lors du séminaire organisé à Paris par l'OCDE en 1974 sur la protection des données, dans lequel il évoque le fait que la protection des données était « souvent » vue comme un obstacle, un « danger », au progrès technique :

« En ce qui concerne les progrès techniques, la protection des données a souvent été considérée comme un danger sérieux. Selon ce point de vue, réglementer les méthodes d'information équivaut à restreindre indiscutablement toute tentative visant à améliorer les techniques existantes […]. » (Simitis, 1974, p. 98)

Contrairement, par exemple, aux discours qui furent ceux du CLODO et des fondateurs de *Terminal*, en France, à la toute fin des années 1970 et au début des années 1980, inspirés du luddisme ou de théoriciens de la Décroissance comme Ivan Illich et Jacque Ellul[174], le paradigme de la modernisation n'est pas frontalement remis en cause dans les documents qui ont constitué notre corpus d'analyse.

Alan Westin concédait ainsi que l'informatique fût utile, et son développement souhaitable, tout en évoquant la nécessité de précautions pour que celui-ci se fasse d'une façon conforme aux « traditions démocratiques » :

« Le fait est que la société américaine souhaite à la fois une meilleure analyse de

172 Traduit de l'anglais. Texte original : « There was an evident opposition. Because the governements, parliaments, were persuaded that you enter a new state in the decision process. And that new state in the decision process would allow you, I would say, the utmost objectivity. »

173 Traduit de l'anglais. Texte original : « When the discussions on automation […] started, they used […] the words « personal data ». And the personal data was used because the personal data was seen as an object permitting […] to develop certain policies, to base certain policies, to explain for whom those policies would be relevant. »

174 Cf. section 2.4.3.

> l'information *et* davantage de vie privée. Depuis que la Constitution a été rédigée, nos efforts pour obtenir à la fois l'ordre et la liberté ont porté leurs fruits, parce que nous avons trouvé des moyens de confier de l'autorité au gouvernement tout en le limitant par des principes, des procédures et des mécanismes d'examen clairs, qui protégeaient les droits. Une société libre ne devrait pas avoir à choisir entre une utilisation plus rationnelle de l'autorité et une vie privée personnelle si nos talents de gouvernement démocratique sont exploités à ces fins. Le bien le plus précieux dont nous disposions actuellement est le délai de quelques années avant que ce problème ne dépasse nos capacités de contrôle. Si nous agissons maintenant, et de manière judicieuse, nous pouvons encore trouver un juste équilibre dans les attentes contradictoires que soulèvent la question de la surveillance des données, s'inscrivant dans cette même tradition de solutions démocratiques et rationnelles[175]. » (Westin, 1967a, p. 537)

Dans la note explicative accompagnant la proposition de résolution sur la protection de la vie privée vis-à-vis des banques de données électroniques dans le secteur public, rédigée par le groupe d'experts du Conseil de l'Europe, en 1973, il est aussi écrit que l'informatique améliore l'efficacité de l'administration (Conseil de l'Europe, EXP/Prot.Priv. (73) 11, p. 2). Plus loin, il y est même clairement rappelé que la proposition ne visait surtout pas à remettre en cause le développement de l'informatique, mais au contraire, à « renforcer » ce développement par des « garanties » :

> « De plus, afin d'éviter tout malentendu, le préambule réaffirme que l'utilisation d'ordinateurs à des fins d'administration publique devrait généralement être considéré comme un progrès. L'objectif de la présente Résolution n'est pas de s'opposer à une telle utilisation mais de la renforcer en posant certaines garanties[176]. » (Conseil de l'Europe, EXP/Prot.Priv. (73) 11, p. 6)

L'utilité de l'ordinateur dans la grande entreprise de modernisation de l'État et de la société est aussi concédée en introduction de la synthèse rédigée par Hans Peter Gassman et

175 Traduit de l'anglais. Texte original : « The fact is that American society wants both better information analysis *and* privacy. Ever since the Constitution was written, our efforts to have both order and liberty have succeeded because we found ways to grant authority to govermnent but to tie it, down with the clear standards, operating procedures and review mechanisms that protected rights. A free society should not have to choose between more rational use of authority and personal privacy if our talents for democratic government are brought to bear on the task. The most precious commodity we have now is the few years of lead-time before this problem grows beyond our capacity for control. If we act now, and act wisely, we can balance the conflicting demands in the area of data surveillance in that same tradition of democratic, rational solutions. »

176 Traduit de l'anglais. Texte original : « Furthermore, in order to avoid any misunderstanding, the preamble reaffirms that the use of computers for purposes of public administration should in general be regarded as a positive development. The purpose of the present Resolution is not to oppose such use, but to reinforce it with certain guarantees. »

Gordon Russel Pipe au compte-rendu du séminaire sur la protection des données organisé par l'OCDE à Paris en 1974 :

> « Dans la plupart des pays de l'OCDE […] on assiste à une augmentation rapide du volume des données d'ordre individuel qui sont collectées par des organismes publics ou privés. Ce phénomène reflète assurément la complexité croissante de nos sociétés développées. La nécessité de digérer, gérer et orienter leur fonctionnement sous ses nombreuses facettes exige des informations précises et à jour. Les innovations dans le domaine de la technologie moderne de l'information, en particulier dans celui de l'informatique et des télécommunications, confèrent de nouvelles dimensions aux méthodes traditionnelles d'enregistrement et d'archivage » (Gassman et Pipe, 1974, p. 13)

Rappelons d'ailleurs que c'est parce que l'informatique était généralement perçue en son sein comme un « progrès » technique fondamental que l'OCDE a mis à son agenda, à partir de 1968, la question des flux de données électroniques transfrontières puis l'étude du développement de lois nationales de protection des données qui, si elles divergeaient trop, pouvaient y mettre des obstacles.

Les défenseurs de la vie privée ont donc pris le temps de rassurer les acteurs extérieurs au groupe. Nombre de ces derniers voyaient et jugeaient le phénomène d'informatisation des fichiers de données personnelles à travers la grille de lecture d'un référentiel global moderniste et keynésien favorable à ce phénomène au nom de la rationalité administrative et économique. Nous verrons comment l'axiologie du paradigme libéral de la vie privée a été articulée avec succès à ce référentiel global, par la construction d'un discours de légitimation des lois de protection des données fondé sur l'argument de la *confiance* en le développement de l'informatique que seules celles-ci pouvaient maintenir ou rétablir chez les citoyens. Les mobilisations qui avaient eu lieu aux Pays-Bas, et qui s'étaient soldées par un nombre important de refus de participer au recensement leur permettaient d'ailleurs de démontrer l'utilité de la confiance du public pour garantir le bon fonctionnement de systèmes de collecte de données personnelles.

La *British Computer Society*, dans un rapport daté de 1972, soutint l'adoption d'une loi de protection de la vie privée vis-à-vis de l'informatisation des données personnelles. L'un des arguments avancés dans le rapport y est la volonté de rétablir le confiance du citoyen en l'informatique :

> « Pour qu'une législation, quelle qu'elle soit, visant à contrôler les banques de données, soit équitable, elle doit à la fois tenir compte de la défiance que ces dernières suscitent et

des contraintes qu'elle pourrait imposer à des banques de données potentiellement bénéfiques. Une telle législation doit à la fois apaiser les craintes du public et permettre un développement par les opérateurs dans une atmosphère raisonnablement libérée de l'appréhension engendrée. Les opérateurs doivent clairement bénéficier d'une protection, et une réflexion sur la nature et l'ampleur de cette protection pose un certain nombre de questions[177]. » (British Computer Society, 1972, p. 18)

Nous avons retrouvé l'argument de la confiance évoqué aussi dans un rapport explicatif annexé à la proposition de loi fédérale allemande de protection des données de 1972, traduite et envoyée aux membres du groupe d'experts du Conseil de l'Europe en 1973 :

« Les dispositions sur la protection des données devraient donner au citoyen un sentiment légitime de sécurité face au pouvoir des entreprises et des administrations, armées comme elles le sont des derniers appareils technologiques. Les dispositions dans la proposition de loi peuvent favoriser la confiance nécessaire dans le traitement moderne des données[178]. » (Conseil de l'Europe, EXP/Prot.Priv./EDB (73) 2, p. 20)

Le rapport HEW insiste lui aussi sur les effets, qu'il présente comme désastreux, de la défiance du public sur l'efficacité des systèmes informatiques :

« […] comme dans le cas des protestations sur les campus contre les systèmes d'inscription informatisés, l'appréhension et la méfiance, même celle d'une minorité, peuvent grandement compliquer ne serait-ce qu'une opération sûre et simple de collecte et d'archivage de données, qui pourrait présenter un avantage social indéniable[179]. » (Ware, 1973, p. 29)

177 Traduit de l'anglais. Texte original : « For any legislation to control data banks to be equitable it must take account of the emotional distrust which they arouse, and the constraints on the development of potentially beneficial data banks which this may produce. Further legislation should both allay public fears, and permit development by operators in an atmosphere reasonably free of the apprehension these engender. Operators are clearly entitled to some protection, and consideration of its nature and extent raises a number of issues. »

178 Traduit de l'anglais. Texte original : « The provisions on data protection should give the citizen a legitimate sense of security in the face of the power of businesses and the administration armed as they are with the latest technological devices. The provisions in the Bill can promote the necessary confidence in modern data processing. »

179 Traduit de l'anglais. Texte original : « […] as in the case of campus protests against computerized registration systems, the apprehension and distrust of even a minority of the public can grossly complicate even a safe, straightforward data-gathering and record-keeping operation that may be of undoubted social advantage. »

Per Svenonius, président du *Computer Utilization Group* de l'OCDE, inaugura le séminaire qu'il a organisé à Paris en 1974 sur la protection des données par un discours rappelant l'objectif de restaurer la confiance des citoyens en l'informatique :

> « Les gouvernements et les parlements ont à tenir compte du sentiment répandu dans le public suivant lequel le besoin accru d'information et la prolifération des systèmes de fichiers informatisés se traduiraient par une réduction du pouvoir d'intervention de l'individu dans les décisions qui le concernent. Il conviendrait de mettre en œuvre de nouvelles dispositions assurant un certain contrôle plus étroit de l'utilisation des fichiers individuels et une plus grande transparence de l'administration. Limiter le secret[180] aux seules informations relatives à des activités nationales ou individuelles renforcerait la confiance du public à l'égard des autorités. Les gouvernements centraux devraient donner l'exemple en établissant des normes et des instruments de réglementation relatifs à la protection des données dans l'administration publique. » (Svenonius, 1974, p. 10)

R.D. Blekeli affirma lui aussi, durant ce séminaire, que regagner la confiance des citoyens était pour lui une priorité :

> « L'objectif fondamental doit être de restaurer la confiance du public à l'égard du traitement des informations retenues par l'administration. » (Blekeli, 1974, p. 76)

Dans une présentation globalement enthousiaste de projets d'informatisation des fichiers de personne, L. Tegnhed[181], fonctionnaire suédois de l'Office national des impôts, toujours au cours de ce même séminaire, concéda aux défenseurs de la vie privée l'importance de la confiance du public en l'informatique pour mesurer l'efficacité d'un système d'information électronique :

> « Il faut […] reconnaître que l'efficacité d'un système ne se mesure pas seulement au volume de la production et au degré d'élaboration, mais aussi à la confiance qu'il suscite dans le grand public, car cette dernière influe sur son aptitude à accepter le système et à y participer. » (Tegnhed, 1974, p. 129-130)

L'argument de la confiance s'est aussi retrouvé dans le préambule de la Résolution de 1974 du Conseil de l'Europe :

180 NDA : il s'agit du secret opposé par l'administration à une demande de d'accès d'un individu aux informations qui le concernent, ou à des documents administratifs.

181 Nous ne connaissons que l'initiale de son prénom.

« Le Comité des Ministres,

[…]

Désireux de contribuer à la compréhension et à la **confiance**[182] du public à l'égard des nouvelles techniques administratives que les autorités publiques mettent en œuvre dans les États membres **en vue d'assurer une meilleure exécution des missions dont elles sont chargées**[183] ;

Conscient que l'utilisation des banques de données électroniques par les autorités publiques a provoqué dans l'opinion publique une prise de conscience accrue de la nécessité de protéger la vie privée des individus ;

[…] » (Préambule de la Résolution (74) 29 du Conseil de l'Europe)

Il nous est méthodologiquement et épistémologiquement impossible d'évaluer les intentions et d'accès aux états internes des enquêtés. Il en découle une impossibilité de savoir s'ils étaient eux-mêmes convaincus par cet argument de la confiance, ou s'il s'agissait d'une simple stratégie rhétorique pour ancrer la légitimité de leurs propositions dans un référentiel global partagé au-delà de leur communauté. Mais nous pouvons supposer qu'il s'agissait plutôt d'une stratégie rhétorique.

Le risque que Spiros Simitis décrivait en entretien comme ayant été perçu dans les années 1960, était que des décisions prises sur la base d'un traitement algorithmique automatisé de données à caractère personnel devienne opaque et impossible à contester. Nous avons déjà vu que la science-fiction dystopique de l'époque sur les ordinateurs a joué un rôle axiologique, au même titre, de façon générale, que des arguments d'inspiration libérale sur le droit à l'autonomie individuelle. De surcroît, dans les échanges entre défenseurs de la vie privée au sein des deux arènes étudiées, nous n'avons pratiquement pas trouvé de trace de cet argument de la confiance. Il ne semble donc pas que l'argument de la confiance ait joué de rôle *axiologique* pour expliquer la motivation des acteurs qui ont milité pour l'adoption de mesures contraignantes de « protection des données ». Mais cet argument a bien joué un rôle essentiel dans la *légitimation* de ces mesures à l'égard du référentiel global modernisateur.

182 Formatage ajouté par l'auteur.
183 Formatage ajouté par l'auteur.

3.9. Conclusion du chapitre

La façon dont fut perçue l'apparition de l'ordinateur électronique aux États-Unis d'Amérique dans les années 1950 et 1960 comme un problème en devenir, la sortie de l'époque McCarthy, et le contexte de mouvements civiques, sont des facteurs qui se sont conjugués pour remettre la question du droit à la vie privée à l'agenda des juristes et du personnel politique de ce pays[184]. Les travaux de William Prosser (Prosser, 1960), inspirés du droit à la vie privée qui avait été théorisé à la fin du XIXe siècle par Samuel Warren et Louis Brandeis (1890), firent évoluer et précisèrent la doctrine juridique états-unienne en précisant le contenu du droit *de la* vie privée. En 1965, la Cour suprême a jugé dans « Griswold contre Connecticut » que le droit *à la* vie privée était bel et bien protégé au niveau constitutionnel, car sous-entendu par certains amendements à la constitution fédérale du pays. Des ouvrages, publiés notamment par Vance Packard (Packard, 1965), Alan Westin (Westin, 1967a, 1967b) ou encore Arthur Miller (Miller, 1971), ont tenté d'alerter leur public sur l'érosion du droit *à la* vie privée face aux nouvelles pratiques et technologies de surveillance, dont l'ordinateur. En 1966, la Chambre des représentants, puis, en 1967, le Sénat, constituèrent des commissions d'enquête sur le sujet. Certains informaticiens de la Rand Corporation, comme Paul Baran et Willis Ware, s'intéressèrent eux aussi au sujet.

Si l'ordinateur a joué un rôle aussi central dans la remise à l'agenda du droit *à la* vie privée aux États-Unis d'Amérique, c'est que son image sociale, liée au complexe militaro-industriel dont il est issu, n'était guère rassurante. La science-fiction, que ce soit dans la littérature avec *1984* de George Orwell, le cinéma, avec *2001 l'Odyssée de l'espace*, ou encore les séries télévisées populaires, avec *Star Trek*, montrait des ordinateurs au rôle ambivalent et anxiogène. Les rapports officiels que nous avons lus font d'ailleurs régulièrement référence à *1984*. Comme suggéré par la seconde hypothèse, c'est donc bien à une *certaine perception* de l'ordinateur que la revendication de mesures de « protection des données » pour protéger la « vie privée » (notamment sa conception libérale) et d'autres libertés publiques doit son existence.

La controverse sur les banques de données électroniques traversa l'Atlantique à la fin des années 1960, et s'y trouva reconfigurée dans de nouvelles arènes. D'un contexte de *Common Law*, la discussion se poursuivit dans un contexte où prédominaient des conceptions de droit continental.

En 1968, l'Assemblée parlementaire du Conseil de l'Europe a adopté une résolution appelant cette organisation intergouvernementale à entamer des travaux de réflexion pour déterminer dans quelle mesure le droit de l'époque permettait, en l'état, d'assurer l'application de l'article 8 de la Convention EDH, protégeant le droit *à la* vie privée, dans un contexte de

184 Cf. section 3.2.

développement de techniques perçues par ses auteurs comme intrusives[185]. La même année, l'OCDE s'inquiéta des disparités entre États-membres en matière d'informatique, et des réunions eurent lieu où il commença à être question de flux de données numériques transfrontières[186]. Dans l'une de ces organisations, la réflexion était fondée sur des préoccupations en matière de droits fondamentaux ; dans l'autre, le cadrage initial était centré sur des préoccupations économiques. Mais dans les deux organisations, cela a abouti, au début des années 1970, à la mise en place de groupes d'experts étudiant le droit *à la* vie privée et son rapport avec le développement de l'informatique. Juste avant, en 1970, le land ouest-allemand de Hesse venait d'adopter la première loi de « protection des données » au monde[187], inaugurant l'emploi d'une formule qui, traduite, allait entrer dans le vocabulaire juridique de toutes les langues officielles européennes (González Fuster, 2014a).

La démarche généalogique adoptée a permis de voir que l'invention d'un droit *à la* protection des données à caractère personnel n'allait pas de soi, n'était pas sans poser problème, sans controverse, sans construction d'un discours de légitimation. À l'intérieur des arènes étudiées, nous avons vu qu'il existait une opposition entre juristes de *Common Law* et de droit continental sur la valeur et la nature des mesures à adopter, en raisons de différences de culture juridique, mais aussi d'une différence de conception non pas tant du droit *à la* vie privée que du droit *à la* liberté d'expression et de la liberté de la presse[188]. À l'extérieur de la coalition, la coalition industrielle rivale, déployant un discours et des arguments néolibéraux, très active, comme nous le verrons dans le chapitre suivant dans les discussions qui ont entouré le processus d'adoption du RGPD entre 2009 et 2016, n'existait pas encore. Mais il a néanmoins fallu que les défenseurs de la vie privée articulent leurs propositions de textes juridiquement contraignant avec un référentiel global selon lequel de tels textes pouvaient être un obstacle à l'efficacité de l'informatisation, de l'automatisation et donc (selon ce référentiel) de la rationalisation de la décision publique grâce à l'informatique et à la quantité rapidement traitée de données collectées[189]. Cette articulation s'est faite par l'invocation de l'argument de la confiance. Autrement dit : les défenseurs de la vie privée sont parvenus à convaincre à l'extérieur de leur groupe que pour que les systèmes d'information électroniques soient réellement efficaces, il fallait éviter que la population ne s'en méfiâte, ce qui impliquait de devoir adopter des mesures – par exemple des lois de protection des données – de nature à regagner la *confiance* du public[190]. Cet argument, qui s'est révélé efficace, fut aussi au cœur de la stratégie argumentative des défenseurs de la vie privée pendant les débats sur l'adoption du RGPD, comme nous allons le voir dans le chapitre qui suit immédiatement.

185 Cf. section 3.4.2.
186 Cf. section 3.4.3.
187 Cf. section 3.3.2.
188 Cf. section 3.7.
189 Nous voyons ainsi, dès les années 1960 et 1970, apparaître un discours qui deviendra, dans les années 2000, le discours sur les promesses du « *Big Data* ».
190 Cf. section 3.8.

Notons enfin que, si conformément aux hypothèses 2 et 3, le but initial des défenseurs de la vie privée de l'OCDE et du Conseil de l'Europe a bien été de protéger la « vie privée », et en particulier sa conception libérale, de l'intrusion par l'ordinateur, un glissement s'opéra et a conduit en Europe à une séparation au moins partielle entre les catégories que sont le droit *à la* protection des données et droit *à la* vie privée. Louis Joinet exprima lui-même cette impression de glissement lors de la conférence organisée à Vienne en 1977 par l'OCDE :

> « 72. Si l'on remonte à la période 1970-73, a-t-il déclaré, celle-ci pourrait être qualifiée de période « informatique et vie privée ». Elle se caractérisait par une approche essentiellement juridique et orientée vers la défense de la personne humaine ou des droits de l'homme [sic] contre l'ordinateur. À la suite de nombreux rapports, réunions de comités, projets de loi, le problème s'est trouvé projeté à l'échelon international, c'est-à-dire au niveau du Conseil de l'Europe et de l'OCDE. L'étude et l'analyse du problème de la protection des données ont montré qu'« il ne s'agit là que d'un aspect particulier d'un problème beaucoup plus général qui, au-delà des libertés, concerne la démocratie, à savoir la libre circulation de l'information ».
>
> 73. La deuxième période allant de 1974 à 1976 pourrait être intitulée : informatique et démocratie. « J'emploie à dessein le mot démocratie, a poursuivi M. Joinet, car, au début, nous n'avions pas clairement saisi cette évidence, à savoir qu'en termes de pouvoir, le traitement de l'information comporte des dimensions éminemment politiques et économiques ». Il s'agissait alors de la circulation de l'information globale et non plus seulement de l'information sur les personnes, ce qui pose une tout autre problématique, et notamment celle de l'accès à l'information. En France, le Premier ministre a créé une commission spéciale chargée de faciliter l'accès des citoyens à la documentation administrative. » (OCDE, DSTI/ICCP/77.47, p. 36)

Nous reviendrons sur cette question en conclusion du chapitre 6, après avoir étudié spécifiquement les controverses définitionnelles autour de la rédaction de la définition de la notion de « donnée à caractère personnel ». L'étude de la formation de la rédaction de la définition de cette notion permet en effet de mieux comprendre la nature de ce glissement, que l'adoption de la directive communautaire de 1995 puis du RGPD en 2016 ne semblent pas remettre en cause.

Chapitre 4 : L’adoption du RGPD (2009-2016)

4.1. Introduction du chapitre

4.1.1. De la Convention 108 au RGPD

Nous avons vu qu’il existe plusieurs façons d’appréhender la « vie privée », tant au niveau du contenu, c’est-à-dire du sens de ce terme, qu’au niveau de sa valeur, de sa désirabilité sociale[1]. Nous venons de retracer la généalogie du droit *de la* protection des données à caractère personnel, en observant la façon dont une coalition transnationale a imaginé cette nouvelle catégorie de droit en réaction au développement de bases de données informatisées perçues comme une menace pour les libertés publiques, au premier rang desquelles une conception libérale du droit *à la* vie privée. Les travaux de ce groupe ont notamment donné naissance aux Lignes directrices de l’OCDE de 1980 et à la Convention 108 du Conseil de l’Europe de 1981[2].

28 ans s’écoulèrent entre 1981, date de la signature de la Convention 108, et 2009, au moment où la Commission européenne a entamé un processus qui aboutira à l’adoption, en 2016, du Règlement général de protection des données (RGPD). Entre temps, l’ordinateur est devenu un bien de consommation courant. L’informatique a rendu possible ou contribué à de profondes transformations de la société[3]. Dans le même temps, la disparition de l’URSS transformait l’organisation du système international, et, sous l’influence des théories monétaristes, le tournant néolibéral des années 1980 a balayé l’ancien référentiel global modernisateur qui était compatible avec les idées keynésiennes (Hall, 1986 ; Jobert, 1994). À la vue de telles évolutions, nous pourrions croire qu’il serait parfaitement logique que le droit ait à s’adapter et s’adapte aux nouvelles réalités du milieu technique, et que, pour cela, le RGPD marque une rupture avec ce qui existait précédemment. Nous pourrions également supposer que l’argumentaire déployé par les défenseurs de la vie privée dans les années 1960 et 1970 ait perdu de son efficacité, notamment en raison du remplacement du référentiel global auquel il permettait d’articuler le paradigme libéral de la privée pour en faire le paradigme sectoriel des politiques publiques de protection des données. Ce dernier aurait alors pu être remplacé par une autre conception de la « vie privée ». Un tel changement de référentiel sectoriel dans les politiques publiques de protection des données aurait alors, toujours selon cette logique, dû entraîné une transformation des dispositions concrètes du droit *de la* protection des données à caractère personnel, à

1 Cf. chapitre 2
2 Cf. chapitre 3
3 Voir par exemple : Castells, 1998 ; George, 2019 ; Moulier Boutang, 2007

commencer par les grands principes et peut-être la définition même de la notion de « donnée à caractère personnel ».

Pourtant, après avoir vu comment l'Union européenne s'est progressivement imposée comme lieu central de production des normes juridiques de protection des données en Europe, nous verrons que le RGPD représente une évolution, mais absolument pas une révolution, du droit des données à caractère personnel. Malgré tous ces changements de contexte que nous venons de décrire, l'essentiel des principes et définitions sont restés remarquablement stables. Nous verrons en étudiant les controverses qui ont accompagné l'adoption de ce règlement que le paradigme libéral de la vie privée a finalement très bien résisté, et que l'argument de la nécessaire confiance du public qui l'articulait avec l'ancien référentiel global keynésien n'a en rien perdu de son efficacité avec le référentiel global qui dominait les discussions sur l'adoption du RGPD entre 2009 et 2016.

4.1.2. La communautarisation du droit des données à caractère personnel

Nous venons dans le chapitre précédent que l'échelon européen est pertinent à étudier pour comprendre la formation de ce droit nouveau *de la* protection des données à caractère personnel. Mais lorsqu'en 1981 les États du Conseil de l'Europe signaient la Convention 108, cela n'impliquait pas encore les Communautés européennes issues des traités de Paris (1951) et de Rome (1957)[4]. L'adoption d'une directive de protection des données par la Communauté

4 À ce stade, il est utile de faire un point sur la terminologie utilisée. Lorsqu'en 1957 le traité de Rome institua, en plus de la CECA, créée par le traité de Paris de 1951, l'Euratom et la CEE, chaque communauté disposait de son propre exécutif, c'est-à-dire de sa propre commission (appelée Haute Autorité dans le cas de la CECA). Les trois communautés partageaient toutefois la même Cour de Justice, et la même Assemblée parlementaire (qui ne devint « Parlement européen » qu'à partir des premières élections européennes, en 1979). La fusion des trois exécutifs communautaires n'intervint qu'en 1967, en application du traité de Bruxelles de 1965, dit Traité de fusion des exécutifs. À partir de cette date, une seule Commission européenne exerça ses compétences sur les trois communautés, qui conservèrent leurs personnalités juridiques. Entre temps, le traité de Maastricht de 1992 a consacré la formule d'« Union européenne » (UE) qui, à l'époque, ne disposait pas de la personnalité juridique. Le terme « UE » désignait trois « piliers » : la CEE, au fonctionnement dit « communautaire », mais aussi la Politique étrangère et de sécurité commune (PESC) et la Coopération policière et judiciaire en matière pénale (CPJP, ou JAI pour Justice et Affaires Intérieures). Les deux derniers piliers étaient intergouvernementaux, et non pas communautaires, car les décisions étaient prises à l'unanimité entre représentants des États membres, sans intervention de nature supranationale et contraignante du Parlement européen et, surtout, de la Cour de justice des communautés européennes (CJCE). Le Conseil des Communautés européennes prit toutefois l'appellation de Conseil de l'Union européenne dès l'entrée en vigueur du traité de Maastricht en 1993 (Mangenot, 2011, p. 12).
Depuis l'entrée en vigueur du Traité de Lisbonne en 2009, les trois piliers ont été fusionnés en une même UE disposant cette fois de la personnalité juridique. D'un point de vue terminologique, l'expression « droit communautaire » (qui désignait le droit de la CEE) a été remplacée par l'expression « droit de l'UE », et la CJCE est devenue Cour de justice de l'Union européenne (CJUE), quoi qu'elle demeure encore compétente pour les affaires qui relèvent de l'Euratom (qui est restée, *de jure*, distincte de l'UE, bien que cette distinction soit devenue fort discutable *de facto*).

économique européenne (CEE) en 1995[5] a été étudiée de façon détaillée par Abraham Newman (Newman, 2008), et il ne nous a pas semblé utile de refaire cette étude. Toutefois, pour comprendre l'adoption du Règlement général de protection des données[6] (RGPD) en 2016 par l'Union européenne (UE), il faut comprendre comment le droit *de la* protection des données à caractère personnel fut mis à l'agenda politique des institutions communautaires. Nous verrons quel rôle les acteurs de la « *privacy community* » y ont joué, et la façon dont le principe du droit à l'auto-détermination informationnelle fut rattaché dans la directive de 1995 aux principes de protection des données (« *Fair Information Principles* »).

Pour comprendre pourquoi les premières discussions à l'échelon européen ont été hébergées par le Conseil de l'Europe et non par l'une des Communautés européennes, il faut rappeler que ces organisations internationales n'ont que des compétences d'attribution. Elles ne peuvent agir que dans les domaines prévus dans les traités qui les instituent, et selon les procédures qui y sont décrites. Le traité instituant le Conseil de l'Europe est le traité de Londres du 5 mai 1949. L'article un paragraphe a) de ce traité décrit le but de cette organisation comme étant celui « de réaliser une union plus étroite entre ses membres afin de sauvegarder et de promouvoir les idéaux et les principes qui sont leur patrimoine commun et de favoriser leur progrès économique et social » (art. 1 a. du traité de Londres de 1949). Le paragraphe suivant précise que « ce but sera poursuivi au moyen des organes du Conseil, par l'examen des questions d'intérêt commun, par la conclusion d'accords et par l'adoption d'une action commune dans les domaines économique, social, culturel, scientifique, juridique et administratif, ainsi que par la sauvegarde et le développement des droits de l'homme et des libertés fondamentales. » (art. 1 b) du traité de Londres de 1949).

Ainsi, dès le début, le Conseil de l'Europe s'est vu attribuer des compétences en matière de droits et libertés fondamentales, ce qui n'a pas été le cas des Communautés européennes. Le Conseil de l'Europe ne peut toutefois pas adopter d'actes juridiques s'imposant aux États membres. Les décisions de cette organisation prennent la forme de traités *ad-hoc*, comme Convention de sauvegarde des droits de l'homme et des libertés fondamentales de 1950 ou la Convention 108 de 1981, ratifiés selon les procédures nationales habituelles de ratification des

---

Le concept de « méthode communautaire » demeure toutefois utilisé pour désigner le processus de prise de décision au sein des institutions de l'UE combinant : le monopole de l'initiative législative de la Commission européenne, l'adoption avec accord du Parlement européen et du Conseil de l'Union européenne statuant selon leurs propres règles et disposant du droit d'amendement, et le contrôle du respect de ces décisions législatives par la CJUE (Magnette, 2009, p. 112).
Quant à la CECA, elle fut dissoute le 23 juillet 2002, conformément au traité de Paris de 1951 qui n'avait été conclu que pour cinquante ans et qui n'a jamais été renouvelé. Les domaines qui relevaient du traité CECA relevèrent dès lors de la compétence de la CEE, puis, à partir de 2009, de l'UE.

5 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (voir : Journal officiel des Communautés européennes 1995 n° L 281, p. 31-50)

6 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (voir : Journal officiel de l'Union européenne 2016 n° L 119, p. 1-88)

conventions internationales. À l'inverse, la CEE était conçue autour d'un objectif économique précis, perçu comme moins sensible politiquement : la constitution d'un marché commun où serait garanti la libre-circulation des biens, des services, des capitaux et des travailleurs, avec un tarif extérieur commun. Mais la CEE, contrairement au Conseil de l'Europe, était dotée de véritables compétences supranationales. Le droit communautaire, y compris celui qui dérive des traités, prime sur le droit des États membres[7], est doté d'un effet direct en droit interne[8], et s'impose même – du moins, selon la Cour de Luxembourg – sur les constitutions nationales[9].

Aujourd'hui encore, l'Union européenne ne dispose toujours pas de compétences générales en matière de droits et libertés fondamentales. Toutefois, depuis l'entrée en vigueur en 2009 du traité de Lisbonne, l'art. 6 (2) du Traité sur l'Union européenne (TUE) prévoit que « l'Union adhère à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. » (art. 6 (2) TUE), tout en précisant dès la phrase suivante que « cette adhésion ne modifie pas les compétences de l'Union telles qu'elles sont définies dans les traités » (art. 6 (2) TUE). De surcroît, cette adhésion se faisant toujours attendre, les dispositions de la CEDH ne s'imposent toujours pas *de jure* aux actes juridiques adoptés par l'UE, même si, *de facto*, la CJCE a, sous la pression notamment du Tribunal constitutionnel fédéral de RFA[10], incorporé progressivement les principes de la CEDH dans le droit communautaire à travers l'invention de « principes généraux du droit » communautaires (Jacqué, 2011 ; Philip, 1975).

En 1989 le Parlement européen avait adopté une première déclaration de droits communautaire, qui n'était pas juridiquement contraignante. Notons au passage qu'il y inscrit un article 6 protégeant le droit *à la* « vie privée », mais que le droit d'accès le droit d'accès d'une personne aux informations qui la concernent y était inscrit à l'article 18 de cette déclaration :

Article 6

(Vie privée)

1. **Toute personne a droit au respect et à la protection de son identité.**

2. **Le respect de la vie privée et de la vie familiale, de la réputation, du domicile et des communications privées est garanti.**

Figure 13 : *Extrait du Journal officiel des Communautés européennes, n° C 120, p. 54.*

7 CJCE 15 juillet 1964 « Costa contre ENEL », Aff. 6/64.

8 Voir : CJCE 5 février 1963 « Van Gend en Loos », Aff. 26/62 pour l'effet direct des traités, et CJCE 14 décembre 1971 « Politi », Aff. 43-71, pour l'effet direct des règlements.
L'effet direct des directives connaît toutefois des limites (voir : CJCE 4 décembre 1974 « Van Duyn » Aff. 41/74, et CJCE 5 avril 1979 « Ratti » Aff. 148/78).

9 CJCE 17 décembre 1970 « Internationale Handelsgesellschaft », Aff. 11/70.

10 Voir la décision « Solange » du Tribunal constitutionnel fédéral de RFA : BVerfGE 37, 271 – Solange I (29 mai 1974).

Article 18

(Droit d'accès aux informations)

Le droit d'accès et de rectification est garanti à toute personne pour les documents administratifs et les données qui la concernent.

Figure 14 : *Extrait du Journal officiel des Communautés européennes, n° C 120, p. 55.*

Une autre déclaration des droits, devenue, elle, juridiquement contraignante au moment de l'entrée en vigueur du traité de Lisbonne, s'impose à l'UE et, lorsqu'ils agissent en application du droit de l'Union, à ses États-membres : il s'agit de la Charte des droits fondamentaux de l'UE. Cette charte protège la vie privée à son article 7, et le droit à la protection des données à caractère personnel à son article 8.

Elle n'octroie toutefois pas de compétence générale à l'UE pour adopter des mesures visant spécifiquement à garantir des droits fondamentaux. Les rares domaines relevant des droits et libertés fondamentaux dans laquelle l'UE peut intervenir sans que cela ne soit rattaché à une autre base légale – telle que l'harmonisation des règles applicables sur le marché intérieur dans le cas de la directive de 1995 sur la protection des données – sont l'égalité hommes-femmes, la lutte contre les discriminations (art. 3 (3) TUE) et… depuis l'entrée en vigueur du traité de Lisbonne, le droit à la protection des données à caractère personnel (art. 16 TFUE). Mais cette dernière n'existait pas encore dans les années 1970, lorsque l'Assemblée parlementaire commença à appeler la Commission européenne à proposer une directive de protection des données à caractère personnel. Pour être en mesure de proposer l'adoption d'une directive sur la protection des données, la Commission européenne devait donc proposer une façon de cadrer cela comme étant une mesure liée au bon fonctionnement du marché intérieur, et pas (seulement) une question de droits et libertés fondamentaux.

En 1975, l'Assemblée parlementaire des Communautés européennes adopta une résolution non-contraignante[11] relative à la « protection des droits de la personne face au traitement automatique des données[12] ». Cette résolution, rédigée à la suite d'un rapport de la commission juridique de cette assemblée, « [priait] instamment la Commission, à la lumière du rapport de cette commission spéciale, d'élaborer à bref délai une directive visant à protéger, dans la Communauté, les citoyens contre les abus engendrés par la mémorisation, le traitement et la communication des renseignements personnels mémorisés dans des banques de données, aussi bien dans le secteur public que dans le secteur privé » (JOCE 1975 n° C 60, p. 49).

11 Rappelons que l'Assemblée parlementaire, et aujourd'hui, le Parlement européen, ne disposent pas du droit d'initiative législative. Ce droit est le monopole exclusif de la Commission européenne.

12 Résolution du 21 février 1975. Voir : Journal officiel des Communautés européennes 1975 n° C 60 p. 48 et s.

En 1976, elle adopte une nouvelle résolution relative « à la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique[13] », puis à nouveau en 1979[14]. Dans cette dernière, l'Assemblée parlementaire, désormais rebaptisée en Parlement européen, insista sur un nouvel argument. D'une part, il faisait « remarquer que des dispositions nationales concernant la protection de la vie privée sont susceptibles d'avoir une incidence directe sur l'établissement et le fonctionnement du Marché commun et notamment d'y fausser les conditions de concurrence »[15], et d'autre part, il estimait « qu'il ne serait pas judicieux que les institutions communautaires attendent pour agir l'apparition de perturbations sérieuses dans le fonctionnement du Marché commun »[16]. Nous voyons ainsi se construire un argumentaire visant à faire de la protection des données à caractère personnel une question de droit du marché commun, qui, lui, tombait bel et bien dans le domaine de compétence où la CEE était habilitée à adopter des règlements et directives contraignants.

En 1981, la Commission européenne répondit à ces demandes répétées du Parlement par l'adoption d'une recommandation non-contraignante encourageant les États membres à ratifier la Convention 108 du Conseil de l'Europe[17]. Il s'agit alors d'une façon de ne pas y donner suite. La Direction générale du marché intérieur de la Commission européenne considérait en effet que la protection des données personnelles ne relevait pas de son domaine, mais du domaine des droits fondamentaux, et que la Convention 108 du Conseil de l'Europe, si elle était ratifiée par l'ensemble des États membres, suffirait largement à éviter que des obstacles n'apparaisse dans la libre-circulation des données entre pays de la CEE. De plus, elle était réticente à adopter des mesures contraignantes s'imposant aux entreprises du secteur privé (Newman, 2008, p. 84-85).

Le Parlement européen réitéra pourtant sa demande en 1982[18]. Dans cette résolution, il poursuivit la construction de son argumentaire faisant de la protection des données un problème politique relevant de la matière du marché commun, en précisant même l'article du traité de Rome conférant selon lui la compétence à la CEE d'adopter des actes juridiques dans ce domaine :

> « [Le Parlement européen] renvoie à l'article 100 du traité CEE qui prévoit le rapprochement des dispositions législatives, réglementaires et administratives des États membres qui ont une incidence directe sur l'établissement et le fonctionnement du marché intérieur » (Journal officiel des Communautés européennes 1982 n° C 87 p. 40)

13 Journal officiel des Communautés européennes 1976 n° C 100 p. 27 et s.
14 Journal officiel des Communautés européennes 1979 n° C 140 p. 34 et s.
15 Journal officiel des Communautés européennes 1979 n° C 140 p. 35.
16 *Idem*
17 Recommandation de la Commission du 29 juillet 1981 concernant une convention du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (voir : Journal officiel des Communautés européennes, 1981, n° L 246, p. 31 et s.)
18 Journal officiel des Communautés européennes 1982 n° C 87 p. 39 et s.

Plus que le Parlement européen, les travaux de recherche effectués par Abraham Newman (2008) ont démontré l'importance du rôle joué par les défenseurs de la vie privée, et en particulier, du réseau transgouvernemental des autorités de protection des données instituées dans certains États européens dans les années 1970 et 1980, dans la remise en cause du *statu-quo* législatif communautaire en matière de protection des données. Leur rôle prend à contre-courant les récits de la construction européenne classiques, tant néo-fonctionnalistes, fondés sur l'idée d'un débordement des politiques supranationales de leurs champs initialement restreints de compétence sous la pression de demandes de la société civile par l'effet d'une intégration fonctionnelle (Haas, 1958 ; Lindberg, 1963 ; Mitrany, 1944), qu'intergouvernementaux, fondés sur l'idée que la construction supranationale est le fruit de moments de convergence d'intérêts d'États-nations cherchant à maximiser leur puissances, et que donc les politiques communautaires sont essentiellement le fruit de choix du Conseil, agissant sur un mode intergouvernemental (Keohane et Hoffmann, 1994 ; Mearsheimer, 1990 ; Moravcsik, 1991). En effet la directive européenne de 1995 est le fruit de ce qu'Abraham Newman désigne par le terme d'« entrepreunariat transgouvernemental » (Newman, 2008, p. 77), c'est-à-dire de l'initiative d'acteurs dotés dans leurs champs de compétence d'un morceau de pouvoir exécutif leur ayant été délégué et qui ont développé des stratégies communes pour imposer leur agenda au législateur, dans le cas présent : le législateur européen[19].

Les autorités de protection des données étaient déjà, dans bon nombre de pays, des autorités administratives indépendantes. En France, la CNIL fut même la première autorité de ce type à être créée. Elles furent caractéristiques des réformes de la bureaucratie traditionnelle à partir des années 1970, désignées de façon générique sous le terme de « Nouveau Management Public » (Caranta, Andenas et Fairgrieve, 2004 ; Talbot, 2003). Ces agences devaient accroître la légitimité de l'action publique en donnant des gages d'indépendance face au pouvoir politique, ainsi que des gages d'expertise (Schick, 2002 ; Talbot, 2003), dans des domaines où le gouvernement n'était pas perçu comme digne de confiance, comme la protection des données (Rossi, 2013), ou encore la politique monétaire (Fontan, 2014). Dans un tel processus, le législateur (ou un exécutif), le « principal », confie à des agences (« l'agent[20] ») des pouvoirs réglementaires qui, dès lors, échappent aux détenteurs traditionnels du pouvoir exécutif, c'est-à-dire aux gouvernements, morcelant ainsi en partie l'intégration horizontale de l'action publique qui caractérisait de façon idéal-typique les bureaucraties classiques (Schick, 2002). Ainsi, dans certains États européens, les autorités de protection des données disposaient sans être soumises à la tutelle de leurs gouvernements de parcelles de pouvoir réglementaire, comme celui d'adopter des décisions d'interdiction de transfert de données personnelles vers des pays n'assurant pas un

19 Abraham Newman indique que cet entrepreneuriat transgouvernemental se caractérise par : (1) une demande de changement législatif provenant d'acteurs infra-étatiques, (2) une mise à l'agenda mobilisant le registre de l'expertise, (3) la mobilisation de l'autorité dont disposent ces acteurs au niveau domestique pour altérer le statu-quo réglementaire supranational, (4) la contribution aux négociations internationales par des réseaux d'acteurs infra-nationaux cherchant à altérer ce statu-quo réglementaire au niveau supranational (Newman, 2008, p. 77).

20 Voir : Elgie, 2002.

niveau qu'elles jugeaient adéquat de protection du droit *à la* protection des données à caractère personnel[21].

En 1988, à l'occasion de la dixième édition de l'ICDPPC, le président de l'autorité luxembourgeoise de protection des données alerta ses collègues français et allemand[22], qui disposaient alors de plus amples pouvoirs que lui, des risques qu'il percevait dans l'établissement d'une base de données informatisée de gestion des points d'entrée dans l'espace Schengen alors en construction : le Système d'information Schengen (SIS). Les autorités de protection des données réunies lors de cette conférence firent alors savoir qu'elles interdiraient les transferts de données à caractère personnel vers la Belgique dans le cadre du SIS tant que cet État n'aurait pas adopté de loi de protection des données à caractère personnel (Meunier et McNamara, 2007, p. 133 ; Newman, 2008, p. 90). En 1989, la CNIL, en France, mit ce type de menaces à exécution et fit usage de son pouvoir réglementaire pour interdire le transfert de données à caractère personnel sur les salariés de Fiat France vers le siège social de l'entreprise à Turin, en Italie (CNIL, délibération 89-78 du 11 juillet 1989).

À l'ICDPPC de 1989, profitant du fait que l'Acte unique européen, adopté en 1986, remettait les questions relatives à l'harmonisation réglementaire dans le marché intérieur européen à l'agenda, les autorités de protection des données appelèrent officiellement la Commission européenne à proposer des mesures d'harmonisation des règles nationales de protection des données. L'année suivante, en 1990, lors d'une conférence organisée au mois de mars, Spiros Simitis, alors commissaire à la protection des données du Land de Hesse, à la Commission européenne et au Conseil de la CEE :

> « S'il n'existe toujours pas de règles communes d'ici 1992 entre les 12 membres de la Communauté, alors cinq des pays de la Communauté européenne qui ne disposent pas de telles lois devront être traités exactement de la même manière que ceux qui ne disposent pas de règles de protection de la vie privée des données [*data privacy*]. Aucun transfert de données à caractère personnel n'aura donc lieu vers ces pays, puisque les commissaires aux données [*data commissioners*] s'opposeront à de tels transferts[23]. » (Spiros Simitis, 1990, cité par : Newman, 2008, p. 89[24])

21 Voir par exemple l'art. 26 de la loi Informatique et Libertés du 6 janvier 1978, dans sa rédaction d'origine.

22 Entretien avec Marie Georges.

23 Traduit de l'anglais. Texte original : « If there are no common rules by 1992 amongst the 12 Community members then quite simply five of the countries of the European Community without such laws will have to be treated in exactly the same way as those with no rules for data privacy. Therefore, there will no personal data transfers to those countries because data commissioners will oppose such transfers. »

24 Cette citation a été reprise par Abraham Newman depuis un article de revue dont nous n'avons pas retrouvé le nom de l'auteur : « Simitis Reports Data Protection Chaos », *Transnational Data and Communication Report*, juin-juillet 1990, p. 26.

En entretien, Spiros Simitis a d'ailleurs confirmé qu'il s'était bel et bien agi d'une menace destinée à pousser la Commission européenne à agir, et la narration faite par Abraham Newman du rôle des autorités de protection des données a été validée plusieurs fois dans des entretiens réalisés dans le cadre de notre terrain sur la généalogie du droit à la protection des données à caractère personnel.

En 1990, la Commission européenne finit par céder à ces demandes répétées et en proposant deux directives, l'une sur « la protection des personnes à l'égard du traitement des données à caractère personnel[25] », et une autre « concernant la protection des données à caractère personnel et de la vie privée dans le cadre des réseaux numériques publics de télécommunications, en particulier des réseaux numériques à intégration de services (RNIS) et des réseaux mobiles numériques publics »[26], présentés dans une seule et même communication publiée au Journal officiel des Communautés européennes[27]. Ces deux propositions ont donné respectivement la directive 95/46/CE du 24 octobre 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[28] », et la directive 97/66/CE du 15 décembre 1997 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications » (première directive « e-Privacy »). De ces deux directives, la directive 95/46/CE fixa le cadre général applicable aux traitements de données à caractère personnel, à l'instar du rôle joué aujourd'hui par le RGPD.

La Commission européenne s'est finalement rangée aux arguments défendus par le Parlement européen selon lesquels la protection des données était une matière relevant du droit du marché intérieur et donc d'un champ de compétence communautaire. Nous venons en effet de voir que les autorités de protection des données, en faisant usage de leurs pouvoirs réglementaires propres, avaient démontré leur capacité de nuisance et d'obstacle potentiel à la libre-circulation des données personnelles sur le territoire de la CEE, et donc à l'approfondissement du marché intérieur, une priorité de l'agenda de la commission Delors. C'est ainsi que le titre de la directive 95/46/CE se termina par « et à la libre circulation de ses données » et qu'elle fut assise sur le fondement juridique de l'article 100A TCE qui, au moment de l'adoption de la directive, était rédigé ainsi :

> « Par dérogation à l'article 100 et sauf si le présent traité en dispose autrement, les dispositions suivantes s'appliquent pour la réalisation des objectifs énoncés à l'article 7A.

25 Voir : Commission européenne, COM(90) 314

26 Voir : Commission européenne, COM(90) 314

27 Journal officiel des Communautés européennes 1990 n° C 277, p. 3 et s. pour la première proposition de directive, et p. 12 et s. pour la seconde proposition

28 Bien que le terme de « protection des données » n'apparaisse pas dans le titre de cette première directive, et rarement dans le corps de son texte, la directive 95/46/CE fut connue sous le nom de « directive de protection des données » ou « Data Protection Directive » en anglais (González Fuster, 2014a, p. 130).

Le Conseil, statuant conformément à la procédure visée à l'article 189B et après consultation du Comité économique et social, arrête les mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des État membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur [...] » (Art. 100A TCE, version consolidée au 31 août 1992, publiée au Journal officiel des Communautés européennes, 1992 n° C 224, p. 32)

Par le mécanisme de la transposition obligatoire en droit national, cette directive harmonisa textuellement à l'échelle de la CEE les définitions de la notion juridique de « donnée à caractère personnel », en imposant partout cette formule, sans forcément changer, au demeurant, le contenu même de la définition. Nous en voyons ici un exemple avec la France :

Définition dans la loi Informatique et Libertés du 6 janvier 1978 avant 2004	Article 4 : « Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale »
Définition de la directive 95/46/CE	Article 2 sous a) : « « Données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »
Définition dans la loi Informatique et Libertés après la loi n° 2004-801 du 6 août 2004 transposant la directive 95/46/CE, au 1er janvier 2005	Extrait de l'article 2 : « […]Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. […] »

Tableau 9 : *Évolution de la notion de donnée à caractère personnel en droit français.*

La directive ne modifia pas les principes de la protection des données[29] des Lignes directrices de l'OCDE et de la Convention 108. Ceux-ci s'y retrouvèrent à l'article 6. Elle apporta toutefois d'importantes précisions concernant le principe de licéité, dont les contours étaient

29 Cf. section 3.4.4.

jusqu'alors restés assez flous. Le consentement devint l'une des « bases légales » permettant à un organisme (le « responsable du traitement[30] ») de « traiter[31] » des données à caractère personnel. Le consentement était défini à l'article 2 sous h) de la directive 95/46/CE comme étant « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Les autres critères, définis à l'article 7, étaient : la nécessité de traiter des données pour l'exécution d'un contrat, le respect d'une obligation légale, la nécessité pour la sauvegarde de la vie de la personne concernée, la nécessité pour l'exécution d'une mission de service public ou relevant de l'exercice de l'autorité publique, la nécessité pour la réalisation de l'« intérêt légitime » du responsable du traitement.

L'importance donnée au consentement, comme première base légale permettant de fonder la « licéité » d'un traitement de données à caractère personnel, consacra une fusion entre le principe du droit à l'auto-détermination informationnelle avec les principes de la protection des données.

Une autre nouveauté apportée par la directive 95/46/CE, par rapport notamment à la Convention 108, est que son article 28 a imposé à tous les États membres l'institution d'autorités indépendantes de protection des données à caractère personnel, dotés de pouvoir effectifs de contrôle auprès des organismes collectant des données personnels, tant dans le secteur public que dans le secteur privé. Son article 29 institutionnalisa d'ailleurs le réseau transgouvernemental de ces autorités, en créant un « Groupe de travail de l'article 29 » (de la directive), généralement désigné en français sous l'abréviation « G29 »[32].

En 1997, l'autre directive proposée en 1990, visant à protéger la vie privée dans le domaine des communications électroniques[33], fut finalement adoptée. Elle fut abrogée par une autre directive, dite directive « e-Privacy », en 2002[34]. Cette dernière fut amendée par la directive

30 À son article 2, la directive 95/46/CE définissait ainsi de la façon suivante la notion de « responsable du traitement » : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire ».

31 À son article 2, la directive 95/46/CE définissait ainsi de la façon suivante la notion de « traitement » de données : « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, tel que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

32 Cf. 4.1.4.

33 Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

34 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

2009/136/CE[35] qui, entre autres, renforça l'obligation à l'article 5 paragraphe 3 de la directive de 2002 de demander l'autorisation à l'utilisateur d'un terminal électronique avant d'y stocker des informations ou d'y accéder[36]. Cette obligation visait notamment les *cookies* installés par de nombreux sites web sur les ordinateurs des internautes, souvent à leur insu. Elle fut, et est toujours, souvent mentionnée dans la presse comme la « loi sur les cookies[37] ». Le règlement 45/2001/CE[38] permit d'appliquer les principes de la directive 95/46/CE aux institutions communautaires, et institua un Contrôleur européen de la protection des données, généralement désigné sous l'acronyme anglais EDPS (pour *European Data Protection Supervisor*[39]). Enfin, en 2008, la décision-cadre 2008/977/JAI[40] était adoptée pour encadrer la protection des données à caractère personne traitées dans le cadre de la coopération policière et judiciaire en matière pénale de l'UE.

La dernière révision de la directive e-Privacy en 2009 fut la dernière réforme législative communautaire en matière de protection des données à caractère personnel avant que la Commission européenne n'entame son travail de réforme de la directive 95/46/CE, qui aboutit en 2016 à l'adoption du règlement 2016/679/UE (le RGPD) et de la directive 2016/680/UE[41] qui a remplacé la décision-cadre JAI de 2008.

35 Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, publiée au Journal officiel de l'Union européenne, 2009, n° L 337, pp. 11-36
Notons pour l'anecdote qu'il s'agit d'un des rares textes qui, adopté fin novembre 2009 juste avant l'entrée en vigueur du traité de Lisbonne, est une directive des Communautés européennes (d'où le fait qu'il s'agisse de la directive 2009/136/**CE**), et fut publié non plus au Journal officiel des Communautés européennes, mais dans le Journal officiel de l'Union européenne, son nouveau nom depuis décembre 2009.

36 Voir l'article 2 paragraphe 5 de la directive 2009/136/CE.

37 Voir par exemple l'article « ICO to enforce cookie law from this weekend » sur *ZDNet* (Espiner, 2012).

38 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

39 Nous conserverons l'acronyme *EDPS* au lieu de l'acronyme français CEPD, pour éviter toute confusion avec le Comité européen de la protection des données institué par le RGPD et succédant au Groupe de l'article de l'Article 29 à partir du 25 mai 2018.

40 Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

41 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

4.1.3. Le Règlement général de protection des données (RGPD)

Avant d'étudier le processus de décision ayant abouti à la signature du RGPD par les présidents du Parlement européen et du Conseil de l'Union européenne le 27 avril 2016 puis à sa publication au Journal officiel de l'Union européenne[42], il convient de rappeler la chronologie des principales étapes de ce processus[43]. Nous résumerons ensuite les principales nouveautés apportées par ce texte, pour pouvoir y faire référence plus facilement lorsque nous présenterons ensuite les points de clivage qui ont structuré la controverse autour de son adoption, et les arguments des coalitions de cause qui se sont opposées. Cet exposé nous permettra aussi de démontrer que le RGPD se situe essentiellement dans la continuité des principes et définitions adoptés dans les années 1970 et consacrés par les Lignes directrices de l'OCDE, la Convention 108 et la directive 95/46/CE.

L'essentiel de la chronologie a été rédigée sur la base des informations fournies par l'outil EUR-LEX, qui est le système d'information juridique de l'UE. Ce système intègre un outil – qui était auparavant un outil distinct, appelé PRE-LEX – permettant le suivi des procédures législatives[44].

Dès le mois de mai 2009, alors même que la directive 2009/136/CE amendant (entre autres) la directive e-Privacy de 2002, était encore en discussion, la Commission européenne organisa une conférence intitulée en anglais « *Personal data – more use, more protection?* » (« Données personnelles – plus d'utilisation, plus de protection ? »). Cette conférence fut organisée par l'unité D5 « Protection des données » de la DG Justice de la Commission européenne, sous la responsabilité du commissaire Jacques Barrot.

Après élections européennes de juin 2009, Jacques Barrot fut remplacé par Viviane Reding qui, avant juin 2009, avait été commissaire européenne à la société de l'information et aux médias. Dès le mois de juillet, une consultation fut ouverte pour recueillir des avis du public sur l'état du droit *de la* protection des données en Europe. Le 28 janvier 2010, Viviane Reding annonça que la Commission européenne avait pour projet de réformer le cadre juridique de la protection des données (Commission européenne, 2010a). En novembre 2010, un autre communiqué de presse (Commission européenne, 2010c) annonça l'ouverture d'une consultation permettant au public de donner son avis sur le contenu souhaité de cette réforme.

42 Le RGPD a été publié au Journal officiel de l'Union européenne, 2016, n° L 119, p. 1-88.
43 Ces étapes ont été résumées dans un tableau en annexe 3.
44 Voir : https://eur-lex.europa.eu/procedure/FR/2012_11 (page consultée le 4 avril 2019).

La Commission européenne publia son projet de réforme du droit de l'UE *de la* protection des données à caractère personnel en janvier 2012, dans trois communications publiées le même jour :

- Une première, intitulée « Protection de la vie privée dans un monde en réseau. Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle » (COM (2012) 9), contenait une présentation générale du projet politique de réforme de la Commission européenne ;
- Une seconde communication, numérotée COM (2012) 010, contenait la proposition de « Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données », précédée d'un exposé des motifs ;
- Une troisième communication, numérotée COM (2012) 011, contenait la proposition de « Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre-circulation de ces données (règlement général de protection des données) », précédée d'un exposé des motifs.

La proposition contenue dans la seconde communication (COM (2012) 010), qui a donné lieu à la procédure législative ordinaire[45] identifiée par la cote 2012/0010 (COD), est devenue, après amendements, la directive 2016/680/UE, et la proposition contenue dans la troisième communication, ayant donné lieu à la procédure 2012/0011 (COD), a abouti au règlement 2016/680/UE, c'est-à-dire au RGPD. C'est sur ce dernier instrument, son adoption, ainsi que les délibérations et controverses qui l'ont entouré, que nous allons nous concentrer dans notre étude.

En février, le Parlement européen désigna la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) responsable du rapport sur la proposition de RGPD. En avril, Jan Philipp Albrecht, député allemand du groupe parlementaire « Verts / Alliance libre européenne » fut désigné rapporteur, et Axel Voss, du groupe parlementaire « Parti populaire européen », « *shadow-rapporteur* » (en français : « rapporteur fictif »). Le Conseil de l'Union européenne, dans sa formation « Justice et affaires intérieures » (JAI), entama les discussions en son sein sur le RGPD le 25 octobre 2012, après une période de plusieurs mois pendant lesquelles les gouvernements nationaux furent invités à transmettre leurs remarques sur la proposition de la Commission européenne (Conseil de l'Union européenne, 2012, document 9897/12).

En 2013, les révélations d'Edward Snowden sur la surveillance exercée par les agences de renseignement états-uniennes (Greenwald, 2013 ; Lyon, 2015 ; Musiani, 2015) remontèrent les

45 Il s'agit du nouveau nom de la « procédure de codécision », qui correspond à la méthode communautaire. Elle est décrite dans les articles 289 et 294 du TFUE.

discussions sur le RGPD dans l'ordre des priorités politiques des institutions européennes. Plusieurs personnes interrogées en entretien ont d'ailleurs souligné avoir perçu un changement dans la nature des négociations, qui seraient alors devenues « plus politiques » et « moins techniques » :

> « La discussion a ensuite pris une tournure beaucoup plus politique. Pourquoi ? Évidemment, parce que nous avons eu les révélations sur la NSA, en mai 2013, je pense[46]. » (entretien Euro5)

> « Et en plus, de manière importante, les révélations d'Edward Snowden ont eu lieu trois mois après le début de nos travaux européens, ce qui a bouleversé notre programme[47]. » (Entretien avec Jens-Henrik Jeppesen)

La commission LIBE du Parlement européen vota sur les amendements proposés le 21 octobre 2013. Le rapport sur le RGPD rédigé par Jan Philipp Albrecht recueillit une vaste majorité des voix en commission, avec 48 voix pour, une contre et trois abstentions (Albrecht, 2013, p. 623). Puis ce rapport fut adopté en vote plénier le 12 mars 2014. Il fallut attendre toutefois encore plus d'un an avant qu'en juin 2015 le Conseil de l'UE publie sa propre version du texte. Une période de discussion, dite de « trilogue », entre le Parlement européen, le Conseil de l'UE et la Commission européenne suivit, pour aboutir à un texte de compromis entre les positions divergentes de ces trois institutions. Le compromis fut publié le 15 décembre 2015, validé par le Conseil de l'UE le 8 avril 2016, adopté en session plénière du Parlement européen le 14 avril 2016, signé le 27 avril et publié au Journal officiel de l'Union européenne le 4 mai.

Après une période transitoire de deux ans, le RGPD est entré en application le 25 mai 2018 dans l'Union européenne, et le 20 juillet 2018 dans les pays de l'Espace économique européen (Norvège, Islande et Liechtenstein)[48].

Le RGPD reprend l'essentiel des définitions de l'article 2 de la directive 95/46/CE, et des principes de l'article 6 de cette même directive, dont nous avons vu qu'ils trouvaient leur origine dans des textes des années 1970 et 1980[49]. La liste des critères permettant de fonder la licéité d'un traitement de données à caractère personnel du RGPD est strictement identique à celle de la directive de 1995[50]. Comme la directive de 1995, le RGPD prévoit l'existence d'autorités de

46 Traduit de l'anglais. Texte original : « Then the discussion kind of turned and became much more political. Why? Well obviously we had the NSA relevations. In May 2013, I believe. »

47 Traduit de l'anglais. Texte original : « And also, importantly, three months after we started our European work, the Edward Snowden revelations came. So this took over the agenda completely. »

48 Voir à ce sujet la Décision du comité mixte de l'EEE n° 154/2018 du 6 juillet 2018.

49 Cf. chapitre 3.

50 Article 7 de la directive 95/46/CE, et article 6 paragraphe 1 du RGPD.

protection des données exerçant leurs compétences en matière de contrôle « en toute indépendance[51] ».

Les droits des personnes physiques à l'égard du traitement des données les concernant sont décrits au chapitre III du RGPD. Ils incluent des droits déjà présents dans la directive de 1995, comme le droit d'être informé[52], le droit d'accès[53], droit de rectification[54], droit d'opposition[55]. Comme la directive de 1995, le RGPD contient des dispositions visant à encadrer, et dans de nombreux cas, interdire, les décisions automatisées[56]. D'autres droits contenus dans le RGPD, comme le droit à l'effacement[57] (ou « droit à l'oubli ») n'étaient pas explicitement reconnus par la directive de 1995, mais avaient déjà été reconnus par la jurisprudence de la CJUE sur le fondement de cette directive[58].

Le RGPD ne marque donc pas de rupture fondamentale avec le régime juridique de la directive de 1995 (Favro, 2017). D'ailleurs, pour Jan Philipp Albrecht comme pour la DG JUST de la Commission, cette directive était considérée par plusieurs acteurs centraux du processus d'adoption du RGPD comme « le niveau de garantie de base » en-deçà duquel aucun compromis sur le texte final ne pourrait être adopté (Albrecht, 2015b). Cela n'a pas empêché le RGPD d'introduire quelques modifications importantes dans le droit de l'Union *de la* protection des données, et donc dans la politique publique européenne de protection des données.

Il n'est pas notre objet de dresser un tableau exhaustif des différences. Pour donner une idée du contenu du RGPD, et mettre ainsi en contexte ce chapitre sur son adoption, il nous paraît toutefois utile d'en rappeler les principaux changements.

Tout d'abord, il s'agit d'un règlement, et non plus d'une simple directive. L'article 288 du TFUE, qui définit les actes juridiques que peut adopter l'Union européenne, définit ces deux types d'acte de la façon suivante :

- « Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre » (art. 288 TFUE) ;
- « La directive lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens » (art. 288 TFUE).

51 Article 28 de la directive 95/46/CE et articles 51 et 52 paragraphe 1 du RGPD.
52 Articles 10 et 11 de la directive 95/46/CE, et articles 12, 13 et 14 du RGPD.
53 Article 12 de la directive 95/46/CE et article 15 du RGPD.
54 Article 12 de la directive 95/46/CE et article 16 du RGPD.
55 Article 14 de la directive 95/46/CE et article 21 du RGPD.
56 Article 15 de la directive 95/46/CE et article 22 du RGPD.
57 Prévu à l'article 17 du RGPD.
58 CJUE 8 avril 2014 « Google contre Espagne », Aff. C-131/12.

Une directive doit en principe être transposée pour être utilisable. Il existe des exceptions à ce principe, les directives, même non transposées, pouvant avoir des effets juridiques dans certains cas, mais elles sont limitées[59].

Un règlement, lui, est doté d'un effet direct, et se passe de transposition. Il créée, dès son entrée en vigueur, non seulement des obligations pour les États membres de l'UE, mais aussi dans les relations entre particuliers. Même si le RGPD renvoie à 56 reprises au droit national pour préciser certains de ces éléments, comme l'âge à partir duquel un mineur peut consentir sans ses parents au traitement de ses données à caractère personnel[60], et même si la question du devenir des données personnelles des défunts est renvoyée aux législateurs nationaux (Castex, Harbinja et Rossi, 2018), il renforce l'harmonisation juridique du droit *de la* protection des données à caractère personnel dans les pays de l'UE. Là où de nombreuses dispositions de la directive de 1995 ne faisaient que fixer des objectifs généraux complétés par des dispositions nationales, le RGPD est beaucoup plus détaillé. Par exemple, le régime juridique dérogatoire applicable à l'utilisation de données à caractère personnel dans le cadre de travaux de recherche scientifique. La directive de 1995 prévoyait qu'il puisse exister un tel régime dérogatoire[61], et suggérait les contours que pouvaient prendre une telle dérogation, tout en laissant aux législateurs nationaux le soin d'adopter effectivement un tel régime, s'ils le souhaitaient[62]. *A contrario*, le RGPD, même s'il laisse une marge de manœuvre nationale, dédie un article spécifique à la description de ce régime dérogatoire (Rossi, 2015a ; Rossi et Bigot, 2018). Un autre exemple est que là où la directive de 1995 ne faisait que fixer l'objectif qu'il y ait des autorités indépendantes de supervision du respect du droit *de la* protection des données dans chaque État membre, dotés de « pouvoirs effectifs d'intervention » (art. 28 paragraphe 3 de la directive 95/46/CE), sans préciser la nature et l'étendue de ces pouvoirs, le RGPD dispose d'un article 83 décrivant de façon détaillée les pouvoirs de sanction administrative de ces autorités.

Le niveau et le montant de ces sanctions administratives que peuvent adopter les autorités nationales de contrôle sont un facteur d'explication essentiel pour comprendre l'implication en moyens humains et financiers de nombreux groupes d'intérêt industriels qui ont cherché à influencer l'issue du processus d'adoption du RGPD. Avant le RGPD, chaque État membre était libre de décider s'il permettait ou non à son autorité de protection des données d'adopter des sanctions pécuniaires administratives. Ceci avait abouti à d'importantes divergences dans le

59 Voir notamment : Conseil d'État (France), Ass., 28 février 1992, « Société Philipp Morris », publié au Recueil et CJCE 4 décembre 1974 « Van Duyn contre Home Office », Aff. 41-74.

60 Voir l'article 8 du RGPD, qui permet aux États membres de fixer cet âge entre 13 et 16 ans.

61 Son considérant 34 précisait ainsi que : « considérant que les États membres doivent également être autorisés à déroger à l'interdiction de traiter des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale - particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie - et tels que la recherche scientifique et les statistiques publiques; qu'il leur incombe, toutefois, de prévoir les garanties appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes »

62 L'article 6 paragraphe 1 sous b) précisait ainsi : « […] Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées »

risque financier de sanctions d'un État membre à l'autre (European Union Agency for Fundamental Rights, 2013 ; Rossi, 2013, p. 38-39). Le montant des amendes prononcées étaient au demeurant assez faibles. En France, la loi de 2004 de transposition de la directive 95/46/CE limitait les sanctions pécuniaires prononçables par la CNIL à 150 000 €, ou 300 000 € en cas de récidive dans les cinq ans[63]. La proposition initiale de la Commission était de porter le montant maximal des sanctions pécuniaires, selon le type d'infraction constatée, jusqu'à 1 % du chiffre d'affaires mondial d'une entreprise[64]. Ce montant fut finalement porté à l'issue de la procédure législative à 4 % du chiffre d'affaires mondial d'une entreprise, ou 20 millions d'euros, l'article 83 du RGPD précisant bien que « le montant le plus élevé [est] retenu ». Ce nouveau montant des sanctions potentielles a stimulé l'expansion considérable d'un marché de conseils en conformité RGPD, représentant l'équivalent de 9 milliards de dollars à l'échelle mondiale selon un article de *Forbes* (Smith, 2018).

Un autre changement touchant aux autorités de protection des données a été la réforme du G29. Celui-ci garde une composition identique mais devient une institution à part entière : le Comité européen de protection des données (CEPD) (art. 68 du RGPD). Chaque autorité nationale composant le CEPD est désormais compétente en priorité pour les affaires touchant les entreprises ayant leur « établissement principal »[65] dans son territoire de compétence : c'est le mécanisme de l'autorité cheffe-de-file, défini à l'article 56 du RGPD. Enfin, des mécanismes de coopération et d'assistance mutuelle entre autorités sont mis en place (arts. 60 à 62 du RGPD), ainsi qu'un mécanisme dit de « cohérence » qui permet au CEPD d'adopter des décisions contraignantes en cas de désaccord entre ses membres, notamment sur un projet de décision d'une autorité de contrôle (art. 65 du RGPD).

Ainsi, l'objectif du RGPD est de renforcer l'harmonisation non seulement des règles de protection des données en Europe, mais aussi de leurs modalités d'application par les autorités nationales, et de permettre à une entreprise disposant de filiales dans plusieurs pays européens d'avoir un point de contact unique en matière de protection des données : l'autorité de contrôle du lieu de son établissement principal.

Le RGPD modifie aussi le champ d'application territorial du droit de l'Union en matière de protection des données à caractère personnel. En dehors de l'UE et de l'EEE, le RGPD s'applique « au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :

63 Voir l'article 7 de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

64 Voir l'article 79 paragraphe 5 de la proposition initiale de RGPD de la Commission (COM (2012) 011)

65 Selon l'art. 4 du RGPD il s'agit du « lieu de [l']administration centrale » du responsable du traitement ou du sous-traitant.

« a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou

b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union » (art. 3 du RGPD)

En pratique, que ce soit des autorités nationales comme la CNIL en France[66] ou le *Garante Privacy* en Italie[67], la directive 95/46/CE s'appliquait dans biens des cas à des entreprises n'ayant pas leur siège social en Europe. Le RGPD simplifie toutefois les critères permettant de faire entrer des responsables du traitement étrangers dans le champ d'application territorial du droit de l'UE en matière de protection des données à caractère personnel.

Outre l'harmonisation, la réévaluation du montant de sanctions administratives, et la modification des critères de détermination du champ d'application territorial, la principale nouveauté est la suppression des formalités de notification préalable des traitements à l'autorité de contrôle prévue à l'article 18 de la directive de 1995. Ce système est remplacé par un ensemble de règles qui visent, en s'inspirant de la notion de « *compliance* », à faire en sorte que les responsables du traitement prennent en charge eux-mêmes la document de leurs processus de mise en conformité permanente aux principes et règles édictés par le RGPD :

> « Toute la nouveauté du RGPD réside dans l'affirmation des outils mis à disposition des différents acteurs pour parvenir à l'application efficace et quotidienne des principes inhérents à la protection de la donnée. C'est dans ce cadre-là que la logique adoptée substitue à l'applicabilité, la mise en conformité. Cette nouvelle logique porte un nom : la compliance. » (Favro, 2017, p. 22)

Ce terme de « *compliance* », que nous avons souvent entendu lors de déplacements sur le terrain et de conversations informelles avec ses acteurs, n'est pas simple à définir, et, s'il y est parfois fait référence en français par le syntagme « conformité », il ne serait en réalité pas réellement traduisible (Favro, 2017 ; Frison-Roche, 2016). La compréhension de ce qu'il signifie est pourtant essentielle pour bien saisir l'esprit de la réforme proposée en 2012 par la Commission et qui a donné naissance au RGPD.

Comme le rappelle Marie-Anne Frison-Laroche, « la compliance peut renvoyer au fait de se comporter bien, de prendre spontanément en considération l'intérêt d'autrui » (Frison-Roche, 2016, p. 1871). Mais, « consultant d'autres sources, l'on trouve l'affirmation tout autre que la compliance renvoie à l'engagement pris par l'opérateur de respecter l'ensemble des

66 Voir par exemple la délibération 2013-420 du 3 janvier 2014 de la CNIL prononçant une sanction pécuniaire à l'encontre de Google Inc., une société californienne, sur le fondement de la loi informatique et libertés du 6 janvier 1978 et du règlement 95/46/CE.

67 Voir par exemple l'Ordinanza di ingiunzione nei confronti di Google Inc. du 18 décembre 2013 sanctionnant l'entreprise californienne Google Inc. à hauteur d'un million d'euros pour des manquements à la directive 95/46/CE et à la loi italienne l'ayant transposée, survenus dans le cadre du service Google Street View.

réglementations. » (Frison-Roche, 2016, p. 1872). Pour Karine Favro, qui tente une définition de ce mot :

> « Rattachée au respect des principes juridiques qui irriguent un secteur, la *compliance* suppose l'exercice d'un contrôle sur la mise en œuvre de ces principes par les acteurs concernés. […] Ces principes ont vocation à gérer des situations globales et internationales mais les acteurs sont acculés à les respecter et, pour ce faire, à entreprendre une veille juridique qui occupe une personne quasiment à temps plein. Cependant, ces objectifs sont légitimes et ont pour principal effet de contenir la confiance des acteurs sur un marché donné et de protéger des libertés que les États peinent à garantir. » (Favro, 2017, p. 23)

La « *compliance* » désigne donc la mise en place d'un processus de gouvernance internalisée – et non plus confiée à une autorité administrative publique – au sein d'une entreprise qui lui permet d'entamer et de documenter une démarche de mise en conformité avec des règles et des principes juridiques auxquels les infractions font l'objet de sanctions. Tant Karine Favro que Marie-Anne Frison-Laroche indiquent que ces principes et règles visent à atteindre des objectifs qu'elles qualifient de « monumentaux » par leur ampleur et leur complexité. Cela est vrai dans le domaine de la protection des données avec l'adoption du RGPD, comme par exemple dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme :

> « En droit du commerce international, bancaire et financier, la compliance [...] est l'expression de la volonté des pouvoirs publics d'imposer des règles dont ils n'ont pas la force d'assurer l'effectivité : des législateurs ou des régulateurs publics adoptent des normes que l'on pourrait dire « monumentales » tant leur but est immense, par exemple, la fin de la corruption, ou la fin de tout commerce avec un pays qu'ils estiment indigne (embargo) ou la fin du terroriste [sic]. Ce sont des maux globaux. Ils vont internationaliser la mise en œuvre de ces normes publiques monumentales dans les structures qui sont de droit et de fait mondiales, informées et puissantes : les entreprises multinationales qui pratiquent les opérations financières internationales. » (Frison-Roche, 2016, p. 1872)

Concrètement, la démarche de « *compliance* », qui, dans le droit *de la* protection des données, remplace la logique précédente des notifications préalables et des demandes d'autorisation se traduit par l'imposition de plusieurs contraintes nouvelles aux responsables du traitement. Le traitement des notifications reçues et des demandes d'autorisation demandait des moyens humains importants aux autorités de contrôle. Dans certains cas, comme dans le cas de l'ancienne *Datenschutzkomision* (DSK) autrichienne[68], qui disposait de moyens humains très

68 Une réforme adoptée par le législateur autrichien pour faire cesser le manquement constaté par la CJUE à l'indépendance de la DSK a été l'occasion d'un changement de nom. L'autorité de contrôle autrichienne s'appelle désormais la *Datenschutzbehörde*.
Voir : CJUE 16 octobre 2012, « Commission contre République d'Autriche », aff. C-614/10, et : Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2013).

limités, le volume d'activité représenté par les démarches de notification et de demandes d'autorisation était tel qu'elles ne disposaient plus des ressources suffisantes pour mener un contrôle *a posteriori* de la conformité au droit *de la* protection des données[69].

La fin des notifications préalables, présentée par la Commission européenne comme la fin d'« obligations administratives inutiles » (Commission européenne, 2012d) et donc comme un gain de temps et d'argent pour les entreprises, a donc surtout été un allègement administratif considérable pour les autorités de contrôle. En échange, les entreprises doivent[70] tenir un registre[71] de leurs « activités de traitement[72] » de données à caractère personnel. L'article 30 du RGPD précise même les informations qui doivent impérativement être portées à ce registre.

Les entreprises doivent aussi intégrer la problématique de la *compliance* au RGPD dans la conception même des logiciels qui collectent et traitent des données à caractère personnel (Favro, 2017). Ces logiciels doivent aussi être paramétrés pour protéger par défaut la vie privée et les données personnelles de leurs utilisateurs. Ces deux obligations sont généralement désignées en anglais par les formules de « *Privacy by Design* » et de « *Privacy by Default* » et sont inscrites à l'article 25 du RGPD. Elles ont pour objectif de faire en sorte que les logiciels soient techniquement conçus pour être conformes aux principes de la protection des données (Cavoukian, 2013).

Le RGPD prévoit également la possibilité pour des organismes d'obtenir des labels et des certifications leur permettant de démontrer leur « *compliance* » (art. 42 du RGPD), soutenant ainsi le développement d'un marché de la certification de la protection des données (Levallois-Barth, 2018).

Par ailleurs, la fonction de délégué à la protection des données est désormais réglementée directement au niveau du droit de l'Union[73] alors que la directive de 1995 ne prévoyait que la faculté des États membres d'adopter des dispositions à cet égard[74]. Ces cadres sont désignés dans leur organisation pour être en charge du contrôle interne de la conformité de leur entreprise au

69 Entretien réalisé avec le vice-président de la DSK à Vienne le 22 avril 2013, dans le cadre d'une recherche précédente (Rossi, 2013).

70 Il existe seulement une exception pour les entreprises ou organisations de moins de 250 salariés « sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 » (art. 30 du RGPD).

71 À titre d'exemple, l'Université de St-Étienne a mis en ligne publiquement son registre des traitements, qui peut être consulté à l'adresse suivante : https://retil.univ-st-etienne.fr/index.php?page=registre_public (page consultée le 20 décembre 2019).

72 Savoir ce que correspond une unité d'activité de traitements, et donc une entrée dans le registre des traitements, a été l'objet et est toujours l'objet de discussions régulières sur le réseau social « Agora » de l'Association française des correspondants aux données personnelles, auquel j'ai pu accéder en tant que membre. L'un des fils de discussion dédiés à cette question, et ouvert le 11 décembre 2018, porte par exemple le titre « Faut-il que j'inscrive au registre autant de traitement [sic] que de licéité, ou un traitement par processus couvrant plusieurs licéités ? » (ce fil de discussion peut être consulté par les membres de l'AFCDP à l'adresse : https://agora-afcdp.jamespot.pro/article/18962 – page consultée le 20 décembre 2019)

73 Articles 37 à 39 du RGPD

74 L'article 18 paragraphe 2 permettait aux États membres d'alléger certaines obligations de notification en échange de la désignation par le responsable du traitement d'un « détaché à la protection des données à caractère personnel » dont les missions étaient décrites en une phrase.

droit *de la* protection des données[75]. Alors qu'il existait une forte diversité dans les modalités d'encadrement de cette profession d'un État membre à l'autre (Rossi, 2015b), le RGPD impose désormais partout dans l'EEE à certains organismes, comme les autorités publiques et les organismes sont les « activités de base […] exigent un suivi régulier et systématique à grande échelle des personnes concernées » ou « consistent en un traitement à grande échelle de catégories particulières de données » sensibles (art. 37 du RGPD). Ses missions, définies à l'article 39 du RGPD, en font le principal responsable de la « *compliance* » de son organisme.

Le RGPD impose aussi des obligations à respecter dans les relations entre le responsable d'un traitement de données personnelles et ses sous-traitants, qui doivent, entre autres, signer un accord dont le contenu est détaillé à son article 28 paragraphe 3. Cela vise à faire en sorte que la chaîne de traitement soit maîtrisée dans son ensemble, et ainsi à réduire les risques du recours à la sous-traitance (Favro, 2017, p. 25).

La question du « risque » et de « l'approche fondée sur le risque » (« *risk-based approach* ») a été l'un des principaux points d'affrontement entre les coalitions de cause ayant cherché à influencer la rédaction du RGPD[76].

Pour Karine Favro (2017, p. 24), la notion de « *compliance* » est très liée à la question du risque. L'article du RGPD qui illustre le mieux la convergence entre « *compliance* » et « approche fondée sur le risque » est l'article 35, sur les « analyses d'impact relatives à la protection des données ». La notion de risque n'était pas absente de la directive de 1995[77] (Gellert, 2016), mais le RGPD lui accorde une importance nettement accrue, ce qui s'est traduit en pratique notamment par l'introduction de cet article 35 sur les analyses d'impact (Böröcz, 2016, p. 470).

Ces dernières doivent être déclenchées lorsqu'« un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques » (art. 35 du RGPD). L'organisme qui le réalise doit alors trouver des solutions pour réduire le niveau de risque observé. L'article 36 précise que l'organisme qui réalise cette étude doit consulter l'autorité de contrôle compétente sur son territoire si elle « indique que le traitement présenterait un **risque élevé**[78] si le responsable du traitement ne prenait pas de mesures pour atténuer le risque » (art. 36 du RGPD).

La comparaison entre la place du « risque » dans la directive de 1995 et dans le RGPD est utile pour comprendre la portée de ce qui est désigné, au sujet du RGPD, par le terme de « *compliance* ». Le considérant 54 de la directive 95/46/CE faisait en effet reposer le calcul du

75 Voir à leur sujet le livre de Kenneth Bamberger et Deirdre Mulligan : *Privacy on the Ground* (Bamberger et Mulligan, 2015)
76 Cf. section 4.3.5.
77 Voir notamment les considérants 27, 46, 53, 54.
78 Mise en forme ajoutée par l'auteur.

risque sur les épaules de l'autorité de contrôle. Les responsables du traitement avaient l'obligation de lui notifier leurs intentions de collecter et utiliser des données personnelles avant le début des opérations de traitement. Dans certains cas, dont les caractéristiques permettaient de soupçonner qu'ils représentent un risque élevé pour les personnes concernées, les responsables du traitement devaient même demander une autorisation à l'autorité de contrôle. Ces cas étaient définis par les droits nationaux des États membres[79]. Or, désormais, avec le RGPD, c'est aux organismes concernés de déterminer eux-mêmes si l'un de leurs projets de traitements de données à caractère personnel présente un « risque élevé » ou non, et ils peuvent être sanctionnés en cas d'erreur.

À des obligations formulées de façon générale en matière de sécurité et de confidentialité des données, présentes tant dans la directive de 1995[80] que dans le RGPD[81], ce dernier ajoute une procédure nouvelle : l'obligation de notification des « violations de données à caractère personnel[82] », c'est-à-dire d'incidents de sécurité ayant compromis la confidentialité des données, et ayant par exemple abouti à leur publication ou à des accès de personnes non-autorisées. L'article 33 impose une notification à l'autorité de contrôle dans les 72 heures (sauf exceptions) et l'article 34 impose de prévenir les personnes sur lesquelles portent les données dont la sécurité a été compromise si l'incident est « susceptible d'engendrer un risque élevé pour [s]es droits et libertés » (art. 34 du RGPD). Notons que nous retrouvons de nouveau cette notion de « risque » qui, s'il dépasse un certain seuil, doit entraîner une action de la part du responsable du traitement, qui doit évaluer lui-même voire deviner le seuil à partir duquel il peut être sanctionné en cas d'inaction. L'article 34 du RGPD peut donc lui aussi être interprété sous cet angle de la « *compliance* ».

En ce qui concerne les droits que des « personnes concernées », c'est-à-dire les personnes sur lesquelles portent les données (et non leurs propriétaires), peuvent exercer, le RGPD reprend pour l'essentiel ceux qui étaient présents dans les Lignes directrices de l'OCDE, dans la Convention 108, et dans la directive de 1995 : droit d'accès, droit de rectification et dans certains cas, droit d'opposition. En plus, le RGPD consacre un droit qui n'était pas clairement formulé dans la directive de 1995 mais qui découlait logiquement d'une lecture attentive de son contenu : le droit à l'effacement, aussi connu sous le terme de « droit à l'oubli », qui permet à une personne de demander l'effacement de données qui la concernent lorsque celles-ci ne sont plus pertinentes pour l'usage initialement légitime pour lequel elles étaient conservées[83]. Enfin, le RGPD complète le droit d'accès par un nouveau « droit à la portabilité[84] » qui permet à une personne de

79 Voir l'article 20 de la directive 95/46/CE.
80 Voir l'article 17 de la directive 95/46/CE.
81 Voir l'article 32 du RGPD.
82 Cette notion est définie à l'article 4 paragraphe 12 du RGPD comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».
83 Voir l'article 17 du RGPD, et la décision CJUE 13 mai 2014 « Google Espagne contre AEPD », aff. C-131/12.
84 Voir l'article 20 du RGPD.

demander une copie sous un format numérique standard des données à caractère personnel qui la concernent et qui sont traitées par l'organisme auquel elle s'adresse.

Enfin, un dernier changement parmi la myriade d'autres détails que nous n'avons pas le temps d'évoquer ici, mérite d'être mentionnée, car il peut transformer le champ de l'action publique en matière de protection des données à caractère personnel : il s'agit de l'article 80 du RGPD, à lire en conjonction avec l'article 82 (Castex et al., 2018 ; Isidro, 2017 ; Walree, 2017).

L'article 80 du RGPD permet à un « un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et est actif dans le domaine de la protection des droits et libertés des personnes concernées » (art. 80 du RGPD) d'être mandaté par des personnes concernées pour introduire une réclamation en leur nom collectif auprès d'une autorité de protection des données ou d'un tribunal et, lorsque le droit national le permet, puisse demander réparation du préjudice subi en raison d'une infraction au RGPD sur le fondement de l'article 82 du RGPD. La mise en œuvre de cette disposition peut buter contre des obstacles procéduraux nationaux (Castex et al., 2018) mais, depuis l'entrée en vigueur du RGPD, plusieurs associations ont introduit des plaintes collectives auprès d'autorités de contrôle ou de tribunaux, et certaines demandent la réparation du préjudice moral subi en raison de la violation du droit *à la* vie privée et *à la* protection des données personnelles par les entreprises attaquées[85]. Au jour de l'écriture de ce chapitre, il est impossible de préjuger du montant des réparations qui pourront ainsi être versées aux personnes concernées, et au coût que cela pourra engendrer pour les responsables du traitement en infraction, mais ce dispositif juridique complète l'aspect coercitif du droit de l'Union *de la* protection des données qui, avant le RGPD, reposait sur de très rares actions au pénal, des actions en civil périlleuses et coûteuse à l'échelle de l'individu, et le contrôle administratif des autorités de contrôle. Les articles 80 et 82 du RGPD permettent donc de venir en renfort de l'action de ces autorités en matière de contrôle et de sanction. C'est d'ailleurs ainsi que cela est décrit par les acteurs concernées. Le 15 mai 2018, Wojciech Wiewiórowski, Contrôleur européen adjoint de la protection des données, avait ainsi publié un billet de blog sur le site officiel de l'EDPS pour affirmer que « les organisations de la société civile sont les alliées naturelles des autorités de protection des données[86] ». Ce billet faisait suite à une réunion publique sur ce le thème de la coopération entre ONG et autorités de contrôle, qui avait eu lieu en janvier à Bruxelles lors de la conférence *Privacy Camp 2018* à laquelle il avait participé aux

85 À titre d'exemple, nous pouvons citer la plainte de l'association français La Quadrature du Net (LQDN), qui a abouti à la délibération de la CNIL n° SAN – 2019 – 001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société Google Inc.
Si la Quadrature du Net n'a, pour des raisons de philosophie politique, pas souhaité demandé la réparation du préjudice auprès d'un tribunal, d'autres associations en Europe ont choisi de déposer un recours collectif et de demander des réparations au civil. C'est le cas de l'association de défense des consommateurs Test Achat en Belgique, qui a introduit une action en justice auprès du Tribunal de commerce de Bruxelles pou réclamer 200 € par utilisateur ayant mandaté l'association pour défendre leurs intérêts en leur nom collectif (voir le communiqué de presse de Test Achat du 28 octobre 2018, disponible à l'adresse web https://www.test-achats.be/action/espace-presse/communiques-de-presse/2018/facebook-29102018 , consultée le 15 avril 2019).

86 Traduit de l'anglais : « Civil society organisations as natural allies of the data protection authorities » (Wiewiórowski, 2018).

côtés de personnes comme Katarzyna Szymielewicz de la Fondation Panoptykon, Joe McNamee d'EDRi, ou encore Fanny Hidvégi de l'association AccessNow[87]. Ces dernières étaient des membres actifs de la coalition des défenseurs de la vie privée[88].

En conclusion, le RGPD ne touche donc ni aux principes ni aux définitions qui remontent pour l'essentiel aux Lignes directrices de l'OCDE de 1980, à la Convention 108 du Conseil de l'Europe et qui avaient été repris dans la directive 95/46/CE. Il apporte des changements sur le plan des procédures de mise en œuvre, en consacrant une démarche de « *compliance* ». Surtout, il augmente considérablement le montant des sanctions administratives qui peuvent être imposées aux organismes qui enfreignent ces principes.

L'importance de ces changements, mais aussi le fait que certains acteurs espéraient profiter de la fenêtre d'opportunité ouverte par le processus d'adoption du RGPD pour réussir à remettre en cause certains principes, définitions et obligations contenues dans la directive de 1995, expliquent l'engagement d'un grand nombre d'acteurs dans les débats ayant accompagné le processus d'adoption du RGPD. 3999 amendements à la proposition de la Commission ont été déposés au Parlement européen entre janvier 2012 et l'adoption du rapport de la commission LIBE en octobre 2013 selon la Commission européenne (Commission européenne, 2013), dont au moins 2617 rien qu'auprès de la commission LIBE[89]. Parltrack[90] recense lui jusqu'à 5316 amendements liés au dossier 2012-011-COD[91]. Ce chiffre est à comparer au nombre moyen d'amendements déposés par procédure législative sur la période 2009-2014, qui est de 47 amendements en moyenne par projet (Dehousse, Novak et Bendjaballah, 2017, p. 59).

Maintenant que nous avons examiné le contenu du texte final du RGPD, les nouveautés qu'il apporte mais aussi l'importante continuité avec la directive qu'il abroge, nous allons pouvoir nous intéresser à la structure du sous-système de politique publique de protection des données à caractère personnel de l'Union européenne, puis à la controverse qui, dans les arènes de ce sous-système de politique publique, en a entouré l'adoption. Nous nous intéresserons en particulier aux discours des acteurs, aux conceptions de la « vie privée » qu'ils ont mobilisé, et à leurs stratégies argumentatives pour tenter d'influencer la rédaction de ce texte normatif.

87 La réunion a été filmée et mise en ligne sur Youtube à l'adresse : https://www.youtube.com/watch?v=RYYqziLGBG4 (page consultée le 15 avril 2019).

88 Cf. section 4.2.

89 Voir le document PE 506.169v02-00 du Parlement européen du 6 mars 2013.

90 Parltrack est un site web qui récupère, trie et présente des données du site du Parlement européen sur les procédures législatives de l'UE : https://parltrack.org/ .

91 Selon les chiffres du projet Parltrack. Voir : http://parltrack.euwiki.org/dossier/2012/0011%28COD%29 (page consultée le 15 avril 2019).

4.1.4. Le rôle structurant du réseau transgouvernemental des autorités de protection des données dans le sous-système de politique publique de protection des données de l'Union européenne

Comme annoncé en introduction, notre souci a été d'identifier les arènes *efficaces*, au sens de Nancy Fraser (2007), où se sont déroulées les discussions qui ont influencé le texte final du RGPD, dont nous venons de résumer le contenu. Formellement, le RGPD est un texte qui a été rédigé par des personnes membres de trois institutions : la Commission européenne, le Conseil de l'UE, et le Parlement européen. D'autres institutions, comme l'EDPS, ou le Comité des régions, ont été sollicitées pour avis. Enfin, une myriade d'autres acteurs, regroupés en coalitions rivales, ont tenté, parfois avec succès, d'influencer le contenu de ce texte. Toutes ces personnes appartiennent à un même sous-système de politique publique à l'échelle de l'Union européenne.

Henri Bergeron, Yves Surel et Jérôme Valluy (Bergeron, Surel et Valluy, 1998, p. 206), en partant du cadre théorique de l'ACF, identifient quatre critères permettant d'identifier un sous-système de politique publique :

1. Les participants eux-mêmes se perçoivent comme faisant partie d'une communauté, fondée sur le partage d'une expertise, et relativement autonome ;
2. Les acteurs qui sont identifiés cherchent de façon durable à influencer la politique publique en question ;
3. Il existe des administrations compétentes sur le domaine étudié de politique publique à tous les niveaux ;
4. Il est possible d'identifier des groupes d'intérêt qui considèrent ce domaine de politique publique comme étant prioritaire.

L'étude de la généalogie de la notion (et de la formule) de « protection des données »[92], ainsi que de l'origine tant du droit *à la* que du droit *de la* protection des données à caractère personnel nous permet déjà, à ce stade, de supposer que la bonne échelle pour étudier les politiques publiques de protection des données à caractère personnel en Europe ne se situe pas à l'échelon national, encore moins infra-national, mais à une échelle supranationale européenne. Nous avons également vu que l'adoption de la directive 95/46/CE sur la protection des données à caractère personnel et leur libre-circulation[93] a fait du droit *de la* protection des données à caractère personnel une matière législative communautaire (voir : Karaboga, 2018). Pouvons-nous, pour autant, parler de politique publique à l'échelle de l'UE ?

92 Cf. chapitre 3.

93 Comme le rappelle Béatrice Dumont, il ne faut pas négliger cet autre objectif de la directive de 1995, qui était de garantir la libre-circulation des données à caractère personnel sur le marché commun (Dumont, 2011).

Avant de répondre à cette question qui porte spécifiquement sur l'existence de politiques publiques de protection des données au niveau de l'UE, il est utile de rappeler que l'existence de politiques publiques au niveau de l'Union européenne est attestée dans de multiples domaines. Cela est bien sûr le cas pour les compétences exclusives de l'UE, comme la politique de la concurrence (Woll, 2009), la politique monétaire (Fontan, 2013). La politique commerciale (Messerlin, 2009) est tellement intégrée à l'échelle de l'UE que c'est cette dernière qui représente ses États-membres à l'Organisation mondiale du commerce. Mais des politiques publiques existent aussi dans le cas de certains domaines de compétence partagée. Les politiques migratoires, par exemple, sont un domaine partagé entre les États-membres et l'Union. L'obligation de coopération entre autorités en charge de la mise en œuvre des accords de Schengen ou encore les règlements de Dublin successifs[94], entraînent la constitution de réseaux de politiques publiques qui ont un effet non négligeable sur la socialisation des acteurs y compris au niveau national, harmonisant les pratiques d'accueil des étrangers (Skowronska, 2014). Un nouvel « espace politique » émergerait de ces interactions au sein de réseaux administratifs transnationaux (Thurner et Binder, 2009). Dans le domaine de la recherche scientifique, nous voyons comment la recherche de financements nous amène à adapter nos projets au langage et aux objectifs des projets européens qui, dans le cadre financier pluriannuel actuel, portent le nom de projets « H2020 ». En France, l'Agence nationale pour la recherche a ainsi adapté la structure de ses appels à projet pour refléter celle des projets H2020 (voir : ANR, 2013, p. 3). Comme l'écrivait Pierre Müller dès 1997, « faire référence » aux politiques européennes est devenu un « passage obligé pour les acteurs nationaux des politiques publiques » (Müller, 1997, p. 6). Quant à la présidence tournante du Conseil de l'UE, où un gouvernement d'un État membre prend à tour de rôle et pendant six mois la présidence des travaux de cette institution, elle est un élément important de socialisation des élites politiques et administratives à l'échelon européen, tant et si bien que selon certains, le Conseil de l'UE perdrait progressivement ses caractéristiques intergouvernementales pour s'assimiler de plus en plus à une institution communautaire supranationale, comme le Parlement et la Commission européens (Mangenot, 2011). Cet ensemble de phénomènes désignés sous ce terme d'européanisation des politiques publiques s'expliquerait empiriquement par des stratégies d'adaptation d'administrations locales à la transformation du contexte de transformations institutionnelles induit par le transfert de compétences à l'échelle supranationale (Olsen, 2002).

Bien qu'il soit contesté sur le plan conceptuel (Olsen, 2002), un concept est utilisé pour désigner le phénomène que nous venons d'évoquer : il s'agit de l'« européanisation[95] », que nous

94 Règlement 343/2003/CE du Conseil du 18 février 2003 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée dans l'un des États membres par un ressortissant d'un pays tiers, puis Règlement 604/2013/UE du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride.

95 Il est parfois question dans le vocabulaire de certains acteurs de « passage à l'Europe », selon l'expression de Luuk van Middelaar, conseiller de Herman van Rompuy à l'époque où celui-ci occupait le poste de président du Conseil européen, et dont l'ouvrage avait eu un succès certain dans le milieu des institutions européennes (Middelaar, 2009). Cette expression, qui n'est pas vraiment conceptualisée d'une façon exploitable en recherche,

pouvons définir, à l'instar de Sabine Saurugger et Yves Surel, comme un « processus de transfert de politique publique » (Saurugger et Surel, 2006) vers l'UE.

Bien que, comme nous l'avions déjà vu dans le premier chapitre[96], il n'apparaisse pas possible de parler avec rigueur d'un *espace public* européen, Pierre Müller identifie ce qu'il appelle un « espace européen d'action publique » (Müller, 1997, p. 3).

Cet espace n'est pas étatique. Cela se traduit par le principe d'autonomie institutionnelle des États membres, qui fait que les institutions communautaires sont rarement dotées des pouvoirs d'exécution des actes législatifs européens, et qui laisse aux États membres le soin de décider de façon autonome de la façon dont ses propres institutions mettent en œuvre sur le terrain les politiques publiques décidées à l'échelon communautaire. Par exemple, bien que la politique commerciale soit une compétence exclusive de l'Union, ce sont des douaniers nationaux qui sont chargés d'effectuer les contrôles douaniers aux frontières extérieures communes et de collecter le tarif extérieur commun. En matière de protection des données, bien que le RGPD soit un règlement de l'Union, seuls les agents publics des autorités nationales de protection des données peuvent procéder à des contrôles administratifs du respect de ce règlement.

Le fait que des agents publics nationaux, de différents pays, soient amenés à s'assurer d'un même texte supranational, entraîne ce que Pierre Müller appelle une « innovation conceptuelle et institutionnelle » se traduisant par « la diffusion permanente, au sein des systèmes nationaux, de procédures et de modes opératoires en décalage par rapport aux traditions nationales » (Müller, 1997, p. 4 ; Smith, 1996). En matière de protection des données, cela s'est traduit par l'imposition par l'article 28 de la directive de 1995 du principe d'indépendance des autorités de contrôle à l'égard de l'exécutif, qui était contraire en Allemagne et en Autriche au principe de constitutionnalité qui devait garantir un lien permanent de toutes les autorités administratives au Parlement élu au suffrage universel à travers le gouvernement, à l'exception de la banque centrale et des organes de contrôle financiers de l'État (Rossi, 2013). Dans le RGPD, ce principe d'innovation conceptuelle et institutionnelle des politiques publiques supranationales de l'UE se traduit aussi par l'invention des mécanismes de cohérence (art. 63 à 67 du RGPD) et de coopération (art. 60 à 62 du RGPD) qui, d'une certaine façon, peuvent être compris comme des façons de contourner le principe d'autonomie institutionnelle des États membres voire de le restreindre[97].

Une autre caractéristique des politiques publiques au niveau de l'UE est le découplage entre la fragmentation des espaces publics médiatiques et la constitution de groupes d'intérêt européens focalisés sur un objectif d'influence des institutions de l'UE (Badouard, 2012 ; Müller, 1997, p. 4). Ces groupes d'intérêt contribuent au travaux de réflexion à travers des consultations et des groupes dits d'experts, en échange de fenêtres d'opportunité pour influencer la production

permet toutefois d'illustrer cette idée de mouvement de déplacement qui sous-tend cette idée d'européanisation, et de montrer la façon dont elle est perçue par des acteurs situés socialement en haut de la hiérarchie politique des institutions européennes.

96 Cf. section 1.1.

97 Voir l'article d'Alin Orgoan au sujet des limites jurisprudentielles du principe d'autonomie institutionnelle (Orgoan, 2016).

des politiques publiques de l'Union, notamment au niveau de la Commission européenne (Bouwen, 2002, 2009 ; Douillet et Maillard, 2010). Ce recours à l'expertise est une des sources de légitimation de l'action politique de la Commission européenne, détentrice dans les matières soumises à la procédure législative ordinaire du monopole de l'initiale législative. Cette expertise est présentée et perçue comme garante de la qualité de la production (« *output* ») de politiques publiques, pouvant compenser un déficit de légitimité démocratique, ou de légitimité par les « *input* » (Scharpf, 2000).

L'UE se caractérise également par un niveau relativement faible de conflictualité et par la culture du consensus qui règne au sein de ses institutions. Selon Pierre Müller, « à côté du registre de la production d'expertise, l'Union européenne fonctionne sur le registre de la *négociation* » (Müller, 1997, p. 5). Une étude quantitative récente menée dans le cadre du projet de recherche *Observatory of European Institutions* (Dehousse et al., 2017) a montré que cette culture du consensus continuait à s'observer au moins jusqu'en 2014 (Dehousse, Novak et Bendjaballah, 2017). Elle permet d'expliquer pourquoi, en dépit du nombre statistiquement extraordinaire d'amendements déposés au cours de la procédure d'adoption du RGPD, le vote du rapport de la commission LIBE ait été quasi-unanime avec une voix contre, trois abstentions et quarante-huit voix pour et avec 95 % des voix en première lecture en plénière (Parlement européen, 2013b).

Une caractéristique des politiques publiques de l'UE importante dans le cadrage du terrain sur le RGPD sur lequel porte le présent chapitre, et qui explique la forte implication d'acteurs de pays tiers, comme des entreprises états-uniennes ou l'*American Chamber of Commerce to the European Union* (AmCham EU), est que l'UE, si elle n'est pas une puissance de *hard power* selon la caractérisation de Joseph Nye (Nye, 2004), est souvent perçue comme une puissance normative, c'est-à-dire capable d'influencer les normes juridiques de pays tiers (Tulmets, 2014). Or, si cette capacité de l'UE à façonner son environnement juridique international en fonction de ses propres préférences est sujette à controverse dans le champ des relations internationales (Zielonka, 2008), en matière d'extension de droit *de la* protection des données à caractère personnel, l'UE est parvenue à imposer à des pays tiers son régime juridique en en faisant le prix de l'accès à son marché unique, qui a longtemps été le plus gros marché intégré en termes de produit intérieur brut[98] (Newman, 2008).

Bien qu'elles revêtent des caractéristiques particulières qui les distinguent de leurs équivalents nationaux, il est donc bel et bien possible de parler de politiques publiques dans le cadre de l'UE. Nous pouvons donc reprendre les critères énumérés en début de section pour

98 Selon la Banque mondiale, le PIB des États-Unis d'Amérique était de plus 19 billions de dollars U.S. en 2017, contre un peu plus de 17 billions de dollars U.S. pour l'UE. En 2014, le PIB de l'UE était encore de près de 18,7 billions de dollars U.S., contre 17,5 pour les États-Unis d'Amérique (source : Banque mondiale, 2019 : https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-US-CN, page consultée le 1er juin 2019).

vérifier s'il existe bel et bien un sous-système de politiques publiques dédié la protection des données à caractère personnel au niveau de l'UE nous permettant d'y appliquer notre modèle théorique fondé sur l'ACF.

Le premier critère était que les participants se perçoivent eux-même comme faisant partie d'une communauté, relativement autonome, et fondée sur le partage d'une expertise. Or, plusieurs travaux ont montré l'existence d'une « *privacy community* » (Bennett, 1992, 2008 ; Bennett et Raab, 2003) qui bien qu'elle ne soit pas limitée à l'Europe, s'est structurée à une échelle européenne, comme nous l'avons vu dans le chapitre précédent, dès les années 1970, avant même que le centre de gravité institutionnelle de la production de normes juridiques européennes en la matière ne se déplace du Conseil de l'Europe à la CEE (devenue entre temps l'UE). Ces acteurs évoluent à un niveau national, mais sont amenés à travailler régulièrement à un niveau transnational voire supranational. Ce fut le cas de Marie Georges qui, travaillant au service des relations internationales de la CNIL en France, partit travailler à Bruxelles en tant qu'experte nationale détachée pendant la période de négociation de la directive de 1995[99]. Pieter Jan Hustinx, connu sous le nom de Peter Hustinx, après une carrière nationale, fut le premier président du G29 en 1996, alors qu'il était président de l'autorité néerlandaise de protection des données, avant de devenir Contrôleur européen à la protection des données en 2004. Il participa même au processus d'adoption du RGPD, puisqu'il occupa ce poste jusqu'en 2014. Stefano Rodotà, que nous avons déjà rencontré dans la période étudiée au chapitre précédent, a été président du *Garante Privacy* en Italie, et fut élu président du G29 en 2000 (G29, 2002). D'autres acteurs peuvent être identifiés comme ayant dans ce sous-système une action uniquement à l'échelle de l'Union européenne. C'est le cas d'eurodéputés comme Jan Philipp Albrecht ou Axel Voss, qui ont été rapporteur et rapporteur fictif du RGPD. C'est le cas des commissaires Viviane Reding et Věra Jourová, qui ont été les commissaires européennes en charge du dossier. C'est également le cas de fonctionnaires de la Commission comme Bruno Gencarelli, fonctionnaire de la Commission à la DG Justice qui fut en charge du dossier du RGPD.

Des trajectoires similaires s'observent chez des acteurs du monde associatif et des représentants d'intérêts industriels. Fanny Hidvégi, après avoir travaillé pour une association hongroise de défense des libertés publiques, est partie travailler pour l'association AccessNow dans ses bureaux bruxellois, partagés au moment de notre terrain avec ceux d'EDRi, une fédération d'associations nationales militant dans leurs pays pour les droits fondamentaux en milieu numérique. Dans cette fédération, certaines personnes sont actives à la fois au niveau national et au niveau européen. Katarzyna Szymielewicz, présidente de l'ONG polonaise Panoptykon, membre d'EDRi, a été très souvent présente dans des réunions à Bruxelles ou à des conférences comme la CPDP. D'autres acteurs, comme Joe McNamee, directeur exécutif d'EDRi de 2009 à 2018, ont joué un rôle plus spécifiquement européen. Du côté des groupes d'intérêt industriels, des associations comme Emota ou DIGITALEUROPE regroupent des entreprises qui sont aussi membres d'associations nationales, mais disposent des salariés qui sont spécifiquement

99 Source : entretien avec l'intéressée.

de développer une veille et une stratégie d'influence au niveau des institutions de l'Union. Une partie de ces associations se sont regroupées pour former un groupe informel, l'*Industry Coalition for Data Protection*, destiné à influencer le processus d'adoption du RGPD.

Le premier critère d'identification d'une politique publique de protection des données à caractère personnel au niveau de l'UE est donc bel et bien rempli.

Le deuxième critère est que les acteurs identifiés cherchent de façon *durable* à influencer la politique publique dont nous cherchons à vérifier l'existence. Paul Sabatier (1998) fixe la durée de ce temps long à dix ans. Or, nous avons déjà montré que certains acteurs impliqués dans la négociation du RGPD étaient déjà impliqués dans les discussions préalables à l'adoption de la Convention 108 au début des années 1970. Quant à l'UE, elle s'est dotée dans les années 1990 d'un groupe nommé « échange d'informations et protection des données » (DAPIX) au niveau du Conseil de l'UE, et a institutionnalisé le réseau transgouvernemental des autorités de protection des données en créant le Groupe de travail de l'article 29 (Newman, 2008), sur lequel nous allons revenir. Les premières décisions fondatrices de la CJUE en matière de droit *à la* de *de la* protection des données à caractère personnel remontent au début des années 2000[100], bien des années avant la publication de la proposition de RGPD en janvier 2012. Du côté de la société civile, nous pouvons identifier des associations actives au niveau de l'UE depuis le début des années 2000 comme EDRi, fondée en 2002[101]. Quant à la *Federation of European Direct and Interactive Marketing* (FEDMA), une fédération d'associations représentant l'industrie du marketing direct, un ancien employé que nous avons interrogé nous a parlé d'archives dont ils disposaient et qui remontaient aux négociations sur la directive de 1995. Il existe donc bel et bien des acteurs – à la fois sur le plan individuel et sur le plan institutionnel – qui ont cherché à influencer de façon durable les politiques publiques de protection des données à caractère personnel, au niveau de l'UE, au moins à partir des années 1990.

Le troisième critère est qu'il doit exister des administrations compétentes à tous les niveaux. En matière de protection des données, les autorités compétentes sont les autorités de protection des données. La directive de 1995, puis le RGPD, ont imposé à chaque État membre de disposer d'au moins une autorité administrative indépendante nationale chargée du contrôle de l'application du droit *de la* protection des données à caractère personnel, dotée de pouvoirs de sanction effectifs. Dans certains États européens fédéraux, ou divisés en régions dotées d'une autonomie étendue, disposent même d'autorités de contrôle à un niveau infra-national. C'est le cas en Allemagne, où chaque Land dispose d'une autorité de contrôle compétente pour tous les responsables de traitements qui ne relèvent pas du droit fédéral. La Flandre, la Catalogne et le Pays Basque disposent aussi de leur propre autorité de contrôle, compétente pour les personnes

100 Voir : CJCE 20 mai 2003 « Österreichischer Rundfunk » Aff. C-465/00, C-138/01 et C-139/01, et CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01.

101 Voir la page de présentation de l'association sur son site web : https://edri.org/about/ (page consultée le 1er juin 2019).

morales de droit public relevant respectivement du gouvernement flamand, et des communautés autonomes catalane et basque.

Contrairement aux autorités régionales, chaque autorité nationale envoie un représentant au Groupe de travail de l'Article 29, créé par la directive de 1995.

Il n'existait aucune institution en charge de la protection des données à caractère personnel à l'échelon communautaire avant 1995. Avec la mise en place du groupe de travail de l'Article 29 (G29), effective en 1996[102], la directive 95/46/CE a toutefois entamé l'institutionnalisation d'une proto-institution qui, si elle n'était dotée que de pouvoirs consultatifs, pouvait *de facto* (à défaut de *de jure*) être considérée comme une institution en charge à l'échelle de l'UE de la protection des données. Son secrétariat était assuré par une unité affectée à la « libre circulation de l'information, protection des données et aspects internationaux s'y référant » de l'ancienne DG XV, la direction générale en charge du marché intérieur et des services financiers (G29, 1997), devenue depuis la DG MARKT (pour DG « Marché intérieur »). En 2004, ce secrétariat a été transféré à l'unité de protection des données de la DG Justice, Liberté et Sécurité, s'émancipant ainsi de la sphère des politiques du marché intérieur (G29, 2005, p. 127). Entre temps, une autre institution était créée à l'échelon communautaire : le Contrôleur européen à la protection des données, autorité administrative indépendante chargée du contrôle du respect du règlement 45/2001/CE[103] imposant des règles de protection des données aux institutions communautaires.

Le G29 était chargé de conseiller la Commission européenne et de publier des avis « sur le niveau de protection dans la Communauté et dans les pays tiers », « sur les codes de conduite élaborés au niveau communautaire », et « sur toute question concernant la protection des personnes à l'égard du traitement de données à caractère personnel dans la Communauté » (art. 29 de la directive 95/46/CE). Ces avis ont joué un rôle important dans la formation d'une doctrine commune aux différentes autorités de protection des données ; ils ont été régulièrement cités dans des décisions nationales. La mise en commun de connaissances permettait en effet aux autorités de protection des données de surmonter leur manque de moyens humains et financiers suffisants pour développer une expertise complète sur l'ensemble des sujets les concernant.

Ce groupe a également permis, d'une façon indirecte, de créer du droit. Par exemple, les règles contraignantes d'entreprise sont l'une des bases légales permettant de déroger à l'interdiction de transfert de données personnelles vers des pays tiers au sein d'un même groupe d'entreprises[104]. Cette modalité n'était pas prévue dans la directive de 1995, mais les membres du G29 s'étaient mis d'accord entre 2003 et 2005 pour inventer cette procédure. Elle fut acceptée par une majorité d'entre eux, en se fondant sur des dispositions de cette directive (G29, 2003 et 2005) bien avant d'être intégrée à un texte de nature législative : le RGPD, qui y consacre l'article 47.

---

102 La première réunion du G29 s'est tenue à Bruxelles le 17 janvier 1996 (G29, 1997, p. 6).

103 Règlement 45/2001/CE du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

104 Article 47 du RGPD

En 2012, plusieurs autorités de protection des données se sont coordonnées pour mener des opérations de contrôle en même temps auprès de l'entreprise Google (Kohnstamm, 2012b et Falque-Pierrotin et al., 2012), aboutissant ensuite à des sanctions qui, elles, furent prises au niveau national, à la suite de procédures nationales, par les autorités nationales de protection des données[105]. La création de mécanismes formels de coopération avait été l'une des revendications du G29 pendant le processus d'adoption du RGPD[106].

Se réunissant plusieurs fois par an à Bruxelles en plénière, c'est-à-dire au niveau des dirigeants des autorités de protection des données, le G29 se subdivisait ensuite en plusieurs groupes de travail thématiques dans lequel participaient des employés de ces autorités. Son président était élu parmi ses membres. Il ne disposait toutefois pas de son propre personnel, ni de la personnalité juridique. Le G29, désormais remplacé par le Comité européen de protection des données – qui dispose de la personnalité juridique – était un réseau transgouvernemental[107] qui pré-existait à la directive de 1995, mais à laquelle cette dernière a donné une forme de reconnaissance institutionnelle qui en a fait, selon les termes de Burkard Eberlein et Abraham Newman (2006), un réseau transgouvernemental « incorporé » (« *incorporated* »).

Pour achever ce tableau des institutions et autorités en charge de la mise en œuvre de la politique communautaire de protection des données à caractère personnel, il faut également mentionner les délégués à la protection des données. Ces personnes, anciennement connus en France sous le nom de correspondants informatique et libertés, sont désignées par un responsable du traitement pour contrôler en interne le respect des règles de protection des données. Imposée entre autres à toutes les autorités publiques – y compris aux collectivités territoriales – depuis le RGPD, cette fonction était déjà prévue et réglementée avant le RGPD dans certains pays de l'UE (Rossi, 2015b). Lorsqu'ils sont nommés par des collectivités territoriales, ils sont un autre relai, à un niveau infra-national, des politiques publiques de protection des données, dont les principaux textes juridiques sont adoptés à l'échelon de l'Union.

Ainsi, lorsqu'en 2009, la Commission européenne entama les premières consultations en vue de réformer le droit communautaire en matière de protection des données à caractère personnel, le G29 avait 13 ans, il existait depuis au moins aussi longtemps une unité en charge de ce domaine de l'action publique à la DG MARKT, puis à la DG JLS, et l'EDPS existait depuis cinq ans (EDPS, 2005).

L'hypothèse de l'existence d'une politique publique de protection des données à l'échelle de l'Union européenne passe donc bien le test de ce troisième critère.

---

105 Voir les décisions de l'*Agencia Española de Protectión de Datos* (AEPD) de 2013 : Procedimiento PS/0034/2013 18 Diciembre 2013, et de la CNIL de 2013 : délibération 2013-420 du 3 janvier 2014 de la formation restreinte prononçant une sanction pécuniaire à l'encontrede la société Google Inc.

106 La question était déjà évoquée avant la publication de la proposition de RGPD, dans un courrier de 2011 adressé à Viviane Reding (Kohnstamm, 2011)

107 Robert Keohane et Joseph Nye définissent ainsi ce concept : « Nous définissons les relations transgouvernementales comme des jeux de relations directes entre sous-unités de différents gouvernements qui ne sont pas contrôlés ou guidés de près par les politiques des cabinets ou ministres de ces gouvernements. » Traduction de l'auteur. Texte original : « We define transgovernmental relations as sets of direct interactions among sub-units of different governments that are not controlled or closely guided by the policies of the cabinets or chief executives of those governments. » (Keohane et Nye, 1974, p. 43)

Enfin, pour considérer qu'il existe véritablement une politique publique au niveau de l'UE de protection des données à caractère personnel, le quatrième critère énoncé précédemment veut qu'il soit possible d'identifier des groupes d'intérêt qui considèrent ce domaine comme étant une priorité. En 2009, les groupes d'intérêt actifs au niveau de l'Union dans ce domaine étaient nettement moins nombreux qu'à la fin de la procédure d'adoption du RGPD, mais ils n'étaient pas absents.

Il existait déjà de nombreuses associations nationales, comme la Quadrature du Net et le Centre d'études sur la citoyenneté, l'informatisation et les libertés (CECIL) en France, *Bits of Freedom* aux Pays-Bas, *Privacy International* au Royaume-Uni ou encore *Digital Rights Ireland*. Ces associations avaient toutes pour priorité la défense des droits fondamentaux en environnement numérique. Au niveau de l'Union, certaines d'entre elles s'étaient déjà fédérées pour fonder en 2002 le collectif Digital Rights Europe, qui dispose depuis 2009 de bureaux et de salariés à Bruxelles (EDRi, 2011).

Au niveau des groupes d'intérêt industriels, plusieurs entreprises ont participé dès 2009 aux consultations de la Commission européenne. Parmi ces entreprises, certaines se sont rapidement regroupées dans des groupes d'intérêt créés pour suivre et influencer le processus de réforme de la directive de 1995. L'*European Privacy Association*, qui a participé à la consultation de 2009, a ainsi été créée avec le soutien d'entreprises comme Microsoft, Google et Yahoo (Baker, 2013 ; Vanheste et Martijn, 2013). D'autres associations de représentation des intérêts industriels, déjà constituées, comme DIGITALEUROPE, participèrent aussi dès 2009 aux consultations (Consultation de 2009, DIGITALEUROPE1, 2009). Alistair Tempest, directeur général de la FEDMA fit partie des participants invités à la conférence sur le futur du droit *de la* protection des données organisée par la Commission européenne le 19 mai 2009 (Tempest, 2009). Cela suggère nécessairement de la part de ces acteurs une activité de veille et d'influence précédant les premières consultations de la Commission en 2009.

Ainsi, bien que la structuration de groupes d'intérêt stables faisant de l'influence des politiques publiques produites par l'UE en matière de protection des données à caractère personnel était relativement récente au moment où la Commission entama le processus de consultations qui aboutit à ses propositions de réforme de janvier 2012, il est tout à fait possible d'identifier de tels groupes actifs sur l'ensemble de la durée du processus. Nous pouvons donc considérer que ce critère est lui aussi rempli par les politiques publiques de protection des données à caractère personnel de l'UE.

L'hypothèse de l'existence d'une politique publique de protection des données à caractère personnel au niveau de l'UE se vérifie donc bel et bien, et ce au moins depuis 2009, l'année des premiers travaux sur la réforme de la directive 95/46/CE. L'étudier au prisme d'une méthodologie fondée sur les approches cognitives des politiques publiques est donc pertinent pour comprendre les interactions entre référentiels et discours rivaux ayant abouti à la rédaction du RGPD tel qu'il a finalement été adopté en avril 2016.

4.1.5. Les groupes d'intérêt dans l'Union européenne : expertise, crédibilité, légitimité

Entre 2009, date des premières consultations de la Commission européenne sur l'avenir du droit communautaire *de la* protection des données à caractère personnel, et 2016, date de l'adoption définitive du RGPD, un grand nombre de groupes d'intérêt, comme EDRi et Digitaleurope, ont cherché à influencer la rédaction de ce texte dans un sens qui leur soit favorable.

Cette notion de groupe d'intérêt constitue « une notion à la fois usuelle et scientifique difficile et délicate à saisir et à définir » (Grossman et Saurugger, 2012, p. 9). Il n'est pas intuitivement évident de regrouper sous une même catégorie des groupes d'acteurs aussi divers que, pour prendre des exemples d'organismes ayant participé à la consultation de la Commission de 2009, des fédérations d'entreprises qui veulent, comme l'*Interactive Advertising Bureau* (IAB), défendre leurs intérêts économiques, des cabinets de conseil comme Ernst & Young, des cabinets d'avocats comme Linklaters, des associations militantes comme *Privacy International*, ou encore des associations regroupant des professionnels comme la *Gesellschaft für Datenschutz und Datensicherung*, qui regroupe en Allemagne des délégués à la protection des données, à l'instar de l'AFCDP française. La tableau peut se complexifier si l'on prend en compte qu'il existe désormais non seulement des associations de professionnels de la protection des données au niveau national, mais que certaines de ces dernières se sont fédérées au sein de la *Confederation of European Data Protection Organisations*. Et, puisque nous évoquons ici la question des associations qui ont notamment pour objectif de défendre les intérêts d'une profession, nous pourrions évoquer la question de groupes d'intérêt qui n'ont pas participé à la consultation de 2009, comme les syndicats, dont une partie sont regroupés dans la Confédération européenne des syndicats[108], les représentants de communautés religieuses[109], ou encore les représentations d'entités infra-nationales, comme les régions. La Bavière est par exemple connue à Bruxelles pour détenir un manoir dans le parc Leopold, jouxtant le bâtiment bruxellois du Parlement européen, à côté de la place du Luxembourg. Le quartier européen entre l'avenue des Arts, la rue du Trône, la chaussée de Wavre, le parc du Cinquantenaire et la rue la Loi, héberge un nombre considérable de bureaux appartenant à des régions, des cabinets d'avocats, des lobbyistes professionnels, des associations de natures diverses…

108 La Confédération européenne des syndicats n'a pas participé à la consultation de 2009, mais a participé à celle de 2010

109 Nous avons récupéré via Lobbyplag un *position paper* du 9 novembre 2012 co-signé par le Conseil des Églises évangéliques d'Allemagne (*Rates der Evangelischen Kirche in Deutschland*) et le Commissariat des évêques allemands (*Kommissariats der deutschen Bischöfe*), contenant des propositions d'amendements au RGPD. Ces organisations n'ont toutefois pas envoyé de contributions aux consultations de 2009 et de 2010.

Figure 15 : *Capture d'écran d'un extrait de la carte de Bruxelles sur le site* Google Maps*, prise le 2 mai 2019, montrant la proximité géographique entre l'hémicycle bruxellois du Parlement européen, le bureau de représentation du Land de Bavière auprès de l'UE, et le siège bruxellois de Google, de part et d'autre du parc Léopold.*

Emiliano Grossman et Sabine Saurugger proposent une définition large de la notion de « groupe d'intérêt », que nous reprenons à notre compte car elle permet justement d'englober cette diversité d'acteurs :

> « Dans son acception la plus large, la notion de groupe d'intérêt est définie comme une entité qui a comme objectif de représenter les intérêts d'une section spécifique de la société dans l'espace public. » (Grossman et Saurugger, 2012, p. 9)

À la différence de la notion de mouvement social, celle de groupe d'intérêt désigne des entités organisées, qui cherchent à influencer des politiques publiques (Grossman et Saurugger, 2012, p. 10-11), mais ne disposent pas elles-mêmes de l'autorité d'adopter des décisions juridiquement contraignantes et qui, contrairement aux institutions politiques ou administratives,

ne peuvent produire du droit que dans un cadre contractuel soumis aux lois et règlements, tout en bas de la hiérarchie des normes.

Cette première définition appelle bien sûr quelques précisions, d'abord sur le fait que ces groupes représentent les intérêts « d'une section spécifique de la société », et ensuite, sur la notion même d'intérêt.

Il serait en effet possible d'objecter à la définition que nous avons choisie que des associations comme Greenpeace défendent l'intérêt de l'ensemble des citoyens, voire dans ce cas précis de tous les organismes vivants sur Terre. Mais si cela est vrai selon les employés, militants et soutiens de Greenpeace, il n'en demeure pas moins que Greenpeace n'existerait sans doute pas s'il existait un consensus social absolu autour des objectifs et intérêts défendus par Greenpeace. Ainsi, même une ONG comme Greenpeace, qui prétend défendre des intérêts universels, et déploie des efforts dont nous pouvons sans trop de difficultés admettre la sincérité pour agir en faveur de l'intérêt commun, agit dans un sens qui ne convient qu'à une partie (même très large) de la société, composée d'individus partageant ses convictions et sa vision de l'intérêt général.

Il peut paraître évident que la survie à long terme de l'espèce humaine est dans l'intérêt de chaque individu, et que, dès lors, il devrait y avoir un consensus autour de mesures destinées, par exemple, à contenir le réchauffement climatique dans des limites compatibles avec un tel objectif. Mais c'est, d'une part, partir du principe qu'il existe un consensus autour de la désirabilité d'une survie à long-terme de l'espèce humaine. D'autre part, et de façon moins controversée, il est possible de croire en la capacité de l'innovation technique à nous permettre d'encaisser les effets du réchauffement climatique. Enfin, il est possible, par ignorance de certaines connaissances scientifiques sur le sujet, ou par doutes sur la légitimité de ces dernières, de ne pas croire en la réalité ou en la gravité du réchauffement climatique. Dans ce cas, il peut paraît incongru de souhaiter adopter des mesures contraignantes, ayant des effets perçus comme négatifs par exemple sur la capacité d'augmentation de la production industrielle.

Ceci nous amène à discuter brièvement du terme « intérêt » composant la notion de groupe d'intérêt, pour rappeler qu'il n'existe pas d'intérêts dans la nature et que ces derniers sont bien le fruit d'une construction sociale.

Une idée fréquemment répandue est qu'il existerait des intérêts objectifs, intégralement dissociables de la perception que les acteurs en ont. Selon cette optique, qui, tant chez les penseurs marxistes que chez les économistes néoclassiques et chez les néolibéraux, est un héritage de l'économie classique, le dévoilement de ces intérêts objectifs, matériels, de nature économique, permettrait d'expliquer en dernier ressort le comportement des humains, sans qu'il soit nécessaire de s'intéresser à leurs discours, à leurs perceptions, à leurs émotions. Si chaque

individu est un *homo economicus* qui cherche à maximiser son utilité matérielle, alors il est possible d'en déduire mécaniquement les intérêts en poursuite desquels il agit. Ainsi, pour reprendre Cornelius Castoriadis, « derrière la tentative d'ériger les forces productives en facteur autonome et déterminant de l'évolution historique, il y a l'idée de condenser dans un schéma simple les « forces » dont l'action a dominé cette évolution. Et la simplicité du schéma vient de ce que les mêmes forces agissant sur les mêmes objets doivent produire les même enchaînements d'effets » (Castoriadis, 2006 [1975], p. 35).

Or les intérêts en vertu desquels agissent les acteurs dépendent de ce qu'ils perçoivent comme étant leurs intérêts, en fonction d'un contexte socio-culturel donné. Ainsi, « qu'un sens économique latent puisse souvent être dévoilé dans les actes qui apparemment n'en possèdent pas, c'est certain. Mais cela ne signifie ni qu'il est le seul, ni qu'il est premier, ni surtout que son contenu soit toujours premier, ni surtout que son contenu soit toujours et partout la maximisation de la « satisfaction économique » au sens capitaliste-occidental » (Castoriadis, 2006 [1975], p. 41). Pour qu'une situation devienne un problème politique dont se saisit un groupe d'intérêt, il faut que les individus qui composent ce groupe perçoivent un intérêt à agir pour changer cette situation. Ce qui suppose des phénomènes de construction du problème, de mise à l'agenda (Cefaï, 1996), mais aussi de construction d'une identité de groupe autour des intérêts défendus (Fillieule et Péchu, 1993).

Il existe une distinction entre des groupes d'intérêt « publics » ou « économiques » (Grossman et Saurugger, 2012, p. 216), fondés sur des intérêts matériels (« *material groups* ») ou d'intention (« *purposive groups* ») (Sabatier, 1998, p. 116) ou encore, « *interests-based* » ou « *principles-based*[110] ». Un groupe d'intérêt économique comme l'IAB a ceci de particulier qu'il doit sa survie économique à la capacité de ses employés à produire des discours qui défendent efficacement les intérêts économiques (souvent réduits aux seuls intérêts financiers à court terme, d'ailleurs) des adhérents payant leurs cotisations. Il en va de même pour un cabinet de conseil en relations publiques, payé pour plaider les intérêts de tiers, qu'il soit convaincu lui-même de ses arguments ou non. Toutefois, même les intérêts défendus par les groupes d'intérêt « économiques » sont le fruit d'un processus de construction social, ancré dans un contexte historique et faisant référence à des imaginaires sociaux.

Même dans le cas de tels groupes d'intérêt industriels, la sélection des intérêts défendus dépend de certains référentiels. Il n'y a rien de naturel dans le fait de considérer que l'intérêt d'une entreprise est la maximisation des gains matériels de ses actionnaires. Il existe d'ailleurs des processus d'apprentissage, y compris chez ces acteurs, qui montrent qu'ils peuvent changer d'avis sur ce qui constitue leur intérêt. Nous avons eu en entretien des illustrations d'acteurs ayant redéfini leurs positions sur certains sujets pendant le processus d'élaboration du RGPD, en revoyant ainsi ce qu'ils ont perçu comme allant dans le sens des intérêts défendus par leur groupe d'intérêt. Un des lobbyistes interrogés évoqua ainsi le fait que des entreprises états-uniennes, confrontées aux discussions autour de l'adoption du RGPD, devinrent peu à peu convaincues de

110 L'expression « principles-based » a été utilisée par Jens-Henrik Jeppesen en entretien.

l'utilité d'une telle loi pour leurs intérêts, comparativement à un paysage juridique de la protection des données aux États-Unis complexe, fragmenté et difficile à maîtriser :

> « […]Quoi que les gens pensent de ce qui s'est produit en Europe, le fait est que l'Europe est probablement meneuse dans ce domaine. […] C'est drôle… enfin, c'est comme ça que fonctionne le lobbying. Un peu comme des montagnes russes : on commence par dire "c'est la fin du monde !", puis ensuite on devient constructif et on cherche des ouvertures, on rencontre quelques opportunités pour discuter, on commence à avoir de nouvelles idées. Puis ensuite… vous savez… on en finit par être confronté à la réalité : okay, certaines choses se sont améliorées, d'autres choses sont encore ouvertes au changement, alors maintenant, comment est-ce qu'on avance ? […] Je pense réellement que vous allez voir que des changements vont se produire du côté des États-Unis[111]. » (Entretien Euro5)

Une expérience similaire a été rapportée par un autre lobbyiste au sujet d'un membre russe de l'association pour laquelle il travaillait :

> « […] nous avons toujours disposé de membres en dehors de l'Europe. Mais ils n'étaient pas réellement impliqués dans les discussions sur le RGPD. Ils ne trouvaient pas cela intéressant, à l'époque. Je pense qu'ils étaient intéressés dans le sens où ils savaient… je veux dire que par exemple, hors de l'Europe, nous avons ce membre russe […] qui [était] intéressé dans le sens où il savait que ces règles concerneraient la Russie tôt ou tard[112]. » (Entretien avec Razvan Antemir)

Jens-Henrik Jeppesen, de CDT, un groupe d'intention (« *purposive* »), évoqua quant à lui la façon dont les membres de CDT ont changé d'avis sur le droit au déréférencement, auquel ils étaient initialement opposés en raison du risque qu'ils y voyaient pour la liberté d'expression :

> « Nous étions inquiets de la façon dont cela allait être utilisé, vous voyez ? C'était très controversé à l'époque. Et, vous savez, les journalistes, les médias, les journaux, etc.,

111 Traduit de l'anglais. Texte original : « […] Regardless of what people feel about what's happened in Europe, is that, actually, Europe is probably leading the way on this. […] It's kind of a funny… I mean that's how lobbying works. You kind of go up and down, and you start like : it's the end of the world ! And then you are constructive, and trying to build, and you get some openings, and some opportunities that you discuss, and you start to have new ideas, then you also, then you kind of, you know, it hits the reality, that, okay, some things have improved, some things are open to change, now how do we move forward ? […] I do think that on the US side you will probably see some changes coming. »

112 Traduit de l'anglais. Texte original : « […] we always had members outside of Europe. But they were not so involved in the GDPR discussions. They didn't see it as as interesting at the time. I think they were interested in the sense that they knew… I mean from outside Europe, for example, we have the Russian member […] who [was] interested in the sense that they knew these rules would come to them sooner or later. »

étaient très critiques des types de matériaux qui pourraient être déréférencés à la suite de décisions sur le droit à l'oubli. […] Nous avions considéré au départ que tout ce qui était publié légalement sur Internet devait pouvoir être retrouvé. [Mais] selon les informations limitées dont nous disposons, je pense que nous pouvons concéder que l'existence aujourd'hui de ce principe n'a pas mené aux conséquences […] graves que nous redoutions. Que des politiciens, des escrocs et des criminels en tout genre allaient pouvoir faire oublier leurs méfaits [*clean their records*][113]. » (Entretien avec Jens-Henrik Jeppesen)

Pour revenir au sujet de discours produits par des acteurs n'y croyant pas, mais payés pour les produire afin de défendre ce que leurs clients perçoivent comme leurs intérêts : ce n'est pas parce que les auteurs initiaux de ces discours peuvent ne pas y croire eux-mêmes, qu'ils ne convainquent personne par la suite. Il est donc méthodologiquement impossible de discriminer entre les discours « sincères » et les discours « intéressés », puisqu'un même discours peut être l'un ou l'autre selon l'énonciateur et selon le contexte. En outre, il est impossible dans la recherche en sciences sociales d'accéder aux intentions des acteurs. Nous ne ferons donc pas de distinctions entre des discours sincères et des discours servant exclusivement des intérêts particuliers ou sectoriels. Nous pourrons au mieux, dans les cas où une telle indication est pertinente, mentionner le fait qu'un discours, dans un contexte donné, concorde avec les intérêts poursuivis par tel ou tel groupe d'acteurs, sans que cela ne préjuge en rien leur sincérité ou insincérité.

Les éléments que nous venons de discuter contribuent à justifier le fait d'avoir une définition de « groupe d'intérêt » qui englobe toutes les entités organisées cherchant à influencer des politiques publiques en fonction d'intérêts sectoriels, malgré la grande diversité d'acteurs que cette définition recouvre, et le fait qu'il paraisse *a priori* contre-intuitif de regrouper sous le même vocable un syndicat et une organisation patronale, une ONG comme Greenpeace et le service chargé des affaires publiques d'une multinationale. Toutefois, à partir du sous-chapitre sur l'identification des coalitions de cause rivales[114] nous serons parfois amenés à distinguer des « ONG » des « lobbies », car ces termes distinguent dans le vocabulaire des acteurs les groupes d'intérêt actifs sur le dossier de l'adoption du RGPD en fonction de leur appartenance, respectivement, à la coalition des défenseurs de la vie privée ou à la coalition industrielle. « ONG » comme « lobbies » demeurent toutefois tous deux des groupes d'intérêt.

113 Traduit de l'anglais. Texte original : « We were worried about the way that this was going to be used, right ? It was very controversial at the time. And, you know, journalists, media organisations, newspapers, etc, were very critical about the types of material that might be delisted as a result of the right to be forgotten decisions. […] Our basic view, was: material that was lawfully published on the Internet must be findable. [But] based on the limited information that we have, I think we would concede that the fact that this principle now exists has not led to the […] dire consequences that we were afraid of. That all manner of politicians, and crooks and criminals would now get to clean their records. »

114 Cf. section 4.2.

Il existe des groupes d'intérêt au niveau national, mais également au niveau supranational. Les groupes d'intérêt ont d'ailleurs, au niveau de l'UE un rôle particulier dans l'élaboration des politiques publiques. Parmi ces groupes, ceux défendant les intérêts économiques d'entreprises ou de fédérations d'entreprises membres dominent très largement en nombre. Cela est dû en partie au fait que les groupes d'intérêt qui défendent des intérêts généraux diffus, ou des biens communs, disposent de moins de ressources que les groupes d'intérêt industriels défendant des intérêts bien définis et concernant un nombre limité d'acteurs qui perçoivent alors aisément le fait que personne d'autre qu'eux n'ira défendre leurs intérêts. À l'inverse, lorsqu'un plus grand nombre de personnes partagent un même intérêt, ces personnes ont la tentation de ne pas s'investir, dans l'idée que de toutes façons, il y aura bien quelqu'un, dans la multitude de gens partageant leurs intérêts, qui s'investiront à leur place (Grossman et Saurugger, 2012, p. 237).

Cette prédominance de groupes d'intérêt économiques est aussi due au fait que les communautés européennes aient historiquement d'abord développé une activité régulatrice dans les domaines de l'industrie et du commerce avant de s'emparer d'autres champs de compétence, comme l'environnement, l'éducation ou les droits humains (Grossman et Saurugger, 2012, p. 237). Ce n'est que relativement tard que des ONG comme Amnesty International ont investi l'échelon européen, pour obtenir de l'UE que ses politiques publiques améliorent la garantie des droits humains, tout en faisant face au fait que l'UE ne dispose pas, sauf exception, des compétences d'attribution requises pour adopter des mesures d'ordre général dans ce domaine (Poinsot, 2005 cité par Douillet et Maillard, 2010, p. 83-84).

Pour donner quelques chiffres, au 2 mai 2019, il y avait 11 752 groupes d'intérêt inscrits au registre de transparence de la Commission européenne, dont 3141 étaient classées dans la catégorie « organisations non-gouvernementales », les autres grandes catégories étant les « cabinets de consultants spécialisés/cabinets d'avocats/consultants agissant en qualité d'indépendants », les « représentants internes, groupements professionnels et associations syndicales et professionnelles », « groupes de réflexion, organismes de recherche et institutions académiques », les « organisations représentant des églises et des communautés religieuses » et enfin les « organisations représentant des autorités locales, régionales et municipales, autres entités publiques ou mixtes, etc[115]. ». Bien entendu, le fait de s'être inscrit dans la catégorie des « ONG » ne garantit en rien le fait que le groupe d'intérêts en question ne soit pas financé par des intérêts industriels, et juridiquement, il n'existe pas de différence entre une association « professionnelle » et une « ONG » qui, lorsqu'elles ont leur siège à Bruxelles, prennent souvent la forme d'une association sans but lucratif de droit belge. Cela dit, ces chiffres permettent de représenter de façon chiffrée – même très imprécise – la domination numérique des groupes d'intérêt industriels vis-à-vis des groupes d'intérêt se construisant autour de la défense d'intérêts publics.

115 Ces chiffres proviennent de recherches effectuées sur le registre de transparence de la Commission européenne à l'adresse : http://ec.europa.eu/transparencyregister/public/consultation/search.do?locale=en&reset= (page consultlée le 2 mai 2019).

La Commission européenne, qui détient le monopole de l'initiative législative au niveau de l'UE, a, pour diverses raisons, développé une relation d'interdépendance assez forte avec les différents groupes d'intérêt qui cherchent à en influencer la production normative.

Plusieurs raisons expliquent cela.

Il y a tout d'abord la faiblesse organisationnelle de la Commission, dont les directions générales ont des effectifs limités. En 2010, il n'y avait ainsi que 350 personnes travaillant à la DG JLS de la Commission européenne, avant sa scission entre la DG Justice – qui a hérité du dossier sur la réforme du droit *de la* protection des données à caractère personnel – et la DG Affaires Intérieures (Douillet et Maillard, 2010, p. 79-80). Cela est très peu par rapport au nombre de dossiers à suivre, à leur complexité, et au nombre d'acteurs qu'ils concernent. Faire appel à de l'expertise extérieure, si possible mise à disposition gratuitement en échange de fenêtres d'opportunité permettant d'influencer la production de politiques publiques (Bouwen, 2002, 2009), est entre autres une façon de combler cette faiblesse structurelle de la Commission (Douillet et Maillard, 2010, p. 78).

Face à un déficit de médiatisation, voire de légitimité démocratique (Badouard, 2012 ; Eriksen, 2009), et perçue – y compris par elle-même – comme étant éloignée du terrain, la Commission européenne peine à trouver des ressources de légitimité lui permettant d'imposer son agenda et ses préférences politiques aux États-membres qui, siégeant au Conseil de l'UE, peuvent rejeter ses propositions législatives. Dès lors, « l'expertise apparaît comme un moyen de mieux défendre les propositions de la Commission en fournissant des ressources supplémentaires mais elle permet aussi de légitimer les positions des agents de la Commission et/ou de les « substantialiser » (*substantiating*) en leur donnant de la crédibilité dans un champ politique contesté » (Douillet et Maillard, 2010, p. 78). Ce recours à l'expertise comme « source de pouvoir[116] » (Newman, 2008, p. 79), auxquels les groupes d'intérêt prêtent – par opportunité – leur concours, confère des ressources en légitimité à la Commission européenne pour mieux poursuivre ses objectifs politiques. Il a en partie pour effet pour effet de renforcer la culture du consensus qui règne dans les processus de décision de l'UE (Dehousse, Novak et Bendjaballah, 2017), car l'expertise agit en délégitimant la parole politique (Robert, 2003). La Commission a mis en place des mécanismes institutionnels pour capter cette expertise et la légitimité qui en découle, notamment par le biais de consultations, ou la mise en place de comités d'experts chargés de la conseiller.

Comme les groupes d'intérêt ne disposent pas du pouvoir d'adopter formellement les décisions qu'ils cherchent à obtenir, ils ne peuvent qu'essayer d'influencer les personnes détentrices de l'autorité compétente. Leur répertoire d'actions possibles va de la négociation au

116 Texte original : « Expertise as a source of power ».

recours à l'expertise en passant par la juridicisation, la protestation et, dans certains cas, la politisation, c'est-à-dire la transformation de certains groupes d'intérêt en partis politiques (Grossman et Saurugger, 2012, p. 16-18).

Au niveau de l'UE, la stratégie de la juridicisation (Grossman et Saurugger, 2012) est fréquemment employée. Nous y reviendrons dans l'étude des controverses jurisprudentielles autour de la notion juridique de « donnée à caractère personnel[117] ». Si la juridicisation suppose la production d'un discours, il s'agit d'un discours fondé sur l'expertise et un langage juridiques et ne cherchant pas à changer la rédaction des textes de droit mais seulement leur interprétation. Il est à distinguer des discours de plaidoyer.

Le plaidoyer, aussi désigné sous le terme anglais de « *lobbying*[118] » consiste à chercher, par divers canaux de communication, formels et informels, à persuader ou convaincre les décideurs publics que l'on cherche à influencer, sans que, contrairement aux discours produits dans le cadre d'une stratégie de judiciarisation, les arguments doivent être limités à un registre juridique. Concrètement, cela peut passer par la participation à des négociations, à des consultations, à des discussions informelles avec des décideurs publics, à l'obtention de rendez-vous avec ces mêmes personnes pour faire valoir son point de vue, à l'envoi de courrier, la publication de *position papers* (ou *policy papers*) détaillant la position officielle du groupe, ou à la participation à des débats publics dans des conférences ou par voie de presse afin d'influencer le cadrage du débat en cours dans les arènes efficaces. Au niveau de l'UE, une modalité fréquemment exploitée est la publication de publirédactionnels dans des journaux et revues qui ont pour cible de marché des personnes travaillant pour les institutions européennes, comme *European Voice*, devenu *Politico Europe* (European Voice et ICDP, 2013). Le plaidoyer peut – et c'est souvent le cas au niveau de l'UE – faire appel au registre de l'expertise afin de renforcer la légitimité et la crédibilité de ses arguments. Dans le vocabulaire des acteurs, un terme qui a été utilisé pour désigner cette action de plaidoyer est celui d'« *engagement* », c'est-à-dire d'interaction :

> « Alors certains experts du CDT sont venus en Europe à l'époque, dans plusieurs conférences, pour participer aux débats, et ainsi de suite. Mais il n'y a pas eu d'*engagement* systématique[119]. » (Entretien avec Jens-Henrik Jeppesen)

117 Cf. section 6.3.

118 La différence sémantique entre les deux termes relève du jugement de valeur, le *lobbying* était normativement déprécié par rapport au « plaidoyer » (en anglais, parfois : « *advocacy* »), dont la connotation est plus noble.

119 Traduit de l'anglais. Texte original : « So some CDT experts have come to Europe at the time, at various conferences, participating in debates, and so on. But there really hasn't been a sort of systematic *engagement.* »

> « Ce qui signifiait que du point de vue des industries, il devenait plus difficile d'*interagir* [*to engage*] avec tous les parties prenantes[120]. » (Entretien Euro5)

Ces « *engagements* » ont pris place dans le cadre d'un processus (« *process* »), d'un « débat » (« *debat* ») ou d'une « discussion » (« *discussion* »), qui a aboutit à l'adoption du RGPD :

> « Je ne pense pas qu'ils soient assez visibles, ni qu'ils aient beaucoup d'influence dans la *discussion*[121]. » (Entretien avec Razvan Antemir)

> « L'un des enjeux de ce *débat* était de définir les données à caractère personnel.[122] » (Entretien Euro5)

La trajectoire des acteurs de groupes d'intérêt ayant participé à ces « discussions » sur le RGPD contribue à justifier la définition englobante que nous avons choisie, puisqu'elle montre une proximité professionnelle forte entre acteurs de groupes d'intérêt de nature diverse œuvrant dans le même sous-système de politiques publiques. Ces trajectoires d'acteurs illustrent un phénomène général, qui n'est pas spécifique à ce sous-système de politiques publiques, de professionnalisation de la représentation d'intérêts au niveau de l'UE (Saurugger, 2012 ; Saurugger et Heike, 2013).

Laura Blanco, de CDT, résuma ainsi son parcours professionnel :

> « Avant, je travaillais dans le département des affaires publiques d'un cabinet d'avocats. Il y avait différents enjeux et différents secteurs. Ce qui m'a personnellement […] réellement attiré dans le fait de travailler pour le CDT est […] sa mission […] parce qu'elle a des conséquences sur la vie quotidienne de tous les citoyens[123] » (Entretien avec Laura Blanco)

120 Traduit de l'anglais. Texte original : « Which meant that for industry perspective it became more difficult to *engage* with all the stakeholders. »

121 Traduit de l'anglais. Texte original : « I don't think they're visible enough, and I don't think they have a lot of influence on the *discussion*. »

122 Traduit de l'anglais. Texte original : « One of the issues with this whole *debate* was trying to define personal data. »

123 Traduit de l'anglais. Texte original : « I was working before for a law firm. But the public affairs department of a law firm. And there were various issues, and various sectors. So for me personally, […] what really attracted me to work for CDT is […] the mission it has […] because it is something that affects the daily lives of every citizen. »

Jens-Henrik Jeppesen, lui aussi de CDT, travaillait auparavant pour des équipes d'affaires publiques dans des entreprises ayant des intérêts économiques et politiques à défendre :

> « J'ai passé de nombreuses années à la tête d'équipes d'affaires publiques et donc d'équipes de lobbying. Et […] une chose qui m'a attiré au CDT était la perspective d'un défi totalement nouveau, […] consistant à défendre non seulement des intérêts commerciaux mais également l'intérêt général[124] » (Entretien avec Jens-Henrik Jeppesen)

Fanny Hidvégi, employée aujourd'hui[125] par l'association AccessNow à Bruxelles, dans des locaux partagés avec EDRi, avait commencé, selon son profil public sur le réseau social LinkedIn[126], sa carrière professionnelle elle aussi par un stage dans un cabinet d'avocats avant de rejoindre en 2012 une ONG hongroise militant pour la liberté de la presse (*Társaság a Sajtószabadságért*). Joe McNamee, l'un des principaux protagonistes des « discussions » autour du RGPD, a été plus de 10 ans consultant pour *Political Intelligence*, un cabinet qui se décrit lui-même comme un « cabinet de conseils en affaires publiques et lobby[127] », avant de devenir, de septembre 2009 à novembre 2018, directeur exécutif d'EDRi[128].

La proximité socioprofessionnelle de ces acteurs, et surtout de ceux qui travaillent à Bruxelles ou s'y rendent régulièrement pour participer à ces « discussions » à l'issue desquelles des décisions sont prises en matière de politiques publiques, peut aussi être liée à la formation. Les réseaux d'anciens élèves de certaines formations, dont celles du Collège d'Europe, créent des canaux de circulation de l'information parallèles aux circuits officiels. Cela est vrai également pour d'autres formations, et à titre personnel, j'ai[129] pu en faire l'expérience au cours de mes travaux de recherche. Plusieurs anciens élèves de la formation en affaires européennes de l'Institut d'études politiques de Lille, dont je suis diplômé, ont entamé une carrière dans le domaine de la protection des données à caractère personnel. Plusieurs d'entre elles, par exemple, travaillent à la CNIL. Une autre, est à l'AmCham EU[130]. À l'édition 2016 de la conférence CPDP, j'ai recroisé un camarade de promotion avec qui j'avais perdu contact et qui entamait alors lui aussi une thèse sur les politiques publiques de protection des données à caractère personnel. Enfin, un autre ancien élève, de la promotion suivante, a été recruté en 2017 pour être le « *policy*

124 Traduit de l'anglais. Texte original : « I spent many years leading corporate governement affairs teams, so lobbying teams. And […] one thing that drew me to CDT was just the prospect of a completely new challenge, […] looking after not only commercial interests, but the public interest. »

125 En mai 2019.

126 https://be.linkedin.com/in/fannyhidvegi (page consultée le 2 mai 2019).

127 Cette description se trouve dans la balise <meta name = "description" /> de sa page d'accueil, dont le contenu est visible en description du lien menant vers le site political-intelligence dans les moteurs de recherche (code source de la page https://www.political-intelligence.com/fr/ consulté le 2 mai 2019).

128 Informations provenant de son profil public sur le réseau social LinkedIn : https://be.linkedin.com/in/joemcnamee (page consultée le 2 mai 2019).

129 La première personne du singulier a été préférée pour parler d'expériences personnelles en dehors de la recherche.

130 Voir le profil de Maaike Fohrenbach sur le site web de l'AmCham EU http://www.amchameu.eu/about-us/staff (page consultée le 2 mai 2019).

officer » de l'AFCDP à Bruxelles en 2017, après des stages effectués à l'EDPS, à AccessNow, à l'AFCDP et à l'Open Rights Group[131].

Les groupes d'intérêt européens, disposent dans une mesure variable de personnel employé à plein temps pour participer à des « discussions » comme celle qui, entamée en 2009, a abouti en 2012 à la publication de la proposition de RGPD, puis après d'autres « débats » et amendements apportés au texte de la proposition initiale, à son adoption par le Parlement européen et le Conseil en 2016. La capacité à participer à ce « processus » est fonction des ressources – et notamment de ces ressources en personnel que nous venons d'évoquer – des différents groupes d'intérêt ; cela les amène à faire des choix stratégiques et à trier entre les dossiers qu'ils souhaitent suivre :

> « […] avec des moyens limités, nous nous sommes accordés sur le fait que nous devions intervenir sur certains points clefs, et voir si nous pouvions **interjeter une réflexion solide et une *expertise* dans le processus**[132]. » (entretien avec Jens-Henrik Jeppesen, CDT)

La citation ci-dessus rappelle aussi l'importance de ce registre de l'expertise dans la production d'arguments au sein de cette « discussion » sur le RGPD.

Cette notion d'expertise est à distinguer de deux autres notions proches, celles de « légitimité » et celle de « crédibilité ».

La crédibilité est une contrainte pour les acteurs des politiques publiques européennes. Elle a notamment été étudiée dans le cadre de l'étude des politiques monétaires de la Banque centrale européenne[133], où la parole des acteurs des banques centrales peuvent avoir un effet sur les anticipations rationnelles des acteurs financiers, et donc être un outil de politique publique, à condition d'être « crédible » aux yeux de ces derniers (Fontan, 2013).

Cet impératif de crédibilité n'a pas les mêmes enjeux pour les groupes d'intérêt que pour les banques centrales, mais il demeure important car il est le crédit, la confiance épistémique[134]

131 Voir le profil public de Grégoire Delette sur le réseau social LinkedIn : https://fr.linkedin.com/in/gregoire-delette (page consultée le 2 mai 2019).

132 Traduit de l'anglais. Texte original : « […] with limited resources, we agreed that we needed to, you know, intervene on a few key points, and see if we could **interject some solid thinking and *expertise* into the process** ».

133 Le sujet de la « crédibilité » a fait l'objet d'un séminaire de l'IDHES à la Banque de France en 2019, sur la « crédibilité des monnaies » : http://www.idhes.cnrs.fr/la-credibilite-des-monnaies-2/ (page web consultée le 2 mai 2019).

134 Gloria Origgi distingue la confiance relationnelle, qui est la confiance en ce qu'autrui à qui je délègue une part de ma capacité d'agir agisse selon un mode qui préserve mes intérêts, de la confiance épistémique, qui est le crédit que j'accorde aux connaissances d'autrui, indépendamment de mon degré de confiance relationnelle en lui

accordée au discours produit par un acteur. Cette crédibilité transforme un discours quelconque en un discours d'expert. Elle peut s'acquérir et se perdre, et ce qu'un groupe d'intérêts peut dire « crédiblement » ou non est strictement encadré :

> « Je pense qu'il est très important […] pour tout militant d'être pris au sérieux par le plus de parties prenantes possible[135]. » (Entretien avec Walter Hötzendorfer)

Pour donner un exemple du rôle de la contrainte de crédibilité dans la construction de ce qui est énonçable par un acteur, Jens-Henrik Jeppesen, directeur général de l'ONG CDT a expliqué comment il lui a fallu gagner la confiance épistémique des eurodéputés de la commission LIBE au début de leur implantation à Bruxelles. Le fait que son association ait par le passé défendu les mêmes positions que la société Google sur la question du droit au déréférencement avait nuit à leur crédibilité auprès de certains parlementaires. En profitant du contexte des révélations d'Edward Snowden pour dénoncer la surveillance exercée par la NSA avec la complicité de sociétés comme Google, CDT a pu reconstruire sa crédibilité en tant qu'ONG :

> « Nous prenons des positions en fonction de nos principes et de nos missions. Et ils ont pu voir cela, pour en revenir à la discussion sur la surveillance, avec les révélations d'Edward Snowden. Lorsqu'elles sont sorties, nous avons été le premier groupe d'intérêt général à témoigner devant la Commission des libertés civiles du Parlement européen dans le cadre de son enquête sur la surveillance électronique. Et ils ont constaté, de par notre témoignage et les documents que nous avons soumis, que nos positions étaient fondées sur des principes[136]. » (entretien avec Jens-Henrik Jeppesen)

L'expertise n'est pas n'importe quel discours. L'expert est doté de compétences spécifiques. Il est, pour reprendre les termes de Corinne Delmas, « rendu habile par l'expérience » (Delmas, 2011, p. 11), « expérience » qui lui permet de se spécialiser, de détenir des compétences et connaissances spécifiques qu'il peut partager en réponse à une demande sociale et mettre au service d'une prise de décision perçue comme de meilleure qualité. L'expertise en tant que savoir a une vocation pratique (Delmas, 2011, p. 16). Un lobbyiste interrogé en entretien a ainsi décrit une stratégie consistant à faire remonter depuis les entreprises

(Origgi, 2004, 2013).

135 Traduit de l'anglais. Texte original : « I think it is very important […] for any activist that one should try to be taken seriously by as many parties involved as possible. »

136 Traduit de l'anglais. Texte original : « We take positions based on our principles and our mission. And one way they saw that was, back to the surveillance discussion, the Edward Snowden revelations. When they came out, we were the first public interest group to give testimony to the European Parliament's Civil Liberties Committee inquiry on electronic surveillance. And they could see from our testimony or the materials that we submitted that our views were principle-based. »

et associations membres de sa fédération d'associations des exemples se voulant concrets afin de consolider leurs prétentions au discours d'expert ancré dans cette expérience pratique : « évidemment nous devions apporter des exemples[137] » (entretien Euro5).

La crédibilité d'un expert est donc une forme de capital social qui offre aux discours qu'il produit sur un sujet spécifique la reconnaissance des ces qualités d'expertise, si bien que le destinataire de ce discours peut y porter du « crédit », lui faire « confiance ». Dans l'exemple de CDT, une ONG active depuis longtemps aux États-Unis mais n'ayant ouvert de bureaux à Bruxelles que depuis 2013, ce capital de crédibilité était à construire, à commencer par la confiance, puisqu'en adoptant des positions proches de celles de Google au sujet du droit au déréférencement, CDT a d'abord été soupçonnée de ne faire que reproduire – sous couvert d'une identité associative militante de façade – les discours dictés par de grandes entreprises du numérique, et donc de ne pas être digne de confiance, puisque mentant sur son identité même. La confiance produite par l'expertise est *épistémique* en ce qu'elle porte sur la qualité des connaissances acquises par l'expérience de l'expert ; comme nous venons de le voir, c'est aussi une confiance *relationnelle* en ce qu'elle rassure sur l'absence de volonté de manipulation en mettant en scène une forme de neutralité axiologique ou, à défaut, de transparence sur les motifs de la participation à la « discussion ».

Un autre exemple du rôle de la « crédibilité » est qu'une « ONG » – c'est-à-dire un « groupe d'intérêt public » dans le vocabulaire des acteurs du terrain – ne peut « crédiblement » parler au nom de petites et moyennes d'entreprise. Elle ne peut pas prétendre à leur propre domaine d'expertise :

> « Différents groupes sont considérés comme crédibles de différentes manières. Si nous disons : "ceci est ridiculement contre-productif pour les petites entreprises", nous disposons d'un certain degré de crédibilité. Si les petites entreprises ne disent pas que cette chose est mauvaise pour elles, alors elles seront crues. […] C'est ainsi que parfois, en tant qu'ONG, vous n'avez nulle part où aller mais vous devez avoir le lobby pertinent de votre côté[138]. » (Entretien avec Joe McNamee)

Construire sa crédibilité est une nécessité. Discréditer l'expertise d'un acteur rival est une stratégie fréquemment mise en œuvre. Par exemple, Joe McNamee, d'EDRi, a exposé en entretien des arguments pour remettre en cause la prétention à la crédibilité et à la représentativité des groupes d'intérêt industriels :

137 Traduction de l'auteur. Texte original : « obviously we had to bring examples. »

138 Traduit de l'anglais. Texte original : « Different groups are perceived as being credible in different ways. If we as civil society go along and say: this is ridiculously unhelpful for small businesses, we have a certain degree of credibility on that. If the small businesses are not saying this is bad for them, then they will be believed. That's where, sometimes, as an NGO, you just have nowhere to go, but you have to have the relevant lobby on your side. »

> « Je nourris quelque crainte à me fier à la bulle bruxelloise des affaires comme représentative des entreprises en général. Parce que je ne pense pas qu'elle le soit.[139] » (Entretien avec Joe McNamee)

Les acteurs des autorités de protection des données, qui, en tant qu'autorité publique, disposent auprès d'autres acteurs institutionnels d'une forme de présomption d'expertise (Grossman et Saurugger, 2012), ont été un allié utile pour les groupes d'intérêt public – autrement dit, les ONG – de la coalition des défenseurs de la vie privée. L'anecdote suivante, rapportée dans un entretien, montre ainsi comment le vice-commissaire à la protection des données irlandais a permis à la coalition des défenseurs de la vie privée de reprendre le dessus sur des acteurs de la coalition industrielle, au cours d'une réunion. Son intervention a efficacement discrédité l'acteur rival, qui n'a plus été en mesure de reprendre la parole au cours de la réunion, ayant perdu sa ressource de crédibilité :

> « Un jour, [les lobbyistes] travaillaient sur un règlement concernant le fromage, et le lendemain ils travaillaient tout d'un coup sur le RGPD. Et ils ont regardé le règlement de protection des données et se sont dit : oh ! Nous pouvons dépeindre cela comme étant la fin du monde tel que nous le connaissons. Un événement a ensuite été organisé au Parlement européen, en décembre 2013, je crois, par un eurodéputé français. Il y a eu une intervention d'une personne qui venait, je pense, de la Fédération Bancaire Européenne. Je crois qu'il y avait deux associations financières. En tout cas, cette personne s'est levée et a dit qu'il lui était impossible de respecter les règles exigeant ceci ou cela. Et Gary Davis, qui était le commissaire adjoint irlandais à la protection des données de l'époque et qui travaille aujourd'hui pour Apple, a gentiment pris le micro de l'eurodéputé en charge, et a demandé : "Vous êtes sûr ? Parce que selon la directive existante, vous avez l'obligation de faire ceci, de faire cela, et tout le reste. Donc, vous êtes en train de dire que vous ne respectez pas ces règles actuellement ? Que vous ne pouvez pas appliquer, et n'appliquerez pas, des règles en vigueur en droit européen ?" Le représentant a fait le choix de ne plus rien dire. Ce type d'intervention est très efficace. […] Mais seule une autorité de protection des données peut faire ce qu'a fait Davis et juste couper court à une telle argumentation en disant que ça suffit, ça n'est pas vrai, arrêtez de mentir, fermez-la[140]. » (Entretien avec Joe McNamee)

139 Traduit de l'anglais. Texte original : « I would be fearful of relying on the Brussels business bubble as representative of business. Because I don't think it is. »

140 Traduit de l'anglais. Texte original : « So one day [lobbyists] were working on regulation for cheese, and the next day they were working on the GDPR. And they looked at the data protection regulation and thought: oh! We can portray this as the end of the world as we know it. And there was one event in the European Parliament in December of 2013, I think, organised by a French EPP member. And there was an intervention by, I think, it was the European Banking Federation… I think there were two financial associations there… Anyway, the guy stood up and said: look, it's absolutely impossible for us to comply with rules that require this and that and the other.

Anna Walkowiak, de la Fondation Panoptykon, souligna elle aussi en entretien le rôle important que les autorités de protection des données, globalement alliées au réseau d'ONG dont elle faisait partie en tant qu'employée de cette fondation, pouvait jouer en termes d'apport d'expertise et de crédibilité, du fait de leur position institutionnelle spécifique dans le champ du sous-système de politiques publiques de l'UE de protection des données à caractère personnel :

> « Ils ont plus d'experts. Des experts qui peuvent participer à différents événements, rassembler plus d'information… ils sont effectivement très importants[141]. » (entretien avec Anna Walkowiak)

Au-delà du processus d'adoption formel d'un acte législatif par les institutions de l'Union européenne, la « discussion » (pour reprendre le terme employé par les enquêtés) sur l'adoption de cet acte commence bien en amont de la proposition formelle publiée par la Commission européenne. Dans le cas du règlement REACH[142] sur la réglementation des substances chimiques commercialisables dans l'UE, son adoption date de 2006, la proposition initiale de la Commission européenne de 2003… mais les premières discussions remontaient à 1998, lorsque le Conseil commanda à la Commission un rapport sur le sujet. Dès 1998/1999, des groupes d'intérêt comme le Conseil européen des fédérations de l'industrie chimique d'un côté, et le Bureau européen des unions de consommateurs (BEUC) de l'autre prirent position et organisèrent des conférences et autres événements de « discussion » visant à influencer la façon dont le problème public de la production de produits chimiques serait cadré en amont de la rédaction de la proposition de règlement ou de directive (Grossman et Saurugger, 2012, p. 220). Dans le cas de notre étude sur l'adoption du RGPD, la période de « discussions » pendant lesquels des groupes d'intérêt ont engagé un dialogue (« *to engage* ») entre eux et avec des acteurs de la Commission, du Parlement européen et du Conseil, a duré de mai 2009 à avril 2016.

Après avoir présenté le RGPD, identifié le sous-système de politiques publiques de l'UE dans lequel celui-ci a été produit, vu le rôle du réseau transgouvernemental des autorités de

---

And Gary Davis, who was the assistant Irish data protection commissioner at the time, and now works for Apple, gently took the microphone from the MEP in charge and he said: are you sure? Because under the existing Directive, you have an obligation to do this, you have an obligation to that, and you have an obligation to do the other. So are you saying that you're not complying with these rules now? Are you saying that you can't and won't comply with rules that are existing in European law? And the representative chose not to speak again. That kind of intervention is very effective. […] But only a DPA could authoritatively do what Davis did, and just shut down that line completely, saying it's not true, stop lying, shut up. »

141 Traduit de l'anglais. Texte original : « They've got more experts. Experts who are able to participate in different events, gather more information… so they are indeed very important. »

142 Règlement 1907/2006/CE du Parlement européen et du Conseil du 18 décembre 2006 concernant l'enregistrement, l'évaluation et l'autorisation des substances chimiques, ainsi que les restrictions applicables à ces substances (REACH).

protection des données et étudié le rôle joué par la crédibilité et l'expertise dans la production du discours des acteurs dans les arènes de ce sous-système, il est temps d'identifier les différentes coalitions de cause qui se sont opposées sur la rédaction de ce règlement, puis d'étudier leurs discours et stratégies argumentatives en utilisant la méthodologie présentée en chapitre 1.

4.2. Identification des coalitions de cause

Un grand nombre d'acteurs ont participé à cette « discussion » entre 2009 et 2016. Ils ont noué des relations soit d'alliance, soit de rivalité, dans la volonté de contrôler le résultat final. Conformément aux hypothèses du modèle de l'ACF, des coalitions de cause se sont ainsi structurées le long de lignes de clivage idéologiques, les groupes d'intérêt et acteurs individuels les composant nouant des alliances en fonction de leurs convictions politiques[143].

Ces acteurs ne se sont pas forcément alliés sur la base du noyau fondamental (« *deep core* ») de leurs croyances, mais se sont rejoints au moins sur un consensus autour du noyau superficiel quant aux objectifs de politique publique à atteindre dans le sous-système où ils agissent (le « *policy core* »). Paul Sabatier lui-même a d'ailleurs nuancé son hypothèse selon laquelle les groupes d'intérêt se regroupaient nécessairement sur la base d'un noyau superficiel (« *policy core* ») en montrant qu'il pouvait exister des rivalités matérielles même entre groupes d'intérêt dirigés par un idéal d'intérêt collectif (« *purposive groupes* »), par exemple pour augmenter sa visibilité et augmenter son nombre d'adhérents (Sabatier, 1998, p. 116). Surtout, nous verrons que ce sont finalement plutôt les mesures concrètes, ces « mesures secondaires » de Paul Sabatier, qui n'ont pourtant rien de secondaire, et qu'il faut soit soutenir soit combattre, qui ont structuré des coalitions de cause, de façon finalement assez pragmatique. Par exemple : comment doit être rédigée la définition juridique de la notion de « donnée à caractère personnel » ? Faut-il inclure une définition du « consentement » qui oblige à ce que ce consentement soit « explicite[144] » ? Deux acteurs soutenant la même rédaction de ces définitions peuvent s'allier même si le noyau fondamental, ou même superficiel, de leurs convictions sont différents.

Nous partageons tout de même le constat que malgré tout, les controverses autour de ces « aspects secondaires » (« *secundary aspects* »), c'est-à-dire les mesures concrètes à adopter, la formulation précise des textes à adopter, sur lesquels se concentre l'attention des acteurs d'une coalition de cause, sont en réalité bien souvent révélatrices de désaccords de fond qui se situent au moins au niveau du noyau superficiel (« *policy core* ») voire du niveau le plus profond de convictions politiques (« *deep core* ») (Sabatier, 1998, p. 117). Avec ces nuances en tête permettant d'adopter les bonnes précautions méthodologiques et de ne pas passer à côté de débats idéologiques qui, au motif qu'ils ne sont pas un facteur de remise en cause de l'unité d'une coalition de cause donnée, n'en sont pas moins révélateurs de référentiels politiques à prendre en

143 Cf. section 1.1.
144 Cf. section 4.3.3.

compte dans le travail, nous pouvons entamer la cartographie de ces derniers au sein du sous-système de politique publique étudié.

Une première façon d'identifier les coalitions de cause est de répertorier les acteurs ayant défendu des amendements identiques.

Lobbyplag était un projet né de la coopération entre la société OpenDataCity et l'association Europe v Facebook. Leur site web, à l'adresse lobbyplag.eu, permet de visualiser des liens entre des amendements au projet de RGPD proposés par des eurodéputés et ceux que des groupes d'intérêt leur ont suggérés. Il permet aussi de visualiser des propositions faites par des ministres au Conseil de l'UE. Les données ayant nourri les graphiques visibles sur le site ont été mises en ligne sur un dépôt Github[145].

Nous avons généré un graphique à partir des fichiers suivants pour visualiser les coalitions de cause ayant cherché à influencer les « discussions » sur le RGPD :

- Une sélection de 4866[146] des 5316 amendements déposés en commission par des parlementaires européens répertoriés dans le dossier dédié à la procédure d'adoption du RGPD (2012-011-COD) et archivés sur le site web Parltrack[147], puis sauvegardés au format JSON sur le répertoire Github du projet Parltrack[148] (fichier amendments.json) ;
- La liste des 1158 propositions d'amendements rédigées par des groupes d'intérêt, extraites à partir des documents répertoriés par le projet Lobbyplag en utilisant des techniques de *scrapping*, et sauvegardées au format JSON[149] (fichier proposals.json) ;
- Une liste de 1975 propositions d'amendements de députés identifiées comme copies à l'identique potentielles de propositions d'amendements formulées par des groupes d'intérêt, et sauvegardées au format JSON[150] (fichier plags.json).

Dans plags.json, certains de ces « plagiats » avaient déjà été validés manuellement par des membres de l'équipe de Lobbyplag comme étant des « plagiats confirmés » d'une proposition d'amendement d'un groupe d'intérêt par un ou plusieurs députés européens signataires de l'amendement[151]. Parmi ceux-ci, nous avons retenu dans notre corpus de propositions copiées celles où le texte de l'amendement et le texte de la proposition formulée par le groupe d'intérêt

145 Ce dépôt est disponible à l'adresse : https://github.com/lobbyplag/ (page consultée le 20 décembre 2019).

146 Les raisons pour lesquelles le nombre d'amendements répertoriés par Lobbyplag est inférieur à celui répertorié par Parltrack ne sont pas indiquées dans la documentation fournie par Lobbyplag sur la page de son dépôt Github (https://github.com/lobbyplag/lobbyplag-data – page consultée le 8 mai 2019).

147 Voir le dossier en ligne sur : http://parltrack.euwiki.org/dossier/2012/0011%28COD%29 (page consultée le 7 mai 2019)

148 Voir le fichier « amendments.json » accessible sur le dépôt Github de Parltrack à l'adresse : https://github.com/lobbyplag/lobbyplag-data/blob/master/data/amendments.json (page consultée le 8 mai 2019).

149 Voir le fichier mis en ligne sur le dépôt Github de Lobbyplag à l'adresse : https://github.com/lobbyplag/lobbyplag-data/blob/master/data/proposals.json (page consultée le 8 mai 2019).

150 Voir le fichier mis en ligne sur le dépôt Github de Lobbyplag à l'adresse : https://github.com/lobbyplag/lobbyplag-data/blob/master/data/plags.json (page consultée le 8 mai 2019).

151 Pour ces amendements, les valeurs des champs « checks » et « verified » sont égales à vrai.

étaient identiques à 95 % ou plus. Nous avons par ailleurs validé automatiquement toutes les paires de proposition de groupes d'intérêt à proposition d'amendement de parlementaire dont les textes étaient identiques à 100 %.

Un script que nous avons rédigé en Python a extrait les données de plag.json, pour générer des tableaux au format CSV qui ont ensuite été retravaillés avec Gephi pour produire ce schéma :

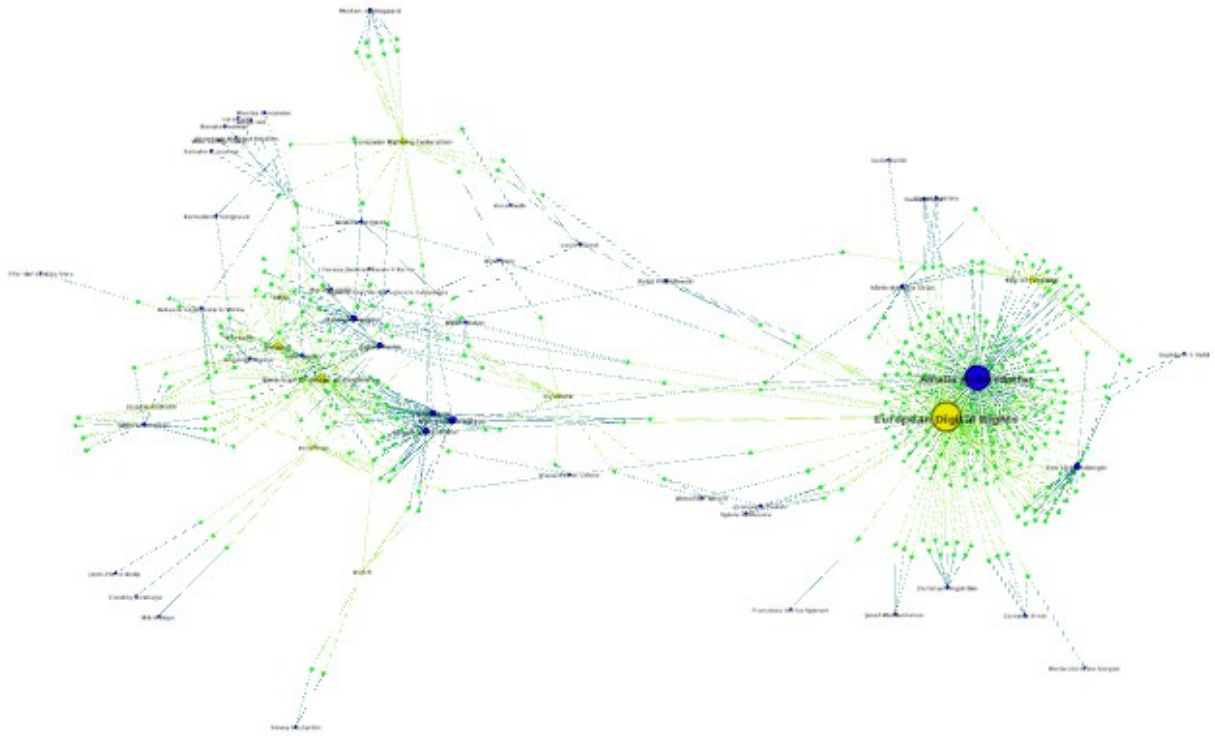


Figure 16 : Cartographie des coalitions de cause avec Gephi sur la base des données fournies par Lobbyplag.

Le graphique ci-dessus fait apparaître une structuration de la controverse autour du RGPD en deux coalitions opposées. Comme nous le verrons, la coalition à gauche sur le graphique est une coalition de cause néolibérale, composée essentiellement d'acteurs issus de groupes d'intérêt industriels. Elle est désignée par les enquêtés comme la « coalition industrielle ». À droite, nous voyons apparaître EDRi et *Bits of Freedom*, qui appartiennent à une coalition d'ONG défendant un paradigme libéral de la « vie privée ». Comme nous l'avons vu dans le chapitre 2, le

libéralisme politique au fondement de cette dernière coalition ne doit pas être confondu avec le néolibéralisme.

La structuration du sous-système de politique publique de protection des données à caractère personnelle de l'UE en deux grandes coalitions rivales est une forme assez classique. De nombreux travaux fondés sur le modèle de l'ACF révèlent eux aussi une structuration en deux coalitions rivales : anglophones contre francophones dans le champ des politiques publiques de l'éducation en Ontario (Mawhinney, 1993), pro-dérégulation et anti-dérégulation à partir de 1970 dans le domaine de la régulation du secteur aérien aux États-Unis d'Amérique (Brown et Stewart, 1993), coalition « pro-développement » et coalition « protectionniste » dans le domaine de la gestion de l'eau en Californie (Munro, 1993), coalition « littéraire » contre coalition des « grands distributeurs » dans la politique de l'édition littéraire (Bergeron, Surel et Valluy, 1998, p. 207-208), « coalition pour l'abstinence » et « coalition pour la réduction des risques » en matière de lutte contre l'addiction aux drogues en Suisse (Kübler, 2002), « coalition pour l'Internet » contre « coalition de l'industrie créative nationale » dans les politiques culturelles du « numérique » des années 2000 en France (Bellon, 2019), ou encore : coalition favorable aux investissements agricoles étrangers « bénéfiques » au nom du développement contre coalition opposée à l'« accaparement des terres » dans le domaine de la politique agricole en Tanzanie (Schlimmer, 2018).

La méthode computationnelle que nous avons utilisée présente un certain nombre de limites dont nous devons impérativement tenir compte. Ces limites sont de trois ordres différents. Tout d'abord, ce n'est pas parce qu'il existe une identité textuelle entre des propositions de certains groupes d'intérêt et de certains parlementaires, que les groupements de propositions obtenus par réseau de propositions identiques recouvrent des réalités perçues par les acteurs. Ensuite, le fichier plags.json de Lobbyplag n'a pu être généré qu'à partir d'un très petit nombre de documents rédigés par des groupes d'intérêt contenant des propositions d'amendements, couvrant seulement 19 groupes d'intérêt pour le fichier proposals.json, parmi lesquels seulement deux associations militantes : EDRi et *Bits of Freedom*. Enfin, il est impossible de savoir quels sont les acteurs ou catégories d'acteurs absents de ce corpus.

Nous avons envisagé de mener une enquête quantitative par questionnaires, comme celle qu'ont effectuée Matthew Zafonte et Paul Sabatier (Zafonte et Sabatier, 1998) sur les politiques publiques de gestion de l'eau dans le delta de la baie de San Francisco, et dans laquelle ils ont demandé à leurs répondants d'identifier les autres acteurs avec lesquels ils étaient en interaction dans ce sous-système de politique publique, et d'indiquer dans quelle mesure ils les percevaient (ou non) comme des alliés.

Mais une telle enquête quantitative ne pouvait réussir qu'à la condition, remplie dans l'exemple que nous venons de citer, de n'avoir qu'un nombre très limité de questions fermées. De plus, la réussite d'une telle démarche sur un objet aussi controversé et récent que l'adoption du RGPD, et au sujet duquel les acteurs impliqués sont, en raison de la thématique même, peu enclins à partager les noms des personnes avec qui ils travaillent, paraissait compromise. Nous avons donc adapté la méthodologie de l'ACF à notre terrain.

Dans le cadre de notre enquête qualitative sur les référentiels des acteurs du sous-système de politique publique de l'UE de protection des données à caractère personnel, nous avons réalisé des entretiens avec des acteurs des « discussions » sur le RGPD. Au cours de ces entretiens qualitatifs et semi-directifs, nous avons intégré des questions sur les personnes avec lesquelles les enquêtés collaboraient ou étaient en rivalité, ainsi que des questions qui visaient à susciter des discours sur leurs convictions, tant au niveau profond (*deep core*) que superficiel (*near-policy core*). Enfin, nous avons demandé quelles mesures concrètes ils ont défendu, les arguments utilisés pour cela, les contre-arguments entendus au sujet de ces dernières, et enfin la réplique typiquement reçue à ces contre-arguments. Un exemple de grille d'entretien est présenté en annexe 7.

Plusieurs extraits d'entretiens retranscrits suggèrent que les acteurs impliqués dans la « discussion » sur le RGPD percevaient le sous-système comme structuré autour d'une rivalité entre d'un côté la coalition des défenseurs de la vie privée regroupée autour des autorités de protection des données et de groupes d'intérêt publics comme EDRi et le BEUC, et, de l'autre, une coalition structurée autour de groupes d'intérêt industriels défendant au nom d'intérêts économiques, de la liberté d'innovation, et de l'impératif de « croissance », un assouplissement des règles de protection des données à caractère personnel.

La citation ci-dessous, extraite d'un entretien avec un lobbyiste travaillant pour l'un des principaux groupes d'intérêt industriels ayant pris part aux « discussions » sur le RGPD, évoque ce qu'il percevait comme la nécessité d'un compromis entre ces deux coalitions, ce qui accrédite l'idée de la structuration de la controverse sur le projet de RGPD autour de cette rivalité :

> « Il ne faut pas être trop EDRi ou trop BEUC, ni trop Microsoft ou trop Google, il faut trouver le bon équilibre[152]. » (Entretien euro5)

La proposition de règlement ePrivacy[153] est un autre instrument juridique de la politique publique de l'UE en matière de protection des données à caractère personnel, plus récent que le

152 Traduit de l'anglais. Texte original : « You can't be too much to EDRi, or BEUC, you can't be too much Microsoft and Google, you have to find the right balance. »

153 Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques») (procédure 2017/03 COD).

RGPD. Kaja Kallas, rapporteure de cette proposition pour la commission Industrie, recherche et énergie (ITRE), a décrit en ces termes, en entretien, les deux coalitions qu'elle pouvait observer depuis sa position dans la « discussion » :

> « Je dirais que les parties prenantes qui nous ont rencontrés [étaient réparties en plusieurs catégories :] d'une part il y avait des personnes très préoccupées par la protection de la vie privée et d'autre part des grands acteurs puissants du marché. […] Il y a des parties prenantes très agressives, les éditeurs, […] les publicitaires[154]. » (entretien avec Kaja Kallas)

Les enquêtés de groupes d'intérêt publics, militants, comme EDRi ou la Fondation Panoptykon, s'identifiaient comme faisant partie non pas d'« associations » (« *associations* ») mais d'« organisations non gouvernementales » (« *NGO's* »), qu'ils opposaient aux « lobbies » (« *lobbies* ») ou aux « compagnies » (« *companies* »). Quant aux enquêtés travaillant ou ayant travaillé pour des groupes d'intérêt industriels, ils se décrivaient comme faisant partie d'« associations » (« *associations* ») et non comme travaillant pour des ONG.

Les deux méthodes utilisées ont donc convergé sur la conclusion que le sous-système de politique publique européen de protection des données à caractère personnel a été, pendant le processus d'adoption du RGPD, structuré autour de deux grandes coalitions rivales :

- La coalition industrielle axée sur l'industrie publicitaire et l'industrie du crédit financier, favorable à un assouplissement des règles en matière de protection des données afin de favoriser une innovation technique perçue par ces acteurs comme favorable à la croissance économique en général et à la leur en particulier, mais aussi à l'intérêt des consommateurs désireux de telles innovations et de croissance ;
- La coalition de la « *privacy community* » (ou « *privacy groups*[155] ») centrée sur l'association European Digital Rights (EDRi) et sur le Groupe de travail de l'article 29, favorable à des règles plus contraignantes de protection des données au nom de la protection des droits fondamentaux, et notamment des droits *à la* vie privée et *à la* protection des données à caractère personnel.

Les acteurs de la coalition industrielle étaient pour l'essentiel des entreprises comme Microsoft et Google, et des groupes d'intérêt que Paul Sabatier qualifierait de « matériels », Sabine Saurugger et Emiliano Grossman d'« économiques ». Ces associations se sont notamment

154 Traduit de l'anglais. Texte original : « I would say that the stakeholders who met us [were categorised into] the people who are very concerned about privacy, and also, the power of big players on the market. […] We have very very agressive stakeholders, publishers, […] advertisers. »

155 Selon l'expression de Jens-Henrik Jeppesen en entretien.

regroupées au sein d'une coalition informelle *ad hoc* : l'*Industry Coalition for Data Protection* (ICDP), qui a joué un rôle structurant dans le fonctionnement de cette coalition :

> « Alors évidemment il y avait un partenariat très fort, nous partagions beaucoup des mêmes inquiétudes que nous avons, d'une certaine façon, mises en commun. Nous avions ce regroupement informel, l'ICDP. Je ne sais pas si vous en avez entendu parler. L'Industry Coalition for Data Protection. Il y avait donc beaucoup de travail, beaucoup d'événements conjoints, beaucoup de réunions. […] Je me souviens que nous avions élaboré toute une série de propositions d'amendements dans cette discussion, d'une quarantine de pages, c'était un travail massif[156]. » (entretien Euro5)

Nous avons retrouvé des *position papers* signés par cette coalition dans notre corpus, portant l'en-tête des différentes associations qui, à la date de la signature du papier, faisaient partie de cette coalition informelle :

156 Traduit de l'anglais. Texte original : « So obviously there was a lot of partnership, a lot of the same concerns and messaging that we, you know, put together. We had this informal grouping, which was the ICDP, I don't know if you've heard of them. The Industry Coalition for Data Protection. So a lot of work there, a lot of joint events, a lot of meetings. […] I remember we did a whole series of sort of proposed amendments in this discussion, which was about forty pages, it was a massive amount of work. »

Figure 17 : *En-tête d'un des* position papers *recueillis par le projet Lobbyplag* (Corpus Lobbyplag, ICDP1, 2011*)*

Les principaux membres de l'ICDP en septembre 2012[157] étaient principalement des entreprises du secteur du logiciel, et des entreprises du secteur de la publicité ou ayant des intérêts communs avec le secteur de la publicité, comme le secteur de l'édition numérique.

Du côté de la coalition des défenseurs de la vie privée, nous retrouvons surtout des groupes d'intérêt que Paul Sabatier qualifierait d'« intentionnels » (« *purposive* ») et Emiliano Grossman et Sabine Saurugger de « publics », et dont les adhérents et employés utilisent le terme d'« ONG » pour les désigner. Deux fédérations d'ONG ont joué un rôle central au niveau de l'UE : le BEUC et surtout EDRi. Cette dernière, qui se présente comme l'association de « défense les libertés civiles dans la société de l'information[158] » fédérait en 2012 33 associations,

157 Cf. annexe 8.

158 Traduit de l'anglais. Texte original : « defend civil rights in information society » (voir : https://web.archive.org/web/20121010105347/http://www.edri.org/about, page consultée le 10 mai 2019).

parmi lesquelles la Fondation Panoptykon de Pologne, l'association Imaginons un Internet solidaire française, le chapitre bulgare de l'*Internet Society*, l'*Electronic Frontier Foundation* (EFF) américaine mais disposant d'un bureau à Bruxelles, le Chaos Computer Club allemand ou encore l'association Article 19 britannique[159].

Les autorités de protection des données à caractère personnel ont également été perçues par ces acteurs comme des alliés. Anna Walkowiak, employée de la fondation Panoptykon, interrogée sur qui faisait partie, selon elle, de la « *privacy community* », y intégra les autorités de protection des données :

> « Lorsque je pense [à la *privacy community*], je pense à des ONG et peut-être à des autorités de protection des données[160]. » (entretien avec Anna Walkowiak)

Les autres entretiens menés avec des acteurs d'ONG ont aussi fait ressortir que les autorités de protection des données étaient perçues comme des alliés précieux en raison de leur présomption institutionnelle de crédibilité[161], de positions défendues similaires, et ce même si le caractère administratif et officiel de ces autorités pouvait limiter leur liberté de ton. Rappelons également, comme nous l'avons vu dans la description du mécanisme d'action de groupe introduit par l'article 80 du RGPD[162], que pour Wojciech Wiewiórowski, alors contrôleur européen adjoint de la protection des données, « les organisations de la société civile sont les alliées naturelles des autorités de protection des données[163] ».

D'autres acteurs ont pu rejoindre cette coalition, notamment des parlementaires et assistants parlementaires[164], ou encore certains universitaires, mais ce sont les autorités de protection des données et le réseau d'ONG structuré par EDRi qui en ont constitué le noyau.

Les convictions des acteurs de la coalition des défenseurs de la vie privée ne sont bien entendu pas parfaitement homogènes, et des désaccords ont pu naître sporadiquement, par exemple au sujet du droit au déréférencement, entre CDT et EDRi, la première se montrant assez critique à l'égard du jugement de 2014 de la CJUE qui a placé entre les mains des entreprises exploitant des moteurs de recherche la responsabilité de décider si un contenu devait être retiré de

159 Voir la liste complète datée du 1er novembre 2010, et telle qu'elle était visible au 3 novembre 2012 sur : https://web.archive.org/web/20121103133134/http://www.edri.org/about/members (page consultée le 10 mai 2019).

160 Traduit de l'anglais. Texte original : « When I'm thinking [about the privacy community], I would think about NGO's and maybe DPA's. »

161 Cf. section 4.1.5.

162 Cf. section 4.1.3.

163 Traduit de l'anglais : « Civil society organisations as natural allies of the data protection authorities » (Wiewiórowski, 2018).

164 Ralf Bendrath, proche d'associations membre d'EDRi comme le Chaos Computer Club, était l'assistant parlementaire de Jan Philipp Albrecht, dont la désignation comme rapporteur pour la commission LIBE de la proposition de RGPD a été largement perçu comme une décision favorable à la coalition des défenseurs de la vie privée, dont les deux se revendiquent.

leurs listes de résultat au nom du droit *à la* protection de la vie privée et des données personnelles, ou bien maintenu au nom du droit *à la* liberté d'expression, et la seconde étant favorable au droit au déréférencement au nom du droit *à la* protection des données personnelles :

> « Nous avons une très forte tradition issue du premier amendement. C'est dans notre ADN […]. Et, vous savez, les journalistes, les organisations médiatiques, les journaux […] étaient très critiques au sujet des types de matériaux qui pourraient être déréférencés suite à des décisions sur le droit à l'oubli[165]. » (Entretien avec Jens-Henrik Jeppesen, CDT)

Des divergences ponctuelles de points de vue ont aussi pu avoir lieu entre des membres d'EDRi, mais sans que cela ne donne jamais lieu à des *veto* formels ni que cela ne remette en cause les mécanismes internes de mise en cohérence des positions de ce réseau d'ONG. Au sujet de ce débat sur le droit au déréférencement, Joe McNamee raconta ainsi qu'EFF, qui s'oppose au droit au déréférencement au nom de la liberté d'expression (voir : Tummarello, 2016), adopta une position de retrait dans des discussions en interne.

EDRi a joué un rôle important de centralisation de l'analyse et de la formulation de propositions au cours du processus d'adoption du RGPD :

> « Nous avons développé une analyse centrale. Bien que certains membres n'aient pas fait une analyse identique à la nôtre, ils n'ont pas ressenti le besoin de s'y opposer au sein de l'organisation[166]. » (entretien avec Joe McNamee)

D'autres entretiens ont permis de confirmer la centralité jouée par EDRi pour la coordination à un niveau européen des prises de position et de la formulation de proposition des associations militantes de la coalition des défenseurs de la vie privée. L'enquêtée de la fondation polonaise Panoptykon, membre d'EDRi pendant la « discussion » sur le RGPD, a décrit en entretien la répartition des rôles entre cette ONG et ses associations nationales membres, dans le contexte d'une gouvernance européenne multi-niveaux :

> « Au niveau européen, dans le cadre d'EDRi, nous avons cette conviction que, tous ensemble, nous sommes en mesure de faire plus. Que nous ne connaissons pas si bien que ça Bruxelles. Nous avons le bureau d'EDRi là-bas. Ils sont incroyablement bons à ce qu'ils font. Ils comprennent les circonstances, connaissent du monde, et nous travaillons

165 Traduit de l'anglais. Texte original : « We have a very strong first amendment tradition. It's in our DNA. […] And, you know, journalists, media organisations, newspapers […] were very critical about the types of material that might be delisted as a result of the right to be forgotten decisions. »

166 Traduit de l'anglais. Texte original : « We have developed an analysis centrally. And while some members have not had an identical analysis, they've not felt the need to oppose that within the organisation. »

donc avec eux. Nous aidons à préparer leurs documents, et si vous consultez certains documents, vous y trouverez également notre logo parce que nous avons participé à leur élaboration[167]. » (entretien avec Anna Walkowiak)

Malgré des divergences ponctuelles d'opinions entre acteurs de la coalition des défenseurs de la vie privée sur certains sujets, l'unité de cette coalition de cause n'a donc pas été remise en cause.

La coalition industrielle a eu, de son côté, des contours plus mouvants. Certains acteurs industriels se sont joints à la « discussion » sur des sujets spécifiques, lorsqu'ils ont eu le sentiment qu'ils les concernaient, mais sans forcément se joindre à la coalition que nous avons décrite. Par exemple, sur l'article 83 de la proposition, devenu l'article 89 du RGPD, qui porte sur l'utilisation des données personnelles à des fins de recherche scientifique, la structuration des coalitions de cause est légèrement différente que sur l'ensemble du texte, puisque nous y observons une présence très nettement renforcée d'acteurs de l'industrie pharmaceutique (Rossi et Bigot, 2018). Ces derniers n'ont cependant pas remis en cause les analyses de l'*Industry Coalition for Data Protection*, mais se sont contentées d'y greffer leurs arguments.

Dans quelques cas, certains groupes d'intérêt ont essayé de démontrer la spécificité de *leurs* demandes de dérogation, quitte à renoncer à défendre les intérêts de l'ensemble de la coalition industrielle. Nous trouvons ainsi la trace d'une telle stratégie dans un *position paper* rédigé par ACCIS, une association représentant les intérêts du secteur de l'information sur le crédit :

« Nous pensons que le projet de Règlement doit être amendé afin de préciser que le droit à l'oubli et l'effacement ne s'applique pas aux données à caractère personnel détenues et traitées par les agences de cotation de crédit, étant donné que ces données sont requises pour les objectifs susmentionnés et que le traitement est autorisé sur la base d'intérêts légitimes[168]. » (Corpus Lobbyplag, ACCIS1, 2012, p. 8)

Un autre élément de nuance qui pourrait questionner la stabilité de ces coalitions – mais aussi l'hypothèse du modèle de l'ACF selon laquelle ce sont les croyances partagées qui fondent

167 Traduit de l'anglais. Texte original : « At the European level, as a part of EDRi, we have this belief that, as a whole, we are able to do more. That we don't know Brussels so well. We have the EDRi office there. They're awfully good at their job. They understand the circumstances, they know people, so we are working with them. We are helping to prepare their documents, so if you look at some documents it will have our logo also because we participated in preparing it. »

168 Traduit de l'anglais. Texte original : « We believe the draft Regulation should be amended to clarify that the right to be forgotten and erasure does not apply to personal data held and processed by credit reference agencies as the data is required for the purposes described above and the processing is permissible on the basis of legitimate interests. »

les coalitions – est la capacité d'un nombre conséquent d'acteurs interrogés à faire alliance, le cas échéant, avec des groupes d'intérêt de l'autre coalition. Ainsi, Walter Hötzendorfer, en entretien, évoqua la manière dont, au niveau autrichien, il y a eu une alliance entre son ONG – Epicenter Works – et des compagnies comme des fournisseurs d'accès à internet, pour contester l'application de lois mettant en œuvre sur le plan national la directive 2006/24/CE sur la conservation des données[169] dont la CJUE a constaté à deux reprises l'incompatibilité avec les droits *à la* vie privée et *à la* protection des données à caractère personnel[170] :

> « Parce que nous avons, pour parler franchement, en particulier en ce qui concerne la conservation de données, des intérêts très similaires à ceux des entreprises de télécoms, des fournisseurs de téléphonie mobile. Nous avons donc fait équipe avec eux dans cette bataille. […] Parce qu'ils y avaient un intérêt financier. Et je suis assez convaincu que ces personnes, chez elles, sont aussi personnellement convaincues que la conservation de données est une mauvaise chose et que c'est inutile, et par intuition elles placent cela dans le champ de la vie privée. Et donc c'est exactement ce qui s'est produit : nous avons fait équipe avec l'industrie pour mener une campagne contre la rétention de données[171]. » (Entretien avec Walter Hötzendorfer)

Au cours d'une discussion de panel lors de l'édition 2017 de la conférence CPDP, intitulée « *Towards a European production order?* », Rita Balogh de Google et Joe McNamee d'EDRi se sont associés pour critiquer fortement un projet de règlement européen visant à faciliter l'accès aux preuves électroniques dans le cadre d'enquêtes de police[172], en permettant aux autorités d'un État membre d'accéder à de telles preuves détenues par une personne située dans un autre État membre de l'Union, sans avoir à passer par des procédures de coopération avec ce deuxième État membre. Pour Joe McNamee, un tel projet reviendrait à « abandonner aux entreprises privées, qu'il s'agisse de Google ou d'une minuscule entreprise, la tâche auparavant judiciaire qui consistait à recevoir l'injonction[173] ». Réagissant à la défense par Joe McNamee des

169 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

170 CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12 et CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15.

171 Traduit de l'anglais. Texte original : « Because we have of course, frankly speaking, in particular about data retention, we have very similar interests as the mobile phone companies, the providers, the mobile phone providers. And so we teamed up in that campaign. […] Because they had a financial interest. And I'm quite convinced that the people there personnally, they're also convinced that data retention is a bad thing, and not very useful, and they intuition it into privacy. And so this was exactly what happened, that we teamed up with the industry to campaign against data retention. »

172 Proposition de Règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale. COM (2018) 225 FINAL

173 Traduit de l'anglais. Texte original : « hand over a previously judicial task of receiving the order into the hands of private companies, whether it be Google or a tiny company »
Extrait du discours de Joe McNamee à la conférence CPDP de 2017, disponible en ligne sur Youtube à l'adresse : https://www.youtube.com/watch?v=8z6Cx7qLLHg (page consultée le 10 mai 2019)

intérêts de Google, Paul de Hert, professeur de droit à la Vrije Universiteit Brussel, dit : « Joe, tu as des mots surprenamment élogieux à l'égard de […] Google[174] », et Rita Balogh, de Google, répondit par une litote humoristique à cette remarque en disant : « oui, il est vrai que je suis d'accord avec certaines des choses qu'il a dites[175] ».

Toutefois, plutôt qu'une remise en cause de la structuration du sous-système de politiques publiques de l'UE de la protection des données à caractère personnel, ce dernier exemple nous semble plutôt une illustration de la séparation entre un sous-système de politiques publiques dédié à la protection des données d'une part, et de l'autre, un sous-système de politiques publiques en matière pénale et de surveillance, composé d'acteurs en grande partie différents, et discutant d'instruments juridiques différents, comme en atteste d'ailleurs la distinction entre le RGPD d'une part, et la Directive 2016/680 sur la protection des données dans les domaines JAI d'autre part.

Les deux coalitions de cause rivales qui ont structuré la « discussion » sur le RGPD, entre 2009 et 2016, étant maintenant identifiées, nous pouvons étudier les échanges de discours et d'arguments entre ces deux coalitions autour des principaux points de controverse, en commençant par identifier ces derniers.

4.3. Les principaux points de controverse

4.3.1. Sélection des points de controverse étudiés

Dans le cadre d'un processus législatif, les mesures concrètes qui traduisent les objectifs des coalitions de cause, et qui sont appelées dans le modèle initial de l'ACF des « mesures secondaires » bien qu'elles ne soient en rien « secondaires » au yeux des acteurs concernés, sont des textes. Dans un texte juridique, chaque mot, chaque signe de ponctuation, compte. Ainsi, l'un des amendements combattus par EDRi, dont il sera question dans le sous-chapitre sur les critères de licéité[176], ne changeait textuellement qu'une seule lettre à la proposition de la Commission, mais il modifiait radicalement le sens de la proposition de la Commission.

174 Traduit de l'anglais. Texte original : « Joe, you surprisingly said so many nice words about […] Google »
Extrait du discours de Paul de Hert à la conférence CPDP de 2017, disponible en ligne sur Youtube à l'adresse : https://www.youtube.com/watch?v=8z6Cx7qLLHg (page consultée le 10 mai 2019)

175 Traduit de l'anglais. Texte original : « yes, I do agree with some of the things he said. »
Extrait du discours de Rita Balogh à la conférence CPDP de 2017, disponible en ligne sur Youtube à l'adresse : https://www.youtube.com/watch?v=8z6Cx7qLLHg (page consultée le 10 mai 2019)

176 Cf. section 4.3.3.

La proposition de RGPD comptait 139 considérants et 91 articles, et le RGPD finalement adopté, 173 considérants et 99 articles. Au total, sur la proposition de RGPD, l'équipe du projet Lobbyplag a identifié 1150 unités de dispositions législatives, en incluant les propositions de nouveaux considérants, articles ou paragraphes d'articles contenus dans des amendements déposés par des parlementaires ou proposés par des groupes d'intérêt[177]. À ces données s'ajoutent des milliers de pages de documents du Conseil, montrant les évolutions du texte au fur et à mesure des négociations intergouvernementales[178], ainsi que l'ensemble des *position papers* soumis à la Commission européenne lors des consultations de 2010 et 2011 et qui contiennent des propositions qui, si elles ne sont pas rédigées sous forme d'amendement, auraient pu l'être si elles avaient été rédigées postérieurement à la publication de la proposition de la Commission européenne.

Pour déterminer les principaux sujets de controverse au cours des « discussions » sur l'adoption du RGPD, nous avons d'abord utilisé comme indicateur quantitatif les dispositions de la proposition de RGPD sur lesquelles s'étaient portés le plus grand nombre d'amendements de parlementaires européens et d'amendements rédigés et proposés par des groupes d'intérêt[179].

Certains sujets font l'objet de dispositions éclatées à différents endroits du texte. Il a fallu regrouper les statistiques de certains amendements éparpillés mais portant sur un même sujet. Ainsi le point de savoir dans quelle mesure la Commission devait se voir accorder le droit d'adopter des actes délégués en application du RGPD a été un important élément de controverse, mais qui ne ressort pas dans le tableau en annexe 5. Toutefois, en faisant le total des amendements sur des dispositions mentionnant la possibilité pour la Commission d'adopter des actes délégués, qui sont éclatés sur l'ensemble la proposition de RGPD, nous obtenons le chiffre de 78 amendements déposés en commission par des eurodéputés, et de 15 amendements proposés sur ce sujet par différents groupes d'intérêt, ce qui fait figurer le sujet en bonne place dans la liste des sujets ayant suscité le plus d'amendements. Un autre exemple est qu'il y a par exemple 106 amendements déposés par des parlementaires en commission, et 34 proposés aux parlementaires par des groupes d'intérêt, qui portent sur des dispositions relatives au consentement, ce qui démontre l'intérêt considérable qui a été porté par les acteurs de la controverse à cette question.

La méthode quantitative consistant à dresser la liste des dispositions ayant fait l'objet du plus grand nombre d'amendements proposés a donc des limites, puisque le regroupement de dispositions autour d'un même sujet de controverse transforme complètement ce classement. En outre, il est impossible à partir des seules données dont un extrait est présenté dans l'annexe 5 de savoir quels sont les sujets de controverse autour desquels cela a un sens de grouper des dispositions pour faire des statistiques sur le nombre d'amendements en rapport avec ce sujet. Pour reprendre l'exemple du sujet d'accorder ou non la faculté à la Commission européenne

177 Voir la page : https://lobbyplag.eu/browse (page consultée le 10 mai 2019).

178 Il s'agit au total de 11800 pages de documents du Conseil de l'UE, dont certains n'étaient pas destinés à être communiqués au public, qui ont été mises en ligne par Lobbyplag sur leur site en un seul document PDF.

179 Cf. annexe 5.

d'adopter des actes délégués fondés sur le RGPD, ce n'est qu'en se déplaçant sur le terrain, en assistant aux débats publics avec notamment des fonctionnaires de la Commission lors de conférences, ou en lisant les nombreux *position papers*, et surtout en lisant les documents résumant les positions des différents États membres au sein du Conseil de l'UE, que nous avons vu ce thème émerger, et que nous avons eu l'idée de regrouper les propositions d'amendements portant sur ce sujet au moment de faire des statistiques.

Outre ceux qui ont été sélectionnés parce qu'ils sont l'objet de dispositions qui ont individuellement fait l'objet d'un grand nombre d'amendements, d'autres sujets ont été sélectionnés en raison de la place centrale qu'ils ont occupé dans des discours d'acteurs de notre corpus. Si cette dernière méthode de sélection suppose une part d'interprétation subjective, elle est indispensable pour prendre en compte des sujets qui, même s'ils n'ont pas fait l'objet d'un nombre très important d'amendements, ont eu une place importante dans les controverses sur le terrain.

4.3.2. Quel degré de transfert de compétences à l'Union européenne ?

La proposition initiale de la Commission européenne prévoyait de remplacer la directive 95/46/CE par un règlement, dont nous avons vu qu'il renforçait considérablement l'harmonisation juridique du droit *de la* protection des données à caractère personnel sur le territoire de l'EEE, les règlements étant, au contraire des directives, revêtus d'un effet direct en droit interne. Les mécanismes de cohérence et d'autorité cheffe-de-file, ainsi que la transformation du G29 en CEPD renforcent cette logique de transfert vers l'échelon supranational de compétences auparavant nationales. La présence dans la proposition initiale de la Commission européenne de nombreuses dispositions lui permettant d'adopter des actes délégués visait à renforcer un peu plus cette tendance par le renforcement des pouvoirs de la Commission européenne.

Certains gouvernements nationaux ont exprimé des positions favorables à un transfert de compétences vers l'échelon de l'UE en matière de droit *de la* protection des données, y compris par le biais de l'adoption d'un règlement pour remplacer la directive de 1995. Ce fut par exemple le cas de la délégation luxembourgeoise[180]. Mais cette position est loin d'avoir été partagée sans nuances par l'ensemble des membres du Conseil de l'UE.

La délégation hongroise a émis des « craintes » relatives au choix d'un règlement, craignant que que cet instrument plus contraignant renforce l'obligation de disposer de consensus larges pour l'adopter, et que cela aboutisse *in fine* à un affaiblissement d'ensemble du droit de l'UE *de la* protection des données à caractère personnel[181]. Ces « craintes » ne sont toutefois pas à

180 Voir : Position luxembourgeoise, Conseil de l'UE, 2012, document 9897/12, p. 74.
181 Voir : Position hongroise, Conseil de l'UE, 2012, document 9897/12, p. 79.

interpréter comme un rejet d'une européanisation de cette matière juridique, puisque la position hongroise poursuit en indiquant qu'à l'instar du G29, elle regrette que le RGPD ne couvre pas également, sous la forme d'un règlement, les domaines de ce qui est devenu la directive 2016/680/UE sur la protection des données en matière de police et de justice[182].

La délégation tchèque souhaitait séparer les dispositions applicables au secteur public de la proposition de RGPD, et les confier à une directive[183]. Sans s'opposer de front à l'adoption d'un règlement, les délégations allemande et suédoise ont rejoint la délégation tchèque sur son souhait d'un niveau d'harmonisation moindre pour les règles applicables au secteur public[184]. La position slovène était quant à elle beaucoup plus tranchée, et s'opposait fermement à l'adoption d'un règlement, au nom du « constitutionnalisme, et des principes de subsidiarité et de proportionnalité[185] » (Voir : Position slovène, Conseil de l'UE, 2012, document 9897/12, p. 87). La Belgique aussi exprima des préférences pour une directive[186]. Ces deux derniers pays furent rejoints par un allié de poids : le Royaume-Uni, qui, adoptant une position souverainiste faisant référence aux « traditions nationales », indiquait :

> « Nous sommes d'avis que le règlement général proposé devrait être une directive, afin de donner davantage de flexibilité aux États membres pour mettre en œuvre les mesures. Un règlement permettrait à l'UE d'adopter des règles sans pour autant devoir accorder la considération nécessaire aux traditions et aux pratiques nationales[187]. » (Voir : Position britannique, Conseil de l'UE, 2012, document 9897/12, p. 114)

La délégation belge a également formulé une « réserve générale » concernant l'octroi d'un pouvoir d'adoption d'actes délégués devant préciser le RGPD à la Commission européenne (Position belge, Conseil de l'UE, 2012, document 9897/12, p. 8). La délégation allemande considérait également que les « habilitations données à la Commission pour adopter des actes délégués et des mesures d'exécution doivent être clairement réduites[188] », comme d'ailleurs la délégation française[189], la délégation suédoise[190] et la délégation britannique[191].

---

182 *Idem*

183 Voir : Position tchèque, Conseil de l'UE, 2012, document 9897/12, p. 12.

184 Voir : Position allemande, Conseil de l'UE, 2012, document 9897/12, p. 25, et : Position suédoise, Conseil de l'UE, 2012, document 9897/12, p. 106.

185 Traduction de l'auteur. Texte original : « constitutionalism, principles of subsidiarity and proportionality. »

186 Voir : Position belge, Conseil de l'EU, 2012, document 9897/12 REV 1, p. 3.

187 Traduit de l'anglais. Texte original : « We are of the view that the proposed general Regulation should be a Directive in order to provide greater member state flexibility to implement the measures – a Regulation would allow the EU to prescribe rules without necessarily giving due regard to national tradition and practice. »

188 Traduction de l'auteur. Texte original : « Die Ermächtigungen zum Erlass delegierter Rechtsakte und zu Durchführungsbestimmungen durch die Kommission müssen deutlich reduziert werden. » (Position allemande, Conseil de l'UE, 2012, document 9897/12, p. 26).

189 Voir : Position française, Conseil de l'UE, 2012, document 9897/12, p. 55.

190 Voir : Position suédoise, Conseil de l'UE, 2012, document 9897/12, p. 106.

191 Voir : Position britannique, Conseil de l'UE, 2012, document 9897/12, p. 114.

Souhaitant se prémunir d'un trop fort transfert de compétences vers l'échelon de l'UE et afin de protéger l'indépendance des autorités de protection des données, certains États membres ont, tout comme, comme nous le verrons, le Parlement européen, formulé des réserves à l'égard de dispositions dans la proposition de RGPD de la Commission européenne qui conféraient à cette dernière des pouvoirs importants dans le fonctionnement interne du CEPD, qui devait remplacer le G29. Ainsi, selon la position britannique :

> « Nous défendons avec ferveur le principe d'indépendance des autorités de supervision nationales, et rejetons sans équivoque toute tentative de diluer leurs pouvoirs indépendants de décision. À cet égard, nous considérons que la Commission doit reconnaître l'indépendance des autorités de supervision nationales.
> L'indépendance, par définition, ne peut être partielle, et le pouvoir de la Commission d'essentiellement rejeter la décision d'une autorité de supervision risque d'affaiblir ce principe qui est une pierre angulaire de la législation sur la protection des données[192]. »
> (Position britannique, Conseil de l'UE, 2013, document 7105/4/13 REV 4 EN, p. 188)

La délégation française s'opposait, au nom de la position de son parlement national, au transfert de compétences supplémentaires au G29[193]. Elle était en outre peu convaincue par la proposition d'instauration d'un système d'autorité cheffe-de-file, au nom de craintes de phénomènes de « forum shopping », c'est-à-dire de choix par les entreprises de s'installer dans les pays aux autorités les plus faibles, ou les plus complaisantes (Position française, Conseil de l'UE, 2012, document 9897/12, p. 56).

Ainsi, sans qu'il n'y ait d'unanimité sur cette question, nous pouvons dire qu'il existait dans l'ensemble de fortes réticences de la part d'États membres détenant une part importante des droits de vote au Conseil de l'UE, aux dispositions de la proposition de RGPD de la Commission qui visaient à renforcer le transfert de compétences vers l'échelon européen en matière de protection des données à caractère personnel. Ces réserves étaient toutefois motivées plus par des préférences générales, dans tous les domaines de l'action publique, à freiner les transferts de compétence vers l'Union, que par des convictions relevant de la protection des données personnelles et/ou de la vie privée.

À l'inverse, la coalition industrielle a vu d'un œil très favorable ce transfert de compétences, et notamment, le choix d'un règlement comme instrument juridique de la réforme

192 Traduit de l'anglais. Texte original : « We strongly support the principle of the independence of national supervisory authorities and resist, unequivocally, any attempts to dilute their independent decision-making powers. In this regard, we consider that the Commission must recognise the independence of national supervisory authorities.
Independence, by definition cannot be partial and the power of the Commission in the proposals to essentially overturn the decision of a supervisory authority risk undermining this principle, which is a cornerstone of data protection legislation. »

193 Voir : Position française, Conseil de l'UE, 2012, document 9897/12, p. 55.

de la directive de 1995. Pour Razvan Antemir, en entretien, le renforcement de l'harmonisation juridique au niveau européen était la demande la plus importante de son groupe d'intérêt.

Dès la consultation de 2009, des associations comme l'IAB Europe[194] et DIGITALEUROPE[195] appelaient à une « plus forte harmonisation » :

> « Nous pensons qu'il faudrait se concentrer sur la recherche d'une meilleure harmonisation, d'une meilleure mise en œuvre et d'une supervision [*enforcement*] plus efficace, et aller vers un système davantage basé sur les résultats [*outcome based*], plutôt que de simplement se concentrer sur les entrées [*inputs*][196]. » (Consultation de 2009, DIGITALEUROPE1, 2009)

Les choix d'un règlement pour remplacer une directive, ainsi que la création de mécanisme de cohérence et le principe d'une autorité cheffe-de-file ont été perçus par les acteurs de la coalition industrielle comme leur étant favorable, car source d'une réduction de la complexité juridique et donc des coûts de conformité au droit *de la* protection des données à caractère personnel :

> « La législation proposée contient des améliorations bienvenues, cruciales pour rendre ce règlement effectif et efficace. Tout d'abord, nous soutenons l'objectif de la Commission européenne de renforcer le marché unique en renforçant l'harmonisation des règles de protection des données à travers les 27 États-membres. L'introduction d'un concept de guichet unique pour les questions de protection des données non seulement augmentera la sécurité juridique mais allégera également le fardeau administratif, et incitera les autorités de protection des données à progresser vers un modèle de reconnaissance mutuelle[197]. » (Corpus Lobbyplag, DIGITALEUROPE1, p.1)

> « Nous soutenons l'objectif de la proposition de parvenir à une harmonisation accrue allant dans la direction d'un Marché unique numérique pour l'Europe. […] Nous saluons aussi le concept d'autorité unique de protection des données fondé sur l' "établissement principal" d'une entreprise, parfois désigné par le terme de "guichet unique", pour la

194 Voir : iab_europe_en.pdf (consultation de 2009).
195 Voir : digital_europe_en.pdf (consultation de 2009).
196 Traduit de l'anglais. Texte original : « We think that the focus should be on achieving more harmonization, better implementation and consistent enforcement, and on moving towards a more outcome-based system, rather than merely focusing on inputs. »
197 Traduit de l'anglais. Texte original : « The proposed legislation contains welcome improvements which are crucial to making this Regulation effective and efficient. First of all, we support the European Commission's goal of enhancing the single market by increasing harmonisation on data protection rules across the 27 Member States. The introduction of the concept of a one stop shop for data protection issues will not only increase legal certainty, but also reduce administrative burdens and create an incentive for DPAs to move to a mutual recognition model. »

conformité. Cela devrait simplifier et fluidifier les relations des entreprises avec les autorités de protection des données[198]. » (Corpus Lobbyplag, BUSINESSEUROPE1, 2012, p. 3)

Toutefois, les acteurs de la coalition industrielle se sont eux aussi inquiétés du pouvoir que la Commission se souhaitait voir confier d'adopter des actes délégués précisant le contenu de certaines dispositions. Pour eux, cela aurait prolongé la durée de l'incertitude quant au contenu final du RGPD, en ajoutant au temps de la procédure législative ordinaire d'adoption du règlement un temps d'adoption de ces nombreux actes délégués et règlements d'exécution. Cherchant à fonder leur argument sur la modalité de l'expertise juridique, ils affirmaient en effet craindre que cela ne porte atteinte à la « sécurité juridique », terme consacré comme étant un principe général du droit depuis 1962[199] :

« Les nombreuses dispositions prévoyant la possibilité d'adopter des actes délégués signifient que les organisations pourraient encore se voir confrontées pendant de nombreuses années après l'adoption du Règlement à l'adoption de nouvelles règles. Cela crée de la confusion sur les droits des personnes concernées. Cela complique également la compréhension par les organisations de traitement des données de leurs obligations. Étant donné que le Règlement prévoit des sanctions substantielles en cas de non-conformité (jusqu'à 2 % du chiffre d'affaires annuel mondial pour certaines infractions), il est impératif que les organisations comprennent clairement leurs obligations[200]. » (Corpus Lobbyplag, AMCHAMEU1, 2013, p. 63)

« Les nombreuses dispositions de réglementation secondaire (délégation et exécution d'actes) réduisent la prévisibilité juridique et menacent de neutraliser l'efficacité des dispositions en compliquant le régime de protection des données[201]. » (Corpus Lobbyplag, BUSINESSEUROPE1, 2012, p. 1)

198 Traduit de l'anglais. Texte original : « We support the aim of the proposal to achieve greater harmonisation towards a Digital Single Market for Europe. […] We also welcome the single Data Protection Authority (DPA) concept based on the "main establishment" of a company principle sometimes referred to as a "one-stop-shop" for compliance. This should simplify and streamline companies‟ relations with data protection authorities. »

199 CJCE 6 avril 1962, « De Geus contre Bosch e.a. », aff. 13-61.

200 Traduit de l'anglais. Texte original : « The many delegated act provisions mean that organisations could face new rules for many years after the Regulation is adopted. This creates confusion about data subjects' rights. It also makes it difficult for organisations processing data to understand their obligations. Because the Regulation includes substantial sanctions for non-compliance (up to 2% of annual worldwide turnover for certain violations), it is critical that organisations understand clearly what their obligations are. »

201 Traduit de l'anglais. Texte original : « The numerous provisions on secondary rulemaking (delegated and implementing acts) undermine legal predictability and risk neutralising the effectiveness of the provisions by complicating the data protection regime. »

Les *position papers* de la coalition des défenseurs de la vie privée n'ont pas accordé beaucoup de place à la question du choix de l'instrument juridique. Le BEUC s'est contenté de « saluer » (« *welcome* ») la proposition de RGPD, et la réforme de la directive de 1995, sans autre forme de précision à ce sujet[202]. L'ONG néerlandaise *Bits of Freedom* est un « pas en avant » (« *a step forwards* » (Copus Lobbyplag, BITSOFFREEDOM1, 2013, p. 1)), là encore sans autre forme de précision sur le choix de l'instrument juridique.

EDRi semblait dans ses *position papers* et propositions d'amendements assez neutre sur le mécanisme du guichet unique, mais a déposé une série d'amendements visant à renforcer les pouvoirs et les moyens des autorités de contrôle pour éviter que le phénomène dit de « forum shopping » :

> « Il existe une tendance des entreprises en ligne multinationales à s'établir dans certains petits États membres de l'Union européenne. Sans mécanisme permettant de garantir que leurs autorités de protection des données ne soient pas, dans de telles circonstances, dépassées par le coût d'une supervision adéquate, de larges disparités de supervision peuvent survenir. Les autorités de protection des données responsables de la supervision de contrôleurs traitant des données à caractère personnel dans plusieurs États membres doivent prendre des mesures appropriées pour coopérer avec leurs homologues d'autres États membres. Dans certains cas, il pourrait ici s'avérer utile d'impliquer le Comité[203]. » (Corpus Lobbyplag, EDRI2, 2012, p. 41)

Comme le BEUC[204], EDRi s'inquiétait par ailleurs des larges pouvoirs que la Commission européenne prévoyait de s'octroyer dans les procédures internes du futur CEPD :

> « La proposition de la Commission donne à la Commission le pouvoir d'exercer une pression significative sur les autorités de protection des données pour qu'elles se conforment à ses recommandations[205]. » (Corpus Lobbyplag, EDRI2, 2012, p. 112)

---

202 Voir le *position paper* du BEUC en date du 27 juillet 2012, disponible en-ligne à l'adresse : https://www.beuc.eu/publications/2012-00531-01-e.pdf (ressource consultée le 13 mai 2019).

203 Traduction de l'auteur. Texte original : « There is a trend for multinational online companies to establish in some smaller EU Member States. Without a mechanism to ensure that these DPAs are not overwhelmed by the cost of providing adequate supervision in such circumstances significant gaps in supervision may occur. DPAs responsible for supervising controllers who process personal data in multiple Member States should take appropriate steps to cooperate with their counterparts in the other Member States. In some cases, it might be useful to involve the Board here. »

204 Voir le *position paper* du BEUC en date du 27 juillet 2012, disponible en-ligne à l'adresse : https://www.beuc.eu/publications/2012-00531-01-e.pdf (ressource consultée le 13 mai 2019).

205 Traduit de l'anglais. Texte original : « The Commission proposal gives the Commission the power to exert significant pressure on DPAs to comply with its recommendations. »

EDRi ne s'est toutefois pas attaqué aussi fortement sur ce dernier point à la proposition de la Commission européenne que le G29 lui-même.

Le G29 a adopté le 23 mars 2012 un avis « sur les propositions de réforme de la Commission européenne » (G29, 2012a), qui commence par l'affirmation du regret du choix de séparer la proposition de RGPD de la proposition de directive devenue la directive 2016/680/UE de protection des données dans les domaines JAI. Le G29 aurait été favorable à un règlement pour l'ensemble de ces domaines, et note que « la directive est décevante en ce qu'elle manque d'ambition par rapport au règlement » (G29, 2012a, p. 5).

Le G29 se disait par ailleurs favorable à l'évolution prévue dans la proposition de RGPD du fonctionnement de la coopération entre autorités nationales de protection des données, et « favorable à la création du concept d'autorité chef de file » (G29, 2012a, p. 20), à condition qu'une telle autorité ne dispose pas d'une compétence exclusive. Le groupe était également favorable à un renforcement de ses compétences et à l'instauration de mécanismes de cohérence.

Dans l'ensemble, les autorités nationales de protection des données étaient donc favorables au renforcement de compétences en matière de protection des données à l'échelon européen. Elles ont toutefois été très critiques sur le rôle que la Commission européenne prévoyait de s'octroyer, tant dans l'adoption d'actes délégués que dans les procédures du CEPD. En effet, le « groupe de travail [a émis] de sérieuses réserves à l'égard de l'étendue du pouvoir conféré à la Commission pour adopter des actes délégués et des actes d'exécution, ce qui est tout particulièrement pertinent au vu du fait qu'il est question d'un droit fondamental » (G29, 2012a, p. 7). Le groupe reprit à son compte l'argument de la coalition industrielle selon laquelle cela « pourrait représenter une insécurité juridique pour les responsables du traitement et les sous-traitants qui espèrent une mise en œuvre rapide » (G29, 2012a, p. 7). Mais leurs objections étaient aussi liées à des réticences à confier à une autorité politique des compétences décisionnaires dans une matière aussi sensible que le droit fondamental *à la* protection des données à caractère personnel, qui ne saurait selon ce groupe être confié qu'à des autorités administratives indépendantes (G29, 2012a, p. 8).

Le G29 demandait également dans cet avis à obtenir son propre secrétariat, indépendant de l'EDPS, soulignant une volonté de renforcer leur réseau transgouvernemental européen sur le plan de la reconnaissance institutionnelle et des moyens octroyés, tout en souhaitant se tenir à distance des institutions de l'Union, y compris de l'EDPS.

La position du G29, qui s'éloignait de la position de certains gouvernements sur le choix du règlement remplaçant une directive, et qui était favorable à une européanisation, rejoignait l'argument de la coalition industrielle sur le risque d'atteinte à la « sécurité juridique » représenté par la nécessité d'adopter des actes délégués, tout en adoptant les mêmes positions que les ONG

sur la volonté de défendre l'indépendance des autorités de contrôle et son autonomie institutionnelle vis-à-vis des autorités politiques de l'UE, dont la Commission.

La position du G29 fut largement reprise par le rapport de la commission LIBE du Parlement européen sur le RGPD. Ce rapport, qui avait été confié au député écologiste allemand Jan Philipp Albrecht, « se félicite que la Commission ait choisi de remplacer la directive 95/46 par un règlement » (Albrecht, 2013, p. 222), et « déplore vivement que la proposition de la Commission ne couvre pas la coopération entre les services répressifs » (Albrecht, 2013, p. 223). En outre : « Le règlement doit également être exhaustif en ce qui concerne la sécurité juridique. Le large recours à des actes délégués et à des actes d'exécution va à l'encontre de cet objectif. Le rapporteur propose donc la suppression d'un certain nombre de dispositions conférant à la Commission le pouvoir d'adopter des actes délégués » (Albrecht, 2013, p. 223). À la place, le rapport explique que les amendements adoptés par la commission LIBE et soumis au vote plénière du Parlement européen précisent certaines dispositions, rendant inutile l'adoption de nombre d'actes délégués, et confie au CEPD[206] le soin de donner des précisions sur les questions restantes. En outre :

> « […] le rapporteur soutient le renforcement des autorités de protection des données en ce qui concerne les pouvoirs d'investigation et les sanctions. La proposition de la Commission était toutefois trop normative. Il propose un système simplifié qui donne davantage de latitude aux autorités de protection des données tout en chargeant le CEPD[207] de veiller à la cohérence de la mise en œuvre » (Albrecht, 2013, p. 226).

Les amendements proposés visaient de fait à supprimer les pouvoirs de la Commission européenne dans les procédures internes au CEPD afin de garantir leur indépendance[208]. EDRi a apporté son soutien à des amendements similaires adoptés par une autre commission du Parlement européen, la commission JURI (Corpus Lobbyplag, EDRI1, 2012).

En définitive, le texte final du RGPD, sur la question du renforcement du transfert de compétences en matière de protection des données à caractère personnel, du choix de l'instrument juridique, et du fonctionnement du réseau transgouvernemental des autorités de protection des données, se rapproche de l'avis du G29 et de la commission LIBE du Parlement européen.

206 NDA : il s'agit de l'EDPB.
207 NDA : il s'agit de l'EDPB.
208 Voir les amendements 162 à 170 du rapport du 21 novembre 2013 de la commission LIBE sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) du rapporteur Jan Philipp Albrecht.

4.3.3. Bases légales, consentement et intérêt légitime

Les dispositions relatives aux bases légales ont été perçues comme fondamentales par les acteurs de la « discussion ». Ces bases légales sont des critères permettant de prouver la licéité d'un traitement. Sans base légale, il est interdit de traiter des données à caractère personnel.

La liste des bases légales permettant de fonder la licéité d'un traitement de données à caractère personnel au sens du droit *de la* protection des données à caractère personnel faisait déjà partie, selon l'interprétation de la CJUE[209], avant même la publication de la proposition de RGPD de la Commission en 2012, des dispositions « claires et inconditionnelles » de la directive de 1995 bénéficiant d'une forme d'effet direct similaire – bien que pas strictement identique – à celui d'un règlement.

Toutefois, si l'article 6 paragraphe 1 de la proposition de la Commission de 2012 ressemble fortement à l'article 7 de la directive de 1995, il contenait, comme nous pouvons le voir en annexe 6, un certain nombre de différences significatives, notamment pour ce qui concerne le recours au consentement ou l'intérêt légitime du responsable du traitement. Cette base légale permettait (et permet toujours) à un responsable du traitement d'échapper à l'obligation de recueillir le consentement de la personne concernée pour collecter et exploiter (« traiter ») des données à son sujet, tout en ouvrant un droit d'opposition pour les personnes concernées, qui fonctionne dans une logique d'*opt-out* là où le fondement du consentement suppose une logique d'*opt-in*.

Selon Joe McNamee, l'un des amendements déposés par des eurodéputés, d'une seule lettre, aurait remis en cause, s'il avait trouvé sa place dans le texte final, l'efficacité de l'intégralité du régime juridique de protection des données à caractère personnel, en permettant d'intégrer la ligne sur l'intérêt légitime aux cas où des données collectées pour une finalité pouvaient être réutilisées à d'autres finalités :

> « Par exemple, le comité IMCO a changé une seule lettre dans un seul article et cela aurait fondamentalement affaibli la législation. […] C'était véritablement l'amendement le plus maléfique [*evil*]. Parce que c'était littéralement une seule lettre[210]. » (entretien avec Joe McNamee)

209 Voir : CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administración del Estado », aff. C-468/10 et C-469/10.

210 Traduction de l'auteur. Texte original : « For example the IMCO Committee changed one letter in one article and this would have fundamentally weakened the legislation. […] That was the most evil amendment. Because it was literally one letter. »

Cette proposition d'amendement était d'autant plus « maléfique » (« *evil* ») pour EDRi que cette ONG proposait même la suppression pure et simple de l'intérêt légitime comme base légale des traitements (Corpus Lobbyplag, EDRI2, 2012, p. 52).

La proposition initiale de la Commission prévoyait, par rapport à la directive de 1995, de supprimer la possibilité de collecter et utiliser des données personnelles pour l'« intérêt légitime » de « tiers ». Cette possibilité fut finalement rétablie[211], suivant la demande forte formulée en ce sens par des acteurs de la coalition industrielle :

> « Le traitement de données à caractère personnel dans l'intérêt légitime de tiers doit être considéré comme licite, dans la mesure où les intérêts ou les droits et libertés des personnes concernées ne sont pas supérieurs. Cette disposition constituait déjà une part importante de la Directive 95/46/CE, et demeure nécessaire, entre autres, à des fins économiques légitimes de crédit ou pour les organismes de recouvrement[212]. » (Corpus Lobbyplag, DIGITALEUROPE2, 2012, p. 27)

Si la faculté de recourir plus facilement au fondement de l'intérêt légitime a été un élément important dans les demandes de la coalition industrielle, c'est cependant autour de la définition du consentement que s'est concentrée une part significative de la controverse. Or, comme nous l'avons vu, le consentement, la faculté offerte aux personnes de faire leurs propres choix sur les données les concernant, sont un élément fondamental de l'architecture juridique construite précédemment sous l'influence du paradigme libéral de la vie privée.

La proposition initiale contenait plusieurs dispositions renforçant les conditions à remplir pour qu'une expression de consentement au traitement de données personnelles soit considérée comme juridiquement valide. Selon la définition proposée, le consentement devait être « toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement » (art. 4 paragraphe 8 de la proposition de RGPD). Ensuite, à l'article 6 paragraphe 1, il était précisé que le consentement ne pouvait être valable que pour « une ou plusieurs finalités spécifiques » (art. 6 paragraphe 1 de la proposition de RGPD). Enfin, un article entier, l'article 7, était – et est toujours dans la version définitive – consacré aux conditions applicables au consentement. Cet article précisait notamment que « la charge de prouver que la personne concernée a consenti au traitement de ses données à

211 Cf. annexe 6.

212 Traduit de l'anglais. Texte original : « The processing of personal data in the legitimate interest of third parties should be deemed lawful, provided that the interests or the rights and freedoms of the data subject are not overriding. Such provision was already a substantial part of Directive 95/46/EC and is still necessary, among others, for legitimate business purposes of credit or collection agencies. »

caractère personnel à des fins déterminées incombe au responsable du traitement », et que « la personne concernée a le droit de retirer son consentement à tout moment » (art. 7 de la proposition de RGPD).

Pour l'ICDP, l'exigence d'une action explicite et spécifique de la part d'une personne pour que celle-ci puisse valablement donner son consentement était contraire aux intérêts même de cette personne, car à force de devoir tout le temps donner (ou refuser) son consentement, cela pourrait risquer de devenir une « routine ». Plutôt que « trop » d'*opt-in*, il faudrait, selon cette coalition de groupes d'intérêt industriels, favoriser des approches prenant en compte le « contexte » (Corpus Lobbyplag, ICDP1, 2011, p. 6). Cet argument fut repris par le FPF, un *think-tank* financé par la coalition industrielle, dans un *position paper* de 2013 sur le consentement (Corpus Lobbyplag, FPF1, 2013), mais aussi par Facebook, pour qui la proposition de la Commission « risque d'inonder les utilisateurs de cases à cocher et d'avertissements qui pourraient altérer et disjoindre de façon disproportionnée son expérience d'utilisation d'Internet[213] » (Corpus Lobbyplag, FACEBOOK2, 2013, p. 19-20).

Pour de nombreux acteurs de la coalition industrielle, comme DIGITALEUROPE, Facebook et Bitkom (une association regroupant des entreprises du numérique en Allemagne) la définition du consentement comme devant être « explicite » était trop contraignante. Elles proposèrent de remplacer ce terme par « sans ambiguïté » (« *unambiguous* », voir : Corpus Lobbyplag, DIGITALEUROPE2, 2012, p. 23 et FACEBOOK2, 2013, p. 21-22 et BITKOM1, 2012, p. 6). Pour Facebook, il fallait supprimer toute référence à un consentement « explicite », ainsi que, dans le considérant 25, au fait qu'« il ne saurait y avoir de consentement tacite ou passif » (considérant 25, proposition de RGPD)[214]. Cette entreprise demandait également à ce qu'il soit possible de refuser l'accès à un service gratuit si une personne ne consent pas à fournir des données à caractère personnel en échange (Corpus Lobbyplag, FACEBOOK2, 2013, p. 21).

En demandant de telles reformulations sur la thématique du consentement, la coalition industrielle souhaitait éviter la raison même pour laquelle des acteurs de la coalition des défenseurs de la vie privée ont salué la proposition initiale : le fait d'éviter que des entreprises puissent se prévaloir d'un consentement « implicite ».

Le G29 a salué dans un avis d'octobre 2012 l'article 7 de la proposition de la Commission, fixant des conditions à la validité du recueil du consentement :

> « L'article 7 de la proposition de règlement apporte également des éléments positifs supplémentaires, en particulier en imposant la charge de la preuve au responsable

213 Traduction de l'auteur. Texte original : « carries the risk of inundating users with tick boxes and warnings and may result in an overly disrupted.
or disjointed internet experience. »

214 Voir : Corpus Lobbyplag, FACEBOOK1, 2013, p. 20.

du traitement, en introduisant des garanties dans le cadre d'une déclaration écrite et en invalidant le consentement lorsqu'il existe un déséquilibre significatif entre la situation de la personne concernée et celle du responsable du traitement. Le groupe de travail se félicite réellement de ces clarifications importantes et du renforcement des droits des particuliers. » (G29, 2012b, p. 8)

Réagissant aux arguments formulés par la coalition industrielle, le G29 poursuivit dans ce même avis en indiquant qu'il « [avait] connaissance de ce que des doutes ont été émis quant au réalisme du mot «explicite» dans le contexte du consentement » (G29, 2012b, p. 8), mais que selon lui, l'emploi de ce mot « constitue une importante clarification du texte, qui est nécessaire pour permettre aux personnes concernées d'exercer véritablement leurs droits, en particulier en ce qui concerne l'internet, où l'usage actuel du consentement est trop souvent abusif. » (G29, 2012b, p. 8).

EDRi proposait d'aller au-delà de la proposition initiale de la Commission, en proposant que soit ajouté, au considérant 33, l'amendement suivant :

Proposition initiale de la Commission européenne	**Texte de l'amendement proposé par EDRi (modifications en gras)[215]**
(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment[216].	(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment. **Consent should also not provide a legal basis for data processing when the data subject**

215 Voir le document EDRI2 du corpus Lobbyplag.
Il est à noter que le considérant qu'EDRi proposait ici d'amender, devenu le considérant 32 du texte définitif du RGPD, s'il ne reprend pas mot pour mot la formulation proposée par cette ONG, en reprend le sens : « Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles. Si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé. » (considérant 32 du RGPD).

216 Version française : « Pour garantir que le consentement soit libre, il y aurait lieu de préciser qu'il ne constitue pas un fondement juridique valable si la personne ne dispose pas d'une véritable liberté de choix et n'est, dès lors, pas en mesure de refuser ou de se rétracter sans subir de préjudice. »

	has no access to different equivalent services. Default settings such as pre-ticked boxes, silence, or the simple use of a service do not imply consent. **Consent can only be obtained for processing that is lawful and thus not excessive in relation to the purpose. Disproportional data processing cannot be legitimised though obtaining consent**[217]**.**

Tableau 10 : *Proposition d'amendement de l'ONG EDRi au sujet du considérant 33 de la proposition initiale de RGPD de la Commission européenne*

En réaction à la proposition d'un amendement en commission du marché intérieur et de la protection des consommateurs (IMCO) du Parlement européen qui visait au contraire à reconnaître la possibilité d'un consentement « implicite » sous certaines conditions, mais qui n'a finalement pas trouvé sa place dans le rapport final de cette commission rédigé par l'eurodéputée du PPE Lara Comi, EDRi s'alarmait en disant que cela aboutirait à « diluer » complètement la notion de consentement (Corpus Lobbyplag, EDRI1, 2012, p. 4).

Pour l'association néerlandaise *Bits of Freedom*, membre d'EDRi, « afin de garantir un consentement en ligne qui ait du sens, il [convenait] de renforcer à la fois les considérants et la définition du consentement[218] » (Corpus Lobbyplag, BITSOFFREEDOM1, 2013, p. 1). Ce renforcement passait pour eux par une formulation renforçant dans le texte l'obligation pour les responsables du traitement d'être capable de « prouver » l'obtention d'un consentement explicite :

217 Traduction en français par l'auteur : « Le consentement ne doit pas non plus fournir de base légale pour le traitement de données lorsque la personne concernée n'a pas accès à d'autres services équivalents. Les paramètres par défaut, tels que les cases pré-cochées, le silence, ou le simple usage d'un service ne doit pas non plus impliquer de consentement.
Le consentement ne peut être obtenu que pour un traitement licite et donc non-excessif eu égard à sa finalité. Le traitement disproportionné de données ne peut être légitimé par l'obtention d'un consentement. »

218 Traduction de l'auteur. Texte original : « In order to ensure meaningful consent online, both the recitals as well as the definition of consent must be strengthened. »

26. Strengthen consent for data processing	Article 4(8)	**Definitions: consent** 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes **by** which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	**Definitions: consent** 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes which **proves that** the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

Figure 18 : *Capture d'écran d'un extrait du document BITSOFFREEDOM1 du corpus Lobbyplag, dans lequel* Bits of Freedom *propose un amendement à la proposition initiale de RGPD de la Commission européenne*

Nous verrons que quelques acteurs de la coalition des défenseurs de la vie privée se sont exprimés de façon sceptique vis-à-vis de la faculté de consentir au traitement de ses données à caractère personnel, voire de façon critique vis-à-vis de l'idée même de droit à l'auto-détermination informationnelle. Cela les a amenés à exiger des conditions particulièrement strictes pour limiter en pratique le recours à cette modalité de légitimation de la collecte et du traitement de données à caractère personnel qui, paradoxalement, ont eu pour effet de renforcer les dispositions juridiques qui traduisent le principe de l'auto-détermination informationnelle dans le RGPD[219].

4.3.4. La définition de la notion de « donnée à caractère personnel »

Un autre point important de controverse a été la définition de la notion juridique de « donnée à caractère personnel ». Le chapitre 6 étant dédié spécifiquement à l'évolution de cette définition dans le temps, et aux controverses définitionnelles qui l'ont entourée, nous ne nous étendrons ici pas longuement sur ce sujet, et ne résumerons que les grandes lignes dont nous ne pouvons faire l'économie pour ensuite comprendre les débats d'ensemble sur le RGPD et les arguments et discours formulés par les acteurs. Cette définition est en effet absolument fondamentale, car c'est d'elle que dépend l'étendue du champ d'application matériel du RGPD[220]. Restreindre, ou au contraire, étendre la définition, aboutissait selon les cas à englober plus ou moins d'inscriptions matérielles – numériques ou non – comme des données à caractère

219 Cf. section 4.6.

220 L'article 2 paragraphe 1 de la proposition initiale disposait : « Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »

personnel, et à étendre ou non à certaines situations le champ d'application matériel du droit *de la* protection des données.

Dans sa proposition initiale, la Commission européenne proposait une réécriture de la notion de « donnée à caractère personnel[221] ». Au lieu de la définir de façon autonome, la nouvelle rédaction proposait de définir cette notion comme étant « toute information se rapportant à une personne concernée », renvoyant ainsi vers une définition plus longue de ce qu'est une « personne concernée », définie comme : « une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (art. 4 paragraphes 1 et 2 de la proposition initiale du RGPD).

Cette proposition ne changeait que bien peu de choses sur le fond, hormis le fait qu'elle précisait désormais de façon explicite le fait qu'une personne physique est réputée « identifiable » dès lors qu'elle l'est « par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement *ou par toute autre personne physique ou morale* » (art. 4 paragraphe 1 de la proposition initiale du RGPD), renforçant ainsi une conception absolue de cette définition par rapport à une interprétation relative.

Nous n'avons d'ailleurs pas trouvé de demandes de la part d'EDRi ou de *Bits of Freedom* de revenir à l'ancienne façon de présenter la définition de « donnée à caractère personnel ». Leur proposition, comme nous le verrons dans le chapitre dédié aux controverses sur cette définition, consistait à rendre explicite le fait qu'une donnée est personnelle même lorsqu'elle ne sert qu'à « distinguer » (« *single out* ») une même personne dans une masse de données sans l'identifier[222].

Plusieurs délégations nationales au Conseil, comme les délégations française[223], slovaque[224] et britannique[225] ont exprimé souhaiter un retour à la définition de 1995, plus claire, et dont les implications jurisprudentielles étaient mieux maîtrisées.

Dès les consultations de 2009 et de 2010, des associations industrielles se sont positionnées pour demander la consécration juridique de nouvelles catégories de données. Ainsi, la *Business Software Alliance* (BSA) écrivait dans sa contribution à la consultation de la Commission de 2010 qu'il fallait définir dans le futur texte de la réforme du droit de l'UE *de la*

221 Cf. section 6.4.1. et annexe 2.
222 Cf. section 6.4.2.
223 Voir : Position française, Conseil de l'UE, 2012, document 9897/12, p. 60.
224 Voir : Position slovaque, Conseil de l'UE, 2012, document 9897/12, p. 95.
225 Voir : Position britannique, Conseil de l'UE, 2012, document 9897/12, p. 117.

protection deux nouvelles catégories de données : les données « anonymes » et les données « pseudonymes » (Consultation de 2010, BSA1, 2011).

Toujours dans ce sens, selon l'ICDP, dont la BSA était membre :

> « Il faut qu'il existe un degré de plausibilité rationnelle [*reasonableness*] et un lien de proximité entre les informations disponibles et l'identification de l'individu en question. L'une des possibilités de traiter ces aspects pourrait consister à introduire une définition harmonisée des données à caractère personnel indirectes ou pseudonymes, pouvant bénéficier d'exigences plus légères de protection, étant donné que le traitement de telles données présente habituellement des risques très bas en termes de vie privée[226]. » (Corpus Lobbyplag, ICDP1, 2011, p. 5)

Après la publication de la proposition de RGPD, de nombreux acteurs de la coalition industrielle ont demandé l'inscription d'une définition des « données pseudonymes », qui dérogeraient à certains principes ou certaines règles applicables aux « données à caractère personnel ». Voici par exemple un amendement proposé en ce sens par l'AmChamEU :

(2) 'personal data' means any information relating to a data subject;	(2) 'personal data' means information relating to a data subject ***that makes identification by the controller reasonably possible;***
	(2a) 'pseudonymous data' means any personal data that has been collected, altered or otherwise processed so that it of itself cannot be attributed to a data subject without the use of additional data which is subject to separate and distinct technical and organisational controls to ensure such non attribution;
	(2b) 'anonymous data' means information that does not relate to a data subject or has been collected, altered or otherwise processed so that it cannot be attributed to a data subject;

226 Traduit de l'anglais. Texte original : « There needs to be a degree of reasonableness and a proximity link between the information available and the identification of the individual in question. One possibility to deal with these aspects could be to introduce a harmonised definition of indirect or pseudonymous personal data that could benefit from lighter data protection requirements as the processing of such type of data usually present very low risks to privacy. »

Figure 19 : *Capture d'écran d'un amendement proposé par l'AmCham EU, dans le document AMCHAMEU1 du corpus Lobbyplag, p. 11*

Pour le FPF, l'introduction d'une définition de la donnée « pseudonyme » devait permettre leur traitement sans le consentement de la personne concernée :

> « Au vu des exigences rigides en matière de consentement et en l'absence de toute clarification additionnelle au sujet de la clause d'intérêt légitime, un nouveau fondement juridique doit être ajouté au RGPD afin **d'autoriser le traitement de données pseudonymisées sans le consentement de la personne concernée**. Cela inciterait les organisations à mettre en œuvre la pseudonymisation[227] […] » (Corpus Lobbyplag, FPF1, 2013, p. 9)

Pour la coalition des défenseurs de la vie privée, le risque avec l'introduction de la notion de « donnée pseudonyme » dans le RGPD, surtout si sa relation avec la notion de donnée à caractère personnel restait incertaine, était qu'elle ne diminue considérablement la portée de ce règlement, en restreignant son application à un nombre de cas bien plus limités que ceux auxquels s'appliquait la directive de 1995. Le G29 proposa donc à son tour une définition du pseudonymat, qui elle, devait servir à créer une obligation supplémentaire pour les responsables du traitement, au lieu d'en faire une possibilité de déroger à la définition juridique des « données à caractère personnel », et, ce faisant, à l'ensemble des obligations du RGPD :

> « Le groupe de travail suggère dès lors d'instaurer une obligation générale d'anonymisation ou de pseudonymisation des données à caractère personnel dans la mesure de ce qui est possible et proportionné par rapport à la finalité du traitement. » (G29, 2012a, p. 12)

C'est également sous cette forme que, selon Jens-Henrik Jeppesen, CDT soutint l'intégration d'une définition de « pseudonymisation » :

> « […] nous l'avons examiné […] comme un outil bien défini et délimité […] de renforcement de la protection de la vie privée, parce qu'il pourrait inciter les entreprises […] à utiliser davantage des données pseudonymisées plutôt que des données à caractère

227 Traduit de l'anglais. Texte original : « Given the stiff requirements for consent and in the absence of additional clarity with respect to the legitimate interest clause, a new legal basis should be added to the GDPR to **authorize the processing of pseudonymized data without data subject consent**. This would incentivize organizations to implement pseudonymization […]. »
Texte mis en gras par l'auteur.

personnel directement identifiables […]. Mais je pense que nous avons communiqué de façon absolument claire sur le fait que les données pseudonymisées demeuraient des données à caractère personnel. Toujours soumises au champ du règlement.[228] » (entretien avec Jens-Henrik Jeppesen)

C'est cette conception de la notion de « pseudonymisation » qui a finalement trouvé sa place dans le texte définitif du RGPD, puisque le texte de sa définition indique clairement que les données « pseudonymes » restent dans le champ des « données à caractère personnel » :

« 5) «pseudonymisation», **le traitement de données à caractère personnel**[229] de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable » (art. 4 du RGPD)

4.3.5. La formule de « l'approche basée sur le risque »

La question des données pseudonymes a été liée, dans l'argumentaire de la coalition industrielle, à un autre thème central des « discussions » sur le RGPD : celui désigné par la formule de l'« approche fondée sur le risque ».

Il est indéniable que le RGPD accorde une place plus importante à la notion de risque que ne le faisait la directive de 1995 (Böröcz, 2016 ; Gellert, 2016 ; Quelle, 2017). Dès la proposition de la Commission, plusieurs dispositions, comme l'article sur l'obligation en cas de « risque élevé » pour les personnes concernées de mener une évaluation d'impact[230], visaient à « implémenter la logique générale de l'évaluation du risque dans le droit de la protection des données[231] » (Böröcz, 2016, p. 468). Comme le rappelle Peter Bernstein (1998) dans son ouvrage sur l'histoire du risque, le risque est un ensemble de techniques permettant de fabriquer des connaissances et de la certitude sur des événements futurs par essence incertains. Le risque s'oppose en fait à cette incertitude, radicale, par l'invention et l'utilisation de méthodes

228 Traduit de l'anglais. Texte original : « […] we looked at it […] as a properly defined, properly delineated […] privacy enhancing tool, because it would incenticise companies […] to make more use of pseudonymised data, rather than directly identifiable personal data […]. But I think we made absolutely clear that pseudonymous data was still personal data. Still within the scope of the regulation. »

229 Texte mis en gras par l'auteur.

230 Article 33 de la proposition initiale de la Commission, devenu l'article 35 dans le texte définitif

231 Texte original : « is intended to implement the general risk assessment logic into data protection law » (Böröcz, 2016, p. 468)

quantitatives, statistiques et probabilistes (Bernstein, 1998 ; Le Breton, 2017). Le risque n'est donc jamais connu *a priori* ; il est une connaissance qui doit se construire par l'application de méthodes spécifiques. Certains des articles du RGPD imposent tout autant qu'ils confient et délègue aux responsables du traitement le soin de faire ce travail de quantification.

L'appel à l'adoption d'une « approche basée sur le risque » (« *risk-based approach* ») se retrouve entre autres dans une part de la littérature académique. Paul Ohm (2010) a par exemple argumenté en faveur de ce que les obligations pesant sur les responsables du traitement soient proportionnelles au risque que ces activités font peser.

Pour les groupes d'intérêt de la coalition industrielle, le discours consistait à utiliser cette formule pour l'opposer à celle, présentée comme étant « dépassée » par l'évolution des techniques informatiques, des traditionnels principes de la protection des données applicables à toutes les situations de traitement de données à caractère personnel, qu'une partie de la littérature académique appelle « l'approche basée sur les droits » (« *rights-based approach* ») (voir : Quelle, 2017).

La position de la coalition industrielle a bien été résumée par Raphaël Gellert :

> « Le postulat de base de cette approche est que les principes clefs traditionnels, au cœur de la législation sur la protection des données (tels que le consentement, la minimisation des données ou encore la limitation des finalités) ne sont pour différentes raisons plus adaptés ni au présent ni à l'avenir des réalités du traitement des données. […] Par exemple, un argument habituel consiste à avancer qu'il est de plus en plus compliqué de mettre en œuvre le consentement. […] Des objections plus fondamentales concernent la limitation des finalités […]. Il est argué que la logique du principe de limitation des finalités est tout simplement diamétralement opposée à celle des algorithmes et du big data. En effet, ce principe nécessite que la collecte et le traitement des données soient limités et liés à un objectif préexistant. À l'inverse, les algorithmes et le big data sont fondés sur la collecte du maximum de données possible, à des fins à définir au fur et à mesure du traitement […]. L'intérêt de l'approche fondée sur les risques est donc de remplacer ces principes fondamentaux par un exercice d'analyse des risques[232]. » (Gellert, 2016, p. 482)

232 Traduit de l'anglais. Texte original : « The basic tenet of this approach is that traditional, so-called core principles of data protection law (such as consent, data minimisation, or purpose limitation) are not suited to the present and upcoming processing reality for a number of reasons. […] For instance, it is usually argued that it is becoming increasingly difficult to implement consent […] More principled objections concern purpose limitation […]. It is argued that the logic of the purpose limitation principle is simply diametrically opposed to that of algorithms and big data. Indeed, it requires that the collection and processing of data be limited and linked to a pre-existing purpose. Algorithms and big data on the other hand are predicated on the collection of as much data as possible for purposes to be determined as the processing unfolds […]. The point of the risk-based approach is therefore to substitute these core principles for a risk-analysis exercise »

En effet, selon un *position paper* de 2013 de DIGITALEUROPE sur l'approche basée sur le risque : « l'approche basée sur le risque évalue le risque inhérent aux opérations et incidents de traitement de données pour déterminer les obligations des responsables du traitement et des sous-traitants[233] » (DIGITALEUROPE, 2013, p. 1).

L'idée d'une l'approche fondée sur le risque fut mobilisée pour légitimer ce qui dans le fond était une demande d'affaiblissement des règles à respecter, voire une remise en cause de certains principes de la protection des données, pour les cas ne représentant qu'un faible risque selon l'évaluation qu'en feraient les responsables du traitement, dont les entreprises de la coalition industrielle. Un courrier envoyé par John Vasallo et Karim Lesina de l'AmCham EU au commissaire européen Jacques Barrot dès avant la consultation de 2009, au moment de la conférence organisée par la DG JLS au sujet de l'avenir du droit *de la* protection des données à caractère personnel, illustre cette position :

> « Le niveau de réidentification de la donnée doit être davantage pris en compte au regard des obligations de conformité [*compliance*] auxquelles ces données sont soumises. Un moyen de gérer ce problème pourrait être d'établir une définition harmonisée des données à caractère personnel indirectes ou pseudonymes, qui pourraient bénéficier **d'exigences plus légères de protection**, étant donné que le traitement de telles données présente habituellement **des risques très bas en termes de vie privée**[234]. » (Courrier de John Vasallo et Karim Lesina, en annexe du document AMCHAMEU1 du corpus de documents de la consultation de 2009, p. 14-21)

L'introduction d'une définition de données « pseudonymes » qui, étant non-nominatives et seulement indirectement identifiantes, feraient peser un moindre risque sur les personnes concernées par rapport à des données directement identifiantes, était donc initialement conçue par la coalition industrielle comme une façon de diminuer leurs obligations au titre du droit *de la* protection des données pour les cas à « faible risque ». C'est aussi ce qu'exprima la FEDMA dans un document envoyé en réponse à la consultation de 2009 de la Commission européenne :

233 Traduction de l'auteur. Texte original : « the risk-based approach assesses the risk inherent in data processing operations and incidents when determining the obligations for data controllers and processors »

234 Traduit de l'anglais. Texte original : « The level of re-identification of the data should be taken more into account with regard to the compliance obligations imposed on such data. One possibility to deal with these aspects could be to introduce a harmonised definition of indirect or pseudonymous personal data that could benefit from **lighter data protection requirements** as the processing of such type of data usually present **very low risks to privacy**. »
Texte mis en gras par l'auteur.

- **Reducing Administrative Burdens for Processing**
    - The rise of the internet and the digitisation of every day processes has greatly increased the number of data processing operations;
    - In order to determine how data should be treated, a data controller must assess whether such data relate to "an identified or identifiable natural person" (which includes the reference to an "identification number"), and whether an individual can be identified from those data and other information which is in the possession of or is likely to come into the possession of the data controller.
    - A change to this rule could be envisaged. The "risk of harm" that could result from the processing of such data should be a key factor when determining conditions and obligations for the processing of the data;
    - In situations where the processing does not pose a risk to the privacy of consumers (or another kind of harm), this should reduce obligations on businesses to register with the data protection authorities; to notify processing; or to collect consent;
    - Such an approach could also be helpful to clarify the debate over IP addresses and when they should be considered personal data;

Figure 20 : *Extrait de la page 5 de la réponse de la FEDMA à la consultation de 2009 de la Commission européenne (document FEDMA1)*

Pour réagir aux arguments de groupes d'intérêt comme DIGITALEUROPE poussant à l'agenda une « approche basée sur le risque » qui viendrait remplacer les principes généraux de protection des données par des règles flexibles dont le degré auquel les entreprises y sont soumises varierait en fonction d'un risque évalué par ces dernières, le G29 a proposé un discours certes favorable à la formule de l'« approche basée sur le risque », mais lui donnant un tout autre contenu (Böröcz, 2016, p. 470 ; Quelle, 2017) :

> « […] le Groupe de travail est d'avis que tous les contrôleurs doivent agir conformément à la Loi, même si cela peut être fait à l'échelle [*in a scalable manner*][235] » (G29, 2013, p. 2)

235 Traduit de l'anglais. Texte original : « […] the Working Party feels that all controllers must act in compliance with the law, though this can be done in a scalable manner ».

Ce point de vue a été confirmé dans une déclaration (« *statement* ») du 30 mai 2014 sur l'« approche basée sur le risque » qui développe sa position sur le sujet. Cette déclaration était une réaction au discours de la coalition industrielle sur ce sujet :

> « […] le Groupe de travail se préoccupe du fait que l'approche fondée sur les risques soit présentée, de plus en plus souvent et à tort, comme une alternative aux droits et principes établis de la protection des données, tant dans le cadre des discussions sur le nouveau cadre juridique de protection des données de l'UE que dans un cadre plus large[236] […] » (G29, 2014b, p. 2)

Nous voyons ici que le G29 a mis au service d'un argument d'autorité la présomption de crédibilité dont nous avons vu que ce réseau transgouvernemental institutionnalisé bénéficiait, pour discréditer le discours de la coalition de cause rivale. À cet argument d'autorité s'ajoutait un argument juridique : l'existence d'un droit ***fondamental*** *à la* protection des données :

> « La protection des données à caractère personnel est un droit fondamental selon l'article 8 de la Charte des droits fondamentaux. Toute opération de traitement, de la collecte à l'exploitation et à la publication, doit respecter ce droit clé[237]. » (G29, 2014b, p. 3)

Les arguments contre la vision de la coalition industrielle de « l'approche fondée sur le risque » développés en entretien par Joe McNamee d'EDRi ont joué sur le même registre de décrédibilisation de son caractère expert, c'est-à-dire fondé sur l'expérience concrète des acteurs dont il se prétend émaner :

> « De notre perspective, si l'on regarde ce qui s'est passé, c'était très clairement un lobby des grandes entreprises [*big business lobby*]. Et l'objectif, stratégiquement, tel qu'il nous est apparu […] était de créer une réglementation suffisamment chaotique pour être exploitable par les plus grandes entreprises tout en étant assez complexe pour être difficile à mettre en œuvre. Pour obtenir un environnement bénéfique pour les grandes entreprises[238]. » (Entretien avec Joe McNamee)

---

236 Traduit de l'anglais. Texte original : « […] the Working Party is concerned that both in relation to discussions on the new EU legal framework for data protection and more widely, the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles […] ».

237 Traduit de l'anglais. Texte original : « Protection of personal data is a fundamental right according to Article 8 of the Charter of Fundamental Rights. Any processing operation, from collection to use and disclosure, should respect this key right. »

238 Traduit de l'anglais. Texte original : « From our perspective, looking at what was happening, it was quite clearly a big business lobby. And the purpose, strategically, as it seemed to us […] was to create legislation which was

En d'autres termes, les groupes d'intérêt industriels qui prétendaient représenter l'ensemble des entreprises concernées par la proposition de RGPD de la Commission, n'auraient été, en produisant et véhiculant leur discours sur leur version de l'approche fondée sur le risque, que les porte-paroles d'une minorité de grandes entreprises qui auraient voulu verrouiller le marché à de petites et moyennes entreprises sous-représentées dans les « discussions » sur le RGPD, de l'aveu de tous les enquêtés interrogés. Cet argument de Joe McNamee d'EDRi porte ainsi atteinte à la confiance épistémique et relationnelle accordable respectivement à ces propos et à leurs auteurs, et donc à la crédibilité, source de légitimité dans les processus législatifs de l'Union[239].

L'argumentaire que nous venons de citer contient en outre des gages d'adhésion d'EDRi – au moins dans les discours – au référentiel global favorable à la croissance économique et à l'innovation. Nous verrons plus tard que l'articulation des arguments de la coalition des défenseurs de la vie privée à ce paradigme néolibéral de la croissance a joué un rôle crucial dans le succès de leurs revendications au cours des « discussions » sur le RGPD[240].

En définitive, c'est la position du G29 qui est reflétée dans le texte définitif du RGPD. En *plus* de l'obligation générale de respecter les principes de la protection des données et les droits des personnes concernées (comme le droit d'accès) dès qu'il y a collecte et utilisation (donc : « traitement ») de données à caractère personnel, un responsable du traitement est désormais obligé d'adopter des mesures supplémentaires lorsque, selon une analyse dont il est lui-même responsable, cela entraîne « un risque élevé pour les droits et libertés des personnes physiques » (art. 35 du RGPD). Il est explicitement écrit qu'il doit prendre en compte ces risques dans la conception des moyens techniques et organisationnels des traitements (art. 25 du RGPD) et adapter le niveau de sécurité des systèmes d'information (art. 32 du RGPD) (voir : Quelle, 2017).

4.3.6. L'encadrement du profilage

Pour Anna Walkowiak, de l'ONG polonaise membre d'EDRi *Fundacja Panoptykon*, l'un des principaux enjeux du RGPD était l'encadrement du profilage[241]. Le profilage désigne un ensemble de techniques consistant à collecter des informations sur les individus puis, en utilisant des techniques statistiques probabilistes, à inférer de nouvelles informations sur ceux-ci en les recoupant avec celles de masses d'autres individus. Ces techniques se sont historiquement développées à des fins de contrôle des populations, et de prévision des comportements. Elles sont

chaotic enough that it would be exploitable by bigger companies, and complex enough for it to be difficult to enforce. So you would have a beneficial environment for big companies. »

239 Cf. section 4.1.5.

240 Cf. section 4.5.

241 Entretien avec Anna Walkowiak.

fortement liées à des techniques de gouvernementalité statistique qui se sont répandues à partir du XIX^{e} siècle. L'ordinateur a très vite été utilisé à des fins de profilage (Vitalis et Mattelart, 2014).

L'actuel article 22 § 1 du RGPD – l'ancien article 20 §1 de la proposition initiale – offre aux personnes physiques le droit « de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire » (art. 22 du RGPD). L'article 20 § 1 initial ne faisait quant à lui pas référence au « profilage », mais à un droit pour une personne « de ne pas être soumise à une mesure produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects personnels propres à cette personne physique ou à analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement » (art. 20 de la proposition de RGPD).

L'article 22 §1 du RGPD est une reformulation de l'article 20 §1 de la proposition qui résulte de l'insertion d'une définition du terme « profilage » à l'article 4 du RGPD. La version initiale de la Commission proposait des mesures d'encadrement et de transparence du profilage à son article 20, mais ne le définissait pas. EDRi fit partie des acteurs qui ont proposé l'insertion d'une définition. Le texte adopté en lecture définitive se rapproche de la proposition d'EDRi :

Proposition d'EDRi[242]	**Définition à l'art. 4 du RGPD**
« 'profiling' means any form of automated processing intended to evaluate**, or generate data about,** aspects relating to natural persons **or** to analyse or predict a natural person's performance at work, economic situation, **location**, health, preferences, reliability, behaviour or personality[243] »	« 'profiling' means any form of automated processing **of personal data consisting of the use of personal data** to evaluate **certain personal** aspects relating to a natural person**, in particular** to analyse or predict **aspects concerning that natural person's** performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, **location** or **movements**[244] »

242 Voir le document EDRi Amendments.pdf du corpus de *position papers* récupéré depuis Lobbyplag.

243 Traduction en français par l'auteur : « 'Profilage', toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer, ou générer des données sur, certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la localisation, la santé, les préférences, la fiabilité, le comportement ou la personnalité. »

244 Version française : « «profilage», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la

Tableau 11 : *Comparaison de la proposition de définition du « profilage » formulée par EDRi en anglais, avec la version en langue anglaise de la définition du « profilage » à l'article 4 du RGPD*

Moyennant une reformulation pour plus de clarté, comme l'inclusion d'une définition du « profilage », les groupes d'intérêt de la coalition des défenseurs de la vie privée étaient favorables au droit énoncé à l'article 20 § 1 de la proposition de RGPD. À l'inverse, plusieurs groupes d'intérêt de la coalition industrielle ont cherché à faire adopter des amendements visant à restreindre considérablement la portée de ce droit, voire à le supprimer.

Facebook a par exemple cherché à convaincre que le profilage pouvait être utile dans de nombreux secteurs de l'activité économique :

> « Les techniques de profilage sont utilisées dans différents secteurs, de la banque à la santé en passant par la vente, et à différentes fins dont la lutte contre la fraude, l'amélioration du service ou le marketing[245]. » (Corpus Lobbyplag, FACEBOOK2, 2013, p. 36)

L'amendement proposé par Facebook consistait à supprimer le paragraphe 1 de l'article 20 de la proposition, et à reformuler le paragraphe suivant, de sorte à supprimer le droit en question, afin de ne pas entraver une telle activité au nom des bénéfices économiques collectifs qui peuvent selon cette entreprise en être retirés.

L'AmCham EU avait rédigé une proposition d'amendement visant à supprimer l'article 20 de la proposition de la Commission européenne pour le remplacer par un court paragraphe :

localisation ou les déplacements de cette personne physique ; »

245 Traduit de l'anglais. Texte d'origine : « Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. »

AmCham EU Amendment

1. ***A data subject*** shall not be subject to a ***decision*** which ***is unfair or discriminatory***, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this ***data subject.***

2. *deleted*

3. *deleted*

4. *deleted*

5. *deleted*

Figure 21 : *Proposition d'amendement à l'article 20 de la proposition de RGPD formulée par l'AmCham EU*

Cette association justifiait sa proposition par le fait que l'article 20 de la proposition initiale risquerait d'interdire tout un ensemble de techniques utilisées dans diverses industries, au lieu de se focaliser sur une interdiction d'abus comme l'usage d'algorithmes de profilage à des fins discriminatoires (Corpus Lobbyplag, AMCHAMEU1, 2012, p. 8). Facebook développa aussi un argumentaire prétendant que l'inclusion d'un droit spécifique à un ensemble de techniques comme le profilage fragiliserait le RGPD, en le rendant moins « technologiquement neutre » (« *technology neutral* »), et donc moins « paré pour le futur » (« *future-proof* ») (Corpus Lobbyplag, FACEBOOK2, 2013, p. 37).

L'article 22 du RGPD est finalement plus proche de la version proposée initialement par la Commission européenne, soutenue par la coalition des défenseurs de la vie privée, que de la position de la coalition industrielle. En particulier, son paragraphe 1 offrant un droit aux personnes physiques de ne pas être soumises à des décisions fondées uniquement sur un traitement automatisé, dont le profilage, a été reformulé, mais maintenu.

Les quelques points de débat présentés dans ce sous-chapitre permettent d'avoir un aperçu des principaux points de clivage entre les deux coalitions de cause structurant le sous-système de politique publique de protection des données de l'UE. Un grand nombre d'autres dispositions du RGPD ont fait l'objet de débats et de propositions d'amendements tirant dans les deux sens, mais en dresser un tableau exhaustif risquerait toutefois d'alourdir inutilement notre propos.

Afin d'augmenter les chances de voir leurs amendements adoptés, et d'influencer le produit du processus d'adoption du RGPD, chaque coalition de cause a développé des arguments, des contre-arguments, et des contre-arguments aux contre-arguments, sur lesquels nous avons interrogé les personnes ayant accepté de répondre à nos demandes d'entretien. L'étude de ces échanges d'arguments a permis de percevoir les référentiels des acteurs impliqués, et de comprendre comment à travers les jeux d'argumentation, ces derniers cherchaient à légitimer les différentes propositions de mesures concrètes qu'ils ont formulé au cours des années de « discussions » sur l'adoption du RGPD.

4.4. L'argument de l'équilibre avec l'objectif d'intérêt général de la croissance économique dans une « économie du savoir »

Les enquêtés interrogés en entretien ont été invités à répondre à une question sur les arguments utilisés par leurs rivaux durant les débats entourant le processus d'adoption du RGPD. Selon Anna Walkowiak, de la fondation Panoptykon, les lobbyistes de la coalition industrielle avaient pour argument principal le fait que la proposition de RGPD coûterait cher, aurait des répercussions économiques négatives, et surtout, mettrait les entreprises européennes dans une position de concurrence défavorable vis-à-vis des entreprises états-uniennes (en particulier les GAFA) qui, elles, seraient soumises une réglementation moins contraignante et, de ce fait, moins coûteuse.

Ces arguments des « lobbies » font référence au référentiel global néolibéral qui s'est imposé dans l'ancien bloc de l'Ouest à partir du début des années 1980, puis au reste du monde à partir de la fin de cette décennie (Hall, 1986 ; Jobert, 1994), jusqu'au point de devenir hégémonique.

Le néolibéralisme est une idéologie favorable à une réduction de l'action de l'État, notamment dans le domaine de l'économie, et ce tant pour des raisons d'efficacité économique que pour des raisons de philosophie morale et politique (Vergara, 2002). En matière économique, ce référentiel est influencé en particulier par les théories économiques de Friedrich Hayek (Hayek, 1944), d'une part, et, d'autre part, par la critique de l'économie keynésienne interventionniste des années 1960 formulée par les économistes dits néoclassiques et par les monétaristes de l'école de Chicago, dont Milton Friedman fut l'un des principaux théoriciens (Friedman, 1960). Les privatisations, la dérégulation, la diminution des prélèvements obligatoires et l'introduction de mécanismes de concurrence « pure et parfaite » (Knight, 1921) pour remplacer l'intervention de l'État ont été le produit de la conversion à ce nouveau référentiel global des élites politiques et économiques occidentales entre les années 1970 et 1990, qui ont alors abandonné l'ancien référentiel global de modernisation keynésienne[246].

246 Cf. section 3.8.

Les discours de la coalition industrielle que nous avons lus ne font néanmoins référence ni aux idées, ni aux propositions concrètes des penseurs néolibéraux de la vie privée, comme Richard Posner et George Stigler, qui remettent en cause le paradigme libéral[247] de la vie privée, et proposent généralement de remplacer le droit actuel *de la* protection des données à caractère personnel par la création de droits de propriété cessibles sur les données à caractère personnel[248].

Comme nous le verrons dans le sous-chapitre dédié à la stabilité du paradigme libéral de la vie privée dans le sous-système de politique publique étudié, dire que l'on souhaite remettre en cause un droit fondamental – et les mesures concrètes qui sont conçues pour en permettre la réalisation – n'est pas chose aisée. Pour reprendre les termes de Joe McNamee, « personne ne veut faire peur aux gens en disant des choses effrayantes[249] ». Aucun acteur des « discussions » sur le RGPD n'a donc publiquement remis en cause, même au nom « d'impératifs économiques » ou de la « nécessité technique », le principe même des droits fondamentaux que la proposition de RGPD visait à renforcer.

Pour ramener dans le débat ces « impératifs économiques », l'argument central, tant selon Joe McNamee que selon un acteur de la coalition industrielle ayant demandé l'anonymat[250], était d'affirmer qu'il fallait trouver un « équilibre » (« *balance* ») entre la protection des libertés fondamentales – dont le droit *à la* protection des données à caractère personnel – et des objectifs d'intérêt général antagonistes mais tout aussi important, au premier rang desquels la croissance économique.

Par exemple, pour l'AmCham EU :

> « [...] le fait que l'information puisse être traitée à des coûts plus réduits et à une plus grande échelle que jamais offre de multiples opportunités à la société, et est en train d'émerger comme moteur clé d'innovation et de croissance. De plus, les nouvelles technologies pourront fournir des solutions soutenables à certains des plus grands défis de la société actuelle, tels que la santé et le changement climatique. **Trouver un équilibre entre la protection des droits fondamentaux à la protection des données et le besoin de rendre possible la croissance économique à travers l'innovation technologique**[251]

247 À ne pas confondre avec néolibéral (voir : Vergara, 2002).
248 Cf. section 2.3.1.
249 Traduit par l'auteur. Texte original : « You don't want to scare people by saying scary things » (entretien avec Joe McNamee).
250 Entretien Euro5.
251 Texte mis en gras par l'auteur.

est l'un des plus importants défis dans le monde numérique d'aujourd'hui[252]. » (Consultation de 2009, AMCHAMEU1, 2009, p. 2)

« Un **bon équilibre**[253] [*right balance*] entre la protection des informations personnelles et la libre circulation des informations, comme inspiré par la Directive 95/46 doit demeurer un élément clé de l'approche globale de protection des données à caractère personnel dans l'Union européenne au bénéfice des citoyens de l'UE[254]. » (Consultation de 2010, AMCHAMEU1, 2011, p. 4)

Microsoft est un autre exemple d'organisation ayant déployé cet argument :

« Nous sommes d'avis que tant l'industrie que les consommateurs peuvent bénéficier de règles claires et harmonisées de protection des données. Mais nous reconnaissons également que les entreprises en ligne, en particulier, nécessitent une flexibilité pour innover et développer de nouvelles solutions en matière de protection de la vie privée. Les amendements que nous proposons **recherchent cet équilibre**[255] [*seek to strike this balance*] en demandant aux organisations de s'engager à mettre en œuvre des protections solides et d'être transparentes et responsables, tout en profitant des nombreux avantages offerts par la technologie d'aujourd'hui.[256] » (Corpus Lobbyplag, MICROSOFT1, 2013, p. 1)

L'argument a convaincu le gouvernement estonien, qui demandait en 2012 au Conseil de l'UE un meilleur « équilibre » entre un objectif de protection des libertés fondamentales, et l'objectif général des politiques du marché interne de croissance économique, auquel, selon les auteurs du document cité, le RGPD doit également être subordonné :

252 Traduit de l'anglais. Texte original : « [...] the fact that information can be processed more cheaply and at a greater scale than ever before also offers multiple opportunities for society, and is emerging as a key driver for innovation and growth. In addition, new technologies will be able to provide sustainable solutions to some of the biggest challenges in today's society such as healthcare and climate change. **Balancing the protection of the fundamental rights to data protection and privacy with the need to enable economic growth through technology innovation** is one of the major challenges in today's digital world. »

253 Texte mis en gras par l'auteur.

254 Traduit de l'anglais. Texte original : « A **right balance** between the protection of personal information and the free flow of information as inspired by Directive 95/46 should remain a key driver of the comprehensive approach on personal data protection in the European Union to the benefit of EU citizens. »

255 Texte mis en gras par l'auteur.

256 Traduit de l'anglais. Texte original : « We believe that industry and consumers can benefit from clear, harmonised data protection rules. But we also recognise that online companies in particular need some flexibility to innovate and to develop new privacy solutions. Our proposed amendments **seek to strike this balance** -- requiring organisations to commit to strong protections and to be transparent and accountable while balancing the many benefits that today's technology can provide. »

> « L'article 1, sous-paragraphe 2, établit la règle selon laquelle le règlement protège les droits et libertés fondamentales des personnes physiques et notamment leur droit à la protection des données à caractère personnel. La libre circulation des données ne doit être ni restreinte ni interdite. Étant donné que l'un des objectifs généraux de la réforme est la **promotion de la croissance économique et de l'innovation**[257], ces idées doivent être désignées comme objectifs du règlement général. Si l'aspect économique était clairement présenté dans les objectifs, il serait plus simple de **trouver un équilibre** [*balance*] **entre les dispositions protégeant les données avec les objectifs du marché interne**[258]. » (Position de l'Estonie, Conseil de l'UE, 2012, document 9897/12, p. 40)

Pour la présidence grecque du Conseil, en 2014, l'insertion d'une définition de la notion de « pseudonymisation » devait aller dans ce sens d'une telle recherche d'« équilibre » :

> « [L'ajout d'une définition de données pseudonymisées] **aidera à trouver le bon équilibre**[259] [*help striking the right balance*] entre la protection des droits et libertés fondamentaux des individus concernés, et le besoin des secteurs public comme privé de traiter de larges quantités de données[260]. » (Position de la présidence, Conseil de l'UE, 2014, document 6762/14, p. 5)

Nous voyons ainsi comment, sans pour autant remettre en cause la légitimité *en principe* d'un droit *à la* vie privée et *à la* protection des données à caractère personnel, des acteurs de la coalition industrielle sont malgré tout parvenus, avec cet argument de l'« équilibre », à mobiliser des arguments de « nécessité » économique d'inspiration néolibérale. Cet argument selon lequel le droit individuel *à la* vie privée, tel qu'il est présenté par le paradigme libéral de la vie privée, doit s'effacer face aux intérêts légitimes du collectif, ou de la communauté, rappelle plus la critique communautariste d'Amitai Etzioni[261] que la conception néolibérale de la « vie privée ». Mais la vision du bien commun défendue par coalition industrielle demeure inspirée par le néolibéralisme.

---

257 Texte mis en gras par l'auteur.

258 Traduit de l'anglais. Texte original : « Art 1 subpar 2 lays down the rule that regulation protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The free movement of data should not be restricted nor prohibited. Since one of the general goals of the reform has been identified as **promotion of economical growth and innovation**, these ideas should be named under the general objectives of the regulation. If the economical dimension is clearly presented in objectives, it would be easier to **balance the data protection provisions with the goals of the internal market**. »
Texte mis en gras par l'auteur.

259 Texte mis en gras par l'auteur.

260 Traduit de l'anglais. Texte original : « [Adding a definition of pseudonymous data] **will help striking the right balance** between the protection of fundamental rights and freedoms of concerned individuals and the need of the public and private sector to process large amounts of data. »

261 Cf. section 2.3.4.

L'idée selon laquelle la croissance économique est une bonne chose, largement partagée dans l'Occident moderne et fondée sur une certaine idée du progrès des conditions matérielles, est aujourd'hui largement partagée tant par le marxisme orthodoxe, le trotskisme, le libéralisme classique, ou encore le néolibéralisme. Il s'agit pourtant bel et bien d'une idée historiquement construite, dans un cadre culturel bien particulier, avant que cette idée ne finisse par devenir hégémonique (Castoriadis, 2006 [1975]). Dans un contexte où l'économie s'est désencastrée du reste des activités sociales (Polányi, 2009 [1944]), la mesure de la croissance par le PIB est devenue progressivement, et notamment par le biais de l'action de l'OCDE, la mesure par excellence de la réussite de toute politique (Schmelzer, 2016). L'hégémonie du modèle de développement par une croissance mesurée quantitativement par le PIB demeure largement inentamée. Cette quête de croissance infinie dans un monde fini où la croissance de la production tend à l'asymptote est une clef importante pour comprendre l'avènement de l'hégémonie du néolibéralisme sur les politiques publiques européennes. En effet, le néolibéralisme promet un programme de réforme censé relancer un cycle d'accumulation de richesses.

Différents travaux portant sur diverses politiques sectorielles de l'UE attestent du caractère de référentiel global des idées néolibérales (Crespy et Ravinet, 2014). Nous le voyons par exemple dans le domaine de la gestion de la crise financière de 2008 par les banques centrales européennes (Fontan, 2013), ou encore dans le domaine des politiques éducatives (Ravinet, 2014), qui sont une déclinaison sectorielle de la stratégie dite de Lisbonne.

Le Conseil européen de Lisbonne a adopté, les 23 et 24 mars 2000, des conclusions qui sont la base programmatique de cette stratégie. La stratégie de Lisbonne, qui n'a pas de valeur juridique contraignante mais revêt une grande importance politique, formule des objectifs politiques de long-terme, sur dix ans, auxquels toute l'action de l'UE est censée se conformer (Conseil européen, 2000).

Ce document commence en exposant un défi : « l'Union européenne se trouve face à un formidable bouleversement induit par la mondialisation et par les défis inhérents à une nouvelle économie fondée sur la connaissance » (Conseil européen, 2000, §1). Nous voyons donc apparaître dans cette citation la formule de « l'économie fondée sur la connaissance ». Plus loin, il est indiqué que « le secteur des services est sous-développé, en particulier dans les domaines des télécommunications et de l'Internet » (Conseil européen, 2000, §4). Il faut donc, poursuit le document, « préparer la transition vers une société et une économie fondées sur la connaissance, au moyen de politiques répondant mieux aux besoins de la société de l'information et de la R&D, ainsi que par l'accélération des réformes structurelles pour renforcer la compétitivité et l'innovation et par l'achèvement du marché intérieur » (Conseil européen, 2000, §5).

La stratégie dite « Europe 2020 » a pris la suite en 2010 de la stratégie de Lisbonne. Sa préface fait directement référence à la crise économique de 2008. Face à cette dernière, la Commission européenne fixa trois priorités :

1. « Une croissance intelligente » ;

2. « Une croissance durable » ;
3. « Une croissance inclusive » (Commission européenne, 2010b, p. 11-12).

La « croissance intelligente » se définit selon ce document de la Commission européenne comme « une économie fondée sur la connaissance[262] » (Commission européenne, 2010b, p. 13). Dans une telle économie, la connaissance et l'innovation sont définis comme le « moteur de notre future croissance » (Commission européenne, 2010b, p. 13). Pour y parvenir, l'une des « initiatives » proposée est une « stratégie numérique pour l'Europe », avec un cadre juridique harmonisé pour le marché numérique unique (« *Digital Single Market* ») (Commission européenne, 2010b, p. 16). Les réflexions déjà entamées depuis 2009 sur la réforme du droit *de la* protection des données à caractère personnel s'inscrivaient pleinement dans le cadre de cette initiative (Karaboga, 2018), qui elle-même est une déclinaison sectorielle d'une stratégie « Europe 2020 » transversale aux différents sous-systèmes de politiques publiques de l'UE.

La formule de « l'économie fondée sur la connaissance » ou de « la société basée sur la connaissance » se retrouve dans plusieurs des *position papers* du corpus.

Ainsi, selon l'AmCham UE, une « société basée sur la connaissance » (« *knowledge-based society* ») est une société dont les individus sont « légitimement » désireux de prospérité, et pas seulement de vie privée. C'est pour cela, selon un *position paper* produit en 2011 par ce groupe d'intérêt, qu'il est impératif d'équilibrer l'objectif de protection des droits fondamentaux de la proposition de RGPD avec l'objectif de rendre compétitif le « marché unique numérique » :

> « Dans une société basée sur les connaissances où "tout Européen est numérique", il est d'importance critique que les règles de protection des données soient interprétées et mises en œuvre de manière respectueuse de l'attente légitime des citoyens européens que l'UE protège tant leur prospérité que leur vie privée. Il ne s'agit pas uniquement de garantir la cohérence du Marché Unique ; il est essentiel de garantir que celui-ci reste compétitif[263]. » (Consultation de 2010, AMCHAMEU1, 2011, p. 4)

262 Notons que la formule de « l'économie basée sur la connaissance » est à distinguer des théories sur le capitalisme informationnel ou cognitif (Castells, 1998 ; Moulier Boutang, 2007), en ce qu'elle constitue moins une analyse scientifique du phénomène qu'un référentiel cohérent d'idées en faveur de ces formes actuelles de capitalisme.

263 Traduit de l'anglais. Texte original : « In a knowledge-based society where 'every European is digital', it is critically important that data protection rules are interpreted and implemented in a way that is respectful of European citizens' legitimate expectation that the EU will protect their prosperity as well as their privacy. This is not just about ensuring the coherence of the Single Market; it is essential to ensuring that the Single Market remains competitive. »

Comme l'AmCham UE, l'ICDP a mobilisé les formules et les mots des stratégies de Lisbonne et Europe 2020 pour formuler un discours présentant leurs propositions comme étant nécessaires pour réaliser l'intérêt général économique de l'Union :

> « Nous invitons la Commission européenne à **équilibrer** [*balance*] judicieusement la protection des droits individuels avec le fonctionnement du Marché Unique. La capacité de la **Société Européenne de l'Information** à générer de l'**innovation** et de la **croissance**, tel qu'envisagé dans l'**Agenda Numérique de la Commission européenne,** dépend de la création de la confiance nécessaire mais également de l'utilisation de tous types de données **au cœur de l'économie numérique**. Des règles trop strictes, statiques et bureaucratiques en matière de protection des données auront un effet négatif sur l'**économie numérique de l'Europe**. Le **Marché Unique**[264] bénéficie d'une concurrence ouverte. Aujourd'hui et à l'avenir, les activités commerciales [*business activities*] basées sur les données sont les instruments essentiels pour permettre une telle concurrence[265]. » (Corpus Lobbyplag, ICDP1, 2011, p. 2)

Nous voyons la même stratégie discursive à l'œuvre dans un communiqué de presse de l'ICDP publié par *European Voice* en 2013, où la proposition de RGPD était présentée comme mettant en péril la croissance et l'emploi en Europe :

> « […] à un moment où l'industrie des technologies de l'information et des communications est l'**un des rares secteurs économiques de l'Europe à continuer de croître,** la proposition de la Commission européenne d'un nouveau règlement de protection des données **menace de bouleverser** [*unravel*] **l'écosystème numérique, mettant en danger des emplois et la croissance** et étouffant potentiellement la capacité de l'Europe à **innover**[266]. » (European Voice et ICDP, 2013)

La même stratégie se retrouve encore dans un *position paper* d'ACCIS :

---

264 Texte mis en gras par l'auteur.

265 Traduction de l'anglais. Texte original : « We urge the European Commission to **balance** in a sensible manner the protection of individual rights with the functioning of the Single Market. The ability of the **European Information Society** to generate **innovation** and **growth**, as envisaged in the **European Commission's Digital Agenda**, depends on creating the necessary trust, but also on the continued use of all kinds of data that are at **the heart of the digital economy**. Overly strict, static and bureaucratic data protection rules will have a detrimental impact on **Europe's digital economy**. The **Single Market** benefits from open competition. Today and in the future data based business activities are the core instruments to allow any such competition to take place. »

266 Traduction de l'anglais. Texte original : « […] at a time when the information and communications technology industry is **one of the few sectors of the European economy that is still growing**, the European Commission's proposal for a new data-protection regulation **threatens to unravel the digital ecosystem**, **putting jobs and growth at risk** and potentially stifling Europe's capacity to **innovate** »

> « […] dans le cas du secteur des bureau de crédits, **des mouvements pouvant restreindre la disponibilité des informations ou la façon dont ces informations peuvent être utilisées pourraient entraîner non seulement un ralentissement du PIB**[267] […] » (Corpus Lobbyplag, ACCIS1, 2012, p. 3)

Pour favoriser la croissance fondée sur « l'économie de la connaissance », le RGPD ne devait pas, à écouter les acteurs de la coalition industrielle, aller à l'encontre de la « réalité technique » (« *technical reality* »), de la « réalité des affaires » (« *business reality* »), ou de l'« innovation » :

> « Une procédure de documentation très détaillée figerait presque immédiatement le cliché **dépassé** d'une réalité en évolution constante, caractérisée par des modalités **complexes de traitement des données** dans un environnement multipartite[268]. » (Corpus Lobbyplag, DIGITALEUROPE2, 2012, p. 51)

> « EK est d'avis que les règles existantes concernant les transferts transfrontières de données, telles qu'elles sont mises en œuvre et appliquées, ne sont pas les plus adaptées aux **réalités commerciales** [*business realities*] **d'aujourd'hui**. Ces règles ont une dimension assez bureaucratique et ne **conviennent pas** vraiment**, par exemple, à l'ère de l'infonuagique**[269] [*cloud computing*][270]. » (Consultation de 2010, EK1, 2011, p. 4)

Si, de l'avis de l'ensemble des enquêtés à qui la question a été posée, les petites et moyennes entreprises (PME) étaient faiblement représentées et peu défendues pendant les « discussions » sur le RGPD, l'image de la PME innovante a été fréquemment mobilisée dans les *position papers* étudiés. Ainsi, selon Mikko Niva de la compagnie Nokia, dans un courrier adressé à un député européen :

> « Le Règlement devra trouver un **équilibre** [*strike a balance*] entre protéger efficacement les données privées et ne pas **surcharger les PME**[271] de contraintes[272]. » (Corpus Lobbyplag, NOKIA1, 2012, p. 1)

---

267 Traduit de l'anglais. Texte original : « […] in the case of the credit bureau industry **moves that might restrict the availability of information or indeed how that information might be used could result in not only a slowing of GDP growth** […]. »
Texte mis en gras par l'auteur.

268 Traduit de l'anglais. Texte original : « A very detailed documentation procedure would remain an almost instantly **outdated** snapshot of a constantly changing reality characterized by **complex data processing** arrangements in a multiparty environment. »

269 Texte mis en gras par l'auteur.

270 Traduit de l'anglais. Texte original : « EK believes that the existing rules for cross-border data transfers as implemented and applied are not best suited for **today's business realities**. The rules are somewhat bureaucratic and rather **unfit e.g. for the era of cloud computing**. »

271 Texte mis en gras par l'auteur.

272 Traduit de l'anglais. Texte original : « The Regulation will have to strike a **balance** between the effective protection of private data and **not over-burdening SMEs** with obligations. »

L'image de la PME innovante qui doit être protégée d'un excès de zèle réglementaire a été repris par la délégation de l'Estonie, un pays où l'informatique est un secteur perçu comme stratégique, dans les négociations au Conseil de l'UE :

> « […] il est important de préciser quelles règles et quelles obligations s'appliquent aux **micro-entrepreneurs** et aux **PME**. Même si nous convenons que les principes généraux de la protection des données doivent s'appliquer aux entreprises et aux organisations de tout type, la taille de l'entreprise devrait être prise en compte dans la possibilité d'exclure les micro-entrepreneurs du champ d'application du règlement. Par exemple, dans certains cas, les obligations du contrôleur ou du processeur pourraient s'avérer **disproportionnées**[273] pour une petite entreprise[274]. » (Position de l'Estonie, Conseil de l'UE, 2012, document 9897/12, p. 40)

Nous voyons aussi apparaître, dans les deux citations ci-dessus, la référence à la croyance en une relation causale[275] selon laquelle toute réglementation est un obstacle, un poids (« *burden* ») à la croissance économique, qui est l'une des propriétés du référentiel néolibéral, méfiant à l'égard de toute action des pouvoirs publics.

En outre, une législation favorable à l'innovation se devait d'offrir de la « sûreté juridique » (« *legal certainty* ») aux entreprises. Comme nous l'avons vu, cette « sécurité juridique » était l'argument invoqué par la coalition industrielle en faveur d'un règlement, et contre la faculté accordée à la Commission européenne d'adopter des actes délégués[276].

Au sujet de la définition, un autre des sujets que nous avons identifiés comme centraux dans la « discussion » sur le RGPD, la délégation irlandaise s'inquiétait – comme nombre d'acteurs de la coalition industrielle – de « l'incertitude » ou de « l'insécurité » juridique produite par l'interdiction pour les responsables du traitement de recourir au consentement de la personne concernée lorsqu'il existe un « déséquilibre significatif entre la personne concernée et le responsable du traitement » (art. 7 § 4 de la proposition de RGPD)[277] :

> « Le critère du 'déséquilibre significatif' établi au paragraphe 4 est vague et sera source d'insécurité juridique : cette **incertitude** n'est pas acceptable dans un contexte de sanctions potentiellement lourdes en cas d'infraction[278]. » (Position de l'Irlande, Conseil de l'UE, 2012, document 9897/12, p. 69)

273 Texte mis en gras par l'auteur.

274 Traduit de l'anglais. Texte original : « […] it is important to clarify which rules and obligations apply to the **micro entrepreneurs** and **SMEs**. Although we agree that general principles of data protection should apply to all types of enterprises and organizations, the size of the enterprise should be taken into account the possibility to exclude micro entrepreneurs from the scope of the regulation. For example in some cases the obligation of the controller or processor could be disproportionally **burdensome** for a small enterprise. »

275 Ou « algorithme » dans la terminologie employée par Pierre Müller (Müller, 2011).

276 Cf. section 4.3.2.

277 Cf. section 4.3.3.

Enfin, selon le FPF, une définition et des conditions aussi strictes sur le consentement que celles inscrites dans la proposition initiale du RGPD aurait rendu impossible l'invention par Facebook de son fil d'actualités (« *News Feed* »). Or, selon le FPF, il s'agirait d'une innovation appréciée par plus d'un milliard d'individus à l'échelle de la planète (Corpus Lobbyplag, FPF1, 2013, p. 7). L'interdire, dans cette optique, eût été aller à l'encontre de l'intérêt général au nom du désir de vie privée d'une minorité d'individus égoïstes.

En résumé, les discours de la coalition industrielle n'ont pas cherché à attaquer de front la légitimité d'un droit *à la* protection des données à caractère personnel. Leur stratégie argumentative s'est fondée essentiellement sur la promotion de l'idée selon laquelle il fallait à tout prix maintenir un « équilibre » entre ce premier objectif, et d'autres objectifs d'intérêt généraux, au premier rang duquel : la croissance économique reposant sur l'innovation dans un contexte « d'économie de la connaissance ». Les différents acteurs de la coalition industrielle ont mobilisé dans ce sens un grand nombre d'arguments et de formules empruntés au vocabulaire de la stratégie de Lisbonne et de la stratégie Europe 2020, qui sont des documents programmatiques transversaux à l'ensemble des secteurs des politiques publiques de l'Union, et qui sont d'inspiration néolibérale. Leurs discours collaient donc d'assez près au référentiel global de l'UE.

4.5. La stabilité de l'argument de la confiance comme articulation entre le paradigme de la vie privée et le référentiel global

Face aux arguments de la coalition industrielle, la coalition des défenseurs de la vie privée a mobilisé le même argument que dans les années 1970 pour articuler leurs revendications motivées par leurs convictions internes au référentiel global : l'argument de la confiance[279].

Cette stratégie d'articulation commence, pour la plupart des défenseurs de la vie privée, par une concession faite au référentiel global : l'allégeance à l'objectif d'innovation et de croissance qui sous-tend les stratégies de Lisbonne et Europe 2020, ou au moins sa validation rhétorique. Ainsi, nous avons vu que des acteurs de la coalition des défenseurs de la vie privée, comme le G29, ont pu soutenir l'introduction de mesures « basées sur le risque », au nom de l'impératif de croissance économique et de réduction du « fardeau bureaucratique » pesant sur les entreprises, tout en les reformulant dans un sens qui soit compatible avec leurs objectifs[280]. Quant au BEUC, une fédération européenne d'association de défense des intérêts des consommateurs,

278 Traduit de l'anglais. Texte original : « The 'significant imbalance' test in paragraph 4 is vague and will create legal uncertainty; this **uncertainty** is not acceptable in the context of potentially large sanctions for infringement. »

279 Cf. section 3.8.

280 Cf. section 4.3.5.

un de ses *position papers* se présentait comme faisant non seulement une analyse des avantages et inconvénients de la proposition de RGPD pour les consommateurs, mais aussi pour les entreprises :

-Overall assessment-	
Impact on consumers	**Impact on businesses**
Strengthening and clarification of key data protection principles, including data minimisation and purpose limitation. Strengthening of the rights of data subjects to access their data. More transparency about how your data is handled, with easy-to-understand information, putting an end to privacy notices full of legal jargon. Notification about breaches of their personal data without undue delay. Improved administrative and judicial remedies in cases of violation of data protection rights. Increased responsibility and accountability for those processing personal data – including through the principles of 'privacy by design' and 'privacy by default'.	A level playing field for businesses through one single law applicable to any business across the EU. This harmonisation is expected to save businesses up to €2.3 billion per year. A 'one-stop-shop' – companies in the EU will be answerable to a single data protection authority (DPA), no matter how many EU countries they do business in. Abolition of the current obligation to notify data processing, which costs businesses about €130 million per year. The accountability principle grants businesses the flexibility to adopt appropriate measures in order to comply with the obligations set by the draft Regulation (Article 22).

Figure 22 : *Extrait du* position paper *intitulé «* Proposal for a Data Protection Regulation – BEUC analysis of consumer benefits versus administrative burden of key provisions *», à la page 3 du document BEUC1 du corpus de* position papers *récupérés depuis le dépôt Github de Lobbyplag*

Cette stratégie visait à démontrer que les propositions de la « *privacy community* » ne remettaient pas en cause l'objectif primordial de croissance économique du référentiel global auquel est soumis, comme les autres sous-systèmes de politique publique de l'UE, celui dédié à la protection des données à caractère personnel.

Au lieu de tenter une remise en cause cet objectif de croissance, les défenseurs de la vie privée ont cherché à démontrer qu'il serait inatteignable sans la confiance des citoyens-consommateurs du marché unique numérique. Cette position se retrouve par exemple clairement énoncée dans la communication rédigée par l'unité de protection des données de la DG JUST en 2012, qui accompagnait la proposition du RGPD et de la directive sur la protection des données dans les domaines JAI :

> « **S'ils n'ont pas confiance**, **les consommateurs hésiteront à effectuer des achats** en ligne et à recourir à de nouveaux services. Dès lors, il est également impératif de garantir un niveau élevé de protection des données pour **accroître la confiance des consommateurs** dans les services en ligne et réaliser le potentiel de l'économie numérique, ce qui stimulera la croissance économique et la compétitivité des entreprises de l'Union. » (Commission européenne, COM 2012 (9) FINAL FR, p. 2)

Un argument identique était formulé en 2011, en réponse à la consultation de la Commission européenne de 2010, par le BEUC :

> « Un haut niveau de protection des données à caractère personnel et de la vie privée est non seulement exigé par l'entrée en vigueur du traité de Lisbonne, mais constitue également une condition sine qua non de la réalisation des objectifs de l'**Agenda numérique de l'UE**, qui doit être **construit sur la confiance des consommateurs** dans l'environnement en ligne[281]. » (Consultation de 2010, BEUC1, 2011, p. 3)

Sans confiance, point de marché unique numérique, et par conséquent, guère de croissance en perspective. Cela sous-entend que même si le RGPD est contraignant, il coûterait toujours moins cher aux acteurs économiques que son absence, car il serait leur condition même d'existence.

Anna Walkowiak, de la fondation Panoptykon, a décrit de façon très précise et directe l'usage de cet argument de la confiance comme contre-argument aux arguments « économiques » de la coalition industrielle décrits dans le sous-chapitre précédent :

> « Habituellement, nous répondons en rappelant que lorsque vous examinez les recherches faites sur le sentiment des gens, vous voyez qu'ils ont le sentiment de ne pas avoir de pouvoir, que les informations qui les concernent… les gens ne savent pas ce qui se passe avec leur information, et c'est **une question de** […] **confiance**, principalement de confiance. Il doit y avoir certaines garanties, certaines règles. […] **Et il faut essayer de construire sur la confiance**. […] Si vous arrivez à créer de la confiance, vous obtenez un nouveau modèle économique **et vous pouvez être compétitif**[282]. » (entretien avec Anna Walkowiak)

Joe McNamee, d'EDRi, a lui aussi développé cet argument de la « confiance » en réponse à la même question :

> « Je recommanderais à cette [personne] de lire l'étude de la NTIA de juin de l'an dernier, qui montrait les importants dommages à… La NTIA étant un organisme gouvernemental, elle utilise un langage très diplomatique pour présenter ses conclusions. Mais elle a

281 Traduit de l'anglais. Texte original : « A high level of protection of personal data and privacy is not only required by the entry into force of the Lisbon Treaty, but it also constitutes a sine qua non condition for the achievement of the objectives of the **EU Digital Agenda**, which needs to be **built upon consumers' trust** in the online environment. »

282 Traduit de l'anglais. Texte original : « Usually we respond by reminding them that when you look at some research about how people feel, they feel that they don't have power, that information about them… they don't know what's going on with information, and **it's a question of** […] **trust**, mainly trust. There should be some safeguards, some rules. […] **And you're trying to build on trust**. […] If you're able to create trust, you have a new business model, **you can be competitive that way**. »

conclu que **45 % des foyers aux États-Unis évitent les transactions en ligne** par crainte d'atteintes à leur vie privée. Et nous, en Europe, avons la possibilité de renforcer notre protection des données pour réduire ces craintes en Europe et créer en Europe un environnement de **confiance**[283]. » (entretien avec Joe McNamee)

Nous voyons dans ce dernier extrait d'entretien que l'argument de la « confiance » y est appuyé par la mobilisation d'études et de données chiffrées qui viennent apporter un renfort de crédibilité au caractère expert du discours, gage de légitimité – et souvent condition de succès – dans le contexte des arènes européennes[284].

L'argument a été utilisé par EDRi notamment pour soutenir ses amendements en faveur d'un encadrement plus strict du profilage, et des décisions automatisées, fondé sur une plus grande transparence des algorithmes[285] :

« Le profilage est source d'importants risques pour les personnes concernées. Il est susceptible de renforcer les discriminations, de rendre les décisions moins transparentes, et comporte le danger inévitable des mauvaises décisions. […] Les profils sont basés sur des algorithmes complexes et dynamiques qui évoluent en permanence et sont difficiles à expliquer aux personnes concernées. Souvent, ces algorithmes constituent des secrets commerciaux et ne seront pas facilement dévoilés aux personnes concernées. Cependant, lorsque des personnes physiques font l'objet de profilage, elles devraient pouvoir obtenir des informations sur la logique de la mesure, ainsi que des explications quant à la décision finale si une intervention humaine a été obtenue. **Cela permet de réduire le manque de transparence, qui pourrait nuire à la confiance** dans le traitement des données et **pourrait mener à une perte de ou** [sic] **confiance** notamment dans les services en ligne[286]. » (Corpus Lobbyplag, EDRI2, 2013, p. 74)

283 Traduit de l'anglais. Texte original : « I would point this [person] to the NTIA study from June last year, which showed that there is vast damage **to online trust**... NTIA being a government body, used very diplomatic terms to describe its findings. But it found that **45 % of US households are avoiding online transactions** because of fears of privacy invasion. And we in Europe have the possibility to reinforce our data protection to reduce that in Europe, and create a **trustworthy** environment in Europe »
Texte mis en gras par l'auteur.

284 Cf. section 4.1.5.

285 Voir notamment la proposition d'amendement n° 102 du document EDRi Amendments.pdf, dans le corpus des documents récupérés depuis Lobbyplag, qui obligerait dans certains cas d'informer les personnes concernées sur la logique sous-jacente au fonctionnement des algorithmes de profilage les concernant. La citation qui suit l'appel à cette note de bas de page est extraite de la justification de cet amendement.

286 Traduit de l'anglais. Texte original : « Profiling can entail serious risks for data subjects. It is prone to reinforcing discriminations, making decisions less transparent and carries an unavoidable risk of wrong decisions. […] Profiles are based on complex and dynamic algorithms that evolve constantly and that are hard to explain to data subjects. Often, these algorithms qualify as commercial secrets and will not be easily provided to data subjects. However, when natural persons are subject to profiling, they should be entitled to information about the logic used in the measure, as well as an explanation of the final decision if human intervention has been obtained. **This helps to reduce intransparency, which could undermine trust** in data processing and **may lead to loss or** [sic] **trust** in especially online services. »
Texte mis en gras par l'auteur.

Le succès de cette stratégie se démontre notamment dans le fait que les acteurs de la coalition industrielle l'ont largement concédé. Ainsi, selon l'ICDP :

> « La capacité de la Société Européenne de l'Information à générer de l'innovation et de la croissance, telle qu'envisagée dans l'Agenda Numérique de la Commission européenne, **dépend de la création de la confiance nécessaire**[287] […] » (Corpus Lobbyplag, ICDP1, 2011, p. 2)

> « Ce lundi (28 janvier) était la Journée européenne de la protection des données, une bonne occasion de rappeler au monde des affaires que **nous devons gagner la confiance des personnes qui utilisent nos produits** et services, grâce à de bonnes pratiques commerciales et des contrôles puissants de protection de la vie privée[288]. » (ICDP, 2013)

Comme l'a rappelé un lobbyiste de la coalition industrielle en entretien :

> « Je pense que si vous posez la question à nos membres, il y a une compréhension fondamentale du fait que la protection de la vie privée est une priorité absolue [*top priority*]. C'est évidemment… c'est ainsi que l'on construit sa crédibilité, ses clients, sa **confiance**. Vous savez, **tout se construit sur cette confiance. Si vous n'avez pas cela, vous n'avez pas de business**[289]. » (Entretien Euro5)

Plusieurs décennies après les premiers discours sur la nécessité de lois de protection des données pour garder la confiance des citoyens et des consommateurs en l'informatique[290], l'argument de la confiance demeure un argument phare pour articuler les revendications des défenseurs de la vie privée fondée sur leur référentiel sectoriel, à un référentiel qui a évolué depuis les années 1960 et 1970, mais a conservé la propriété d'être favorable à la collecte et à l'exploitation en masse de données à caractère personnel. Cet argument se retrouve d'ailleurs

287 Traduit de l'anglais. Texte original : « The ability of the European Information Society to generate innovation and growth, as envisaged in the European Commission's Digital Agenda, **depends on creating the necessary trust** […]. »
Texte mis en gras par l'auteur.

288 Traduit de l'anglais. Texte original : « This Monday (28 January) was European Data Protection Day – a good reminder for the business community that **we have to earn the trust of the people that use our products** and services through good business practices and strong privacy controls. »
Texte mis en gras par l'auteur.

289 Traduit de l'anglais. Texte original : « I think if you ask our membership that there is a fundamental understanding that privacy is top priority. It is obviously… that's how you build your credibility, customers, clients, your **trust**, you know, **that all builds into this trust**. So **if you don't have that in place, you don't have a business**. »
Texte mis en gras par l'auteur.

290 Cf. section 3.8.

invoqué par des acteurs impliqués dans les arènes de standardisation technique que nous étudierons dans le chapitre suivant[291].

4.6. La stabilité du paradigme libéral de la vie privée

Le paradigme libéral de la vie privée[292] a, comme nous l'avons vu dans le chapitre précédent[293], largement inspiré les dispositions des premiers textes de protection des données à caractère personnel dans les années 1970. Il a pour caractéristique de valoriser le droit *à la* vie privée de l'individu pour que celui-ci puisse préserver son autonomie individuelle.

Alan Brandeis et Alan Westin furent deux des principaux théoriciens de ce paradigme libéral. Dans notre corpus d'analyse[294], la chaîne de caractères « westin » n'a d'occurrence que dans un seul document sur 556. La chaîne de caractères « brandeis » n'apparaît nulle part. Le contenu des discours produits par les acteurs ayant participé aux « discussions » sur le RGPD n'en demeure pourtant pas moins marqué par l'empreinte, implicite mais omniprésente, du paradigme libéral de la vie privée.

Dans un communiqué de presse de la Commission du 25 janvier 2012 annonçant le lancement des procédures législatives 2012-010 et 2012-011 ayant donné, respectivement, la directive de protection des données dans les domaines JAI et le RGPD, la commissaire Viviane Reding affirmait que « […] nos concitoyens […] n'ont pas toujours le sentiment de maîtriser entièrement les données à caractère personnel les concernant ». La citation se poursuit par l'annonce que ses « propositions législatives contribueront […] à susciter la confiance dans les services en ligne parce que les utilisateurs seront mieux informés de leurs droits et auront une plus grandes maîtrise des informations qui les concernent » (Commission européenne, 2012d, p. 2)

Cette idée de la maîtrise individuelle sur ses données à caractère personnel, qui s'oppose au demeurant à l'idée de la création de droits de propriété cessibles sur ces dernières, s'est également retrouvée dans des discours de parlementaires impliqués dans ce sous-système de politique publique, de bords politiques différents. Ainsi, pour Kaja Kallas, eurodéputée estonienne libérale de l'Alliance des démocrates et des libéraux européens, le droit *de la* protection devait préserver avant tout le libre-choix de l'individu :

> « [La protection des données] est de plus en plus importante car nous constatons qu'il y a une immense quantité de données sur les individus, partout. Et les gens ne sont pas toujours réellement conscients que leurs données sont traitées comme elles le sont. Je

291 Cf. section 5.6.3.
292 Cf. section 2.2.
293 Cf. chapitre 3, notamment section 3.6.
294 L'ensemble des documents parcourus par le script est énuméré en annexe 4.

pense que les gens devraient le savoir et devraient avoir le choix[295]. » (Entretien avec Kaja Kallas)

Dans le rapport rédigé par le rapporteur Jan Philipp Albrecht, eurodéputé écologiste allemand aux convictions politiques très différentes de celles de Kaja Kallas, il est rappelé que :

> « Le consentement devrait demeurer l'élément clé de l'approche de la protection des données de l'Union européenne, puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement des données. » (Albrecht, 2013, p. 224-225)

L'un des chapitres du livre que ce député écologiste a publié au cours du processus d'adoption du RGPD a pour titre *How can we achieve digital sovereignty?* (en français : *Comment parvenir à la souveraineté numérique ?*) (Albrecht, 2015a, p. 75-99). Cela peut sembler à première vue une référence au cadrage de la « vie privée » sous l'angle de la « souveraineté numérique[296] ». Mais à y regarder de plus près, le discours développé dans ce chapitre s'intéresse en fait à la « souveraineté » de l'individu sur lui-même, sur ses propres données, qu'il doit pouvoir soustraire à la surveillance et au contrôle dans un espace informationnel de liberté individuelle. Lorsque l'auteur développe dans ce chapitre une critique du *Quantified Self*[297], qu'il désigne sous le terme de « *Big Data about yourself* », il y oppose « l'auto-détermination » de l'individu doté du droit *à la* protection des données à caractère personnel :

> « Les Big Data générés sur vous vont nécessairement générer une logique d'optimisation. Car une fois que les données fondamentales sont disponibles, les points initiaux nécessitant des améliorations se dégagent et deviennent évidents. Vivre plus sainement, travailler plus efficacement, cuisiner mieux, trouver un meilleur partenaire. […] À défaut d'autre chose, ne serait-il pas logique d'ignorer, voire de s'opposer, à cette logique d'amélioration de l'efficacité du Big Data, simplement parce qu'elle fait de nous des machines poussées à la limite de leur efficacité ? […] Le chemin vers le regain de la souveraineté sur nos données implique également de **retrouver notre auto-détermination** et de prendre en main nos vies à l'ère numérique[298]. » (Albrecht, 2015a, p. 92-93)

---

295 Traduit de l'anglais. Texte original : « [Data protection] is more and more important, because we see there is immense data about people everywhere. And people are not actually very aware that their data is being processed the way it is. And therefore, I feel that people should know and people should have the choice. »

296 Cf. section 2.4.2.

297 Cf. section 2.4.1.

298 Traduit de l'anglais. Texte original : « The Big Data about yourself is bound to generate an optimisation logic. For once the fundamental data are available, the initial areas needing improvement become evident. Live more healthily, work more efficiently, cook better, find a better partner. […] If nothing else, would it not make sense to ignore or even oppose the Big Data efficiency enhancement logic simply because it makes us into machines being driven to the limits of their efficiency. […] The path towards the recovery of sovereignty over our data also involves **recovering our self-determination** and taking responsibility for our own lives in the digital era. »
Texte mis en gras par l'auteur.

Le rapporteur du RGPD voyait donc dans les techniques du *Quantified Self* un frein à l'autonomie individuelle. Il rappelle, d'une part, qu'« en tant que consommateur, [il] doit être en position de pouvoir fondamentalement décider pour lui-même [s'il] souhaite révéler des informations sur [lui], ou préférerait les garder pour [lui][299] » (Albrecht, 2015a, p. 41). D'autre part, il indique que le droit *à la* vie privée n'est selon lui pas suffisant pour protéger cette autonomie individuelle et cette liberté de choix. Il distingue un droit *à la* vie privée, qui serait selon lui une approche états-unienne, d'un droit *à la* protection des données à caractère personnel, européen, qui serait synonyme de droit à l'auto-détermination informationnelle (Albrecht, 2015a, p. 30). À plusieurs reprises, il cite d'ailleurs l'arrêt de 1983 du Tribunal constitutionnel fédéral de RFA ayant révélé l'existence du droit à l'auto-détermination informationnelle[300], et écrit que « la protection des données est entièrement une affaire de protection des personnes et de leur droit à l'auto-détermination[301] » (Albrecht, 2015a, p. 25).

Nous voyons bien apparaître dans ces citations un discours fondé sur les idées du paradigme libéral de la vie privée, qui, outre Jan Philipp Albrecht, a inspiré nombre de défenseurs de la vie privée impliqués dans les « discussions » sur le RGPD. La coalition industrielle n'est pas parvenue à remettre en cause la pertinence de la vision libérale de la « vie privée », ancrée depuis plusieurs décennies comme référentiel sectoriel des politiques publiques de protection des données. Elle ne semble d'ailleurs guère avoir essayé.

La coalition industrielle, comme nous l'avons vu, a adhéré assez largement à l'argument de la confiance. Elle jugeait toutefois que des objectifs de croissance économique et l'agenda néolibéral du référentiel global des politiques publiques européennes pouvaient justifier un assouplissement des règles de protection des données, cadrées dans leurs discours comme étant des « fardeaux bureaucratiques[302] ». Cela justifiait l'argument central de leur discours : celui d'un « nécessaire » équilibre entre le droit fondamental *à la* protection des données à caractère personnel (et/ou du droit *à la* vie privée) d'une part, et des mesures favorisant la croissance d'autre part. Mais revendiquer un « équilibre » de ces droits avec d'autres objectifs, ce n'est pas la même chose que remettre directement ces droits en cause.

Selon l'un des lobbyistes interrogés, il était impossible de remettre en cause que ces droits sont de caractère *fondamental* :

> « Je pense, vous savez, que ces discussions partaient toujours du postulat que la protection de la vie privée est un droit fondamental. Alors, comment argumenter ? Je veux dire…

299 Traduction de l'auteur. Texte original : « As a consumer, I must be in a position in which I am fundamentally able to decide for myself, whether I wish to reveal information about myself, or would rather keep it to myself »

300 Décision du Tribunal constitutionnel fédéral allemand BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil).

301 Traduction de l'auteur. Texte original : « Data protection is all about protecting people and their right to self-determination. »

302 Cf. section 4.4.

tout le monde veut avoir des droits fondamentaux. Il est très difficile de déconstruire cet argument. Et bien sûr, il faut le reconnaître[303]. » (entretien Euro5)

Malgré cela, les acteurs de cette coalition auraient pu tenter de redéfinir le contenu du droit *à la* vie privée et/ou du droit *à la* protection des données à caractère personnel, dans un sens allant à l'encontre des convictions – et des revendications – des défenseurs de la vie privée. Bien que de tels exemples sont extrêmement rares dans notre corpus, il est intéressant d'examiner brièvement l'exemple le plus poussé.

L'un des *position papers* rédigés par le *Future of Privacy Forum* (FPF), et répertorié dans le corpus de documents du dépôt Github de Lobbyplag, est un rapport dédié au consentement intitulé « Livre blanc sur le consentement » (« *White paper on consent* »). Il contient une référence à Alan Westin comme étant le fondateur de la conception de la vie privée intégrée à l'état du droit *de la* protection des données, et notamment des dispositions sur le consentement des personnes concernées :

> « La conceptualisation canonique du savant et pionnier de la protection de la vie privée Alan Westin définit la vie privée comme un contrôle individuel sur des informations personnelles[304]. De cette manière, tous les cadres juridiques de protection de la vie privée existants mettent considérablement l'accent sur le consentement[305]. » (Corpus Lobbyplag, FPF1, 2013, p. 3)

Toutefois, selon le FPF, cette approche serait dépassée. En effet, dans le contexte technologique actuel, l'obligation de demander toujours un consentement explicite fatiguerait l'utilisateur. Permettre « l'*opt-out* » pour valider le consentement serait dès lors une façon de prendre en compte la « réalité technique » contemporaine :

> « The effect [of systematic opt-in consent] has been to burden individuals with difficult, complicated choices, which become a detriment to user interfaces and cause notice fatigue. As new technologies emerge, the opportunities for consent expand geometrically and eventually become meaningless, as consumers tick boxes reflexively in order to proceed with the use of the technology. Moreover, as the « Internet of Things » advances,

303 Traduit de l'anglais. Texte original : « I think, you know, in these discussions, it was always coming from the premise that privacy is a fundamental right. So how do you argue ? I mean. We're all for… everybody wants to have the fundamental rights. It is very difficult to sort of deconstruct that argument. And obviously you have to recognise that. »

304 Note de bas de page dans le texte : « Alan Westin, PRIVACY AND FREEDOM 7 (Antheneum, 1967) »

305 Traduit de l'anglais. Texte original : « Privacy scholar and pioneer Alan Westin's canonical conceptualization depicts privacy as individual control over personal information. Accordingly, all existing privay frameworks place considerable emphasis on consent. »

and as the prevalence of screens on which choices may be indicated diminishes, just-in-time explicit consent may not be possible at all[306]. » (Corpus Lobbyplag, FPF1, 2013, p. 4)

L'argumentaire du FPF, s'il s'en était tenu à l'argument selon lequel il faut, dans l'intérêt de l'individu, renoncer à demander systématiquement son consentement préalable à la collecte de données, pour ne pas le fatiguer, n'aurait rien eu d'original. Nous retrouverons en effet le même argument dans des *position papers* qui défendent une vision classiquement libérale du droit *à la* vie privée et *à la* protection des données à caractère personnel.

Mais il va plus loin, en attaquant l'idée même de l'auto-détermination informationnelle. Pour ce faire, les auteurs du document citent les travaux d'Helen Nissenbaum sur la vie privée contextuelle (Corpus Lobbyplag, FPF1, 2013, p. 7). L'idée centrale de la théorie d'Helen Nissenbaum est que le sentiment d'intrusion naît de la violation des frontières du contexte dans lesquelles il est socialement admis qu'une information sur un individu circule[307] (Nissenbaum, 2004, 2010). Si, comme nous le verrons dans le chapitre suivant[308], cette idée peut être utilisée pour dire que les mécanismes de consentement individuel à la collecte de données sont une façon d'assurer le respect de ces normes sociales et d'éviter des circulations non souhaitables d'information, ici, le FPF propose d'éliminer ou de réduire ces mécanismes de consentement à partir du moment où la circulation de données personnelles se fait à l'intérieur d'un contexte socialement admis. À charge alors au responsable du traitement de déterminer les frontières d'un tel contexte. Cela permettrait de mieux s'adapter aux changements de société et, surtout, à cette « réalité technique » (« *technical reality* ») qui rendrait le paradigme libéral obsolète sauf dans des cas exceptionnels aux contours flous :

« Certains avancent l'argument que le fait de solliciter un consentement exprès doit être une condition préalable de *tout*[309] déplacement des frontières [contextuelles] existantes. Toutefois, en réalité, les évolutions des périmètres contextuels ne sont pas toujours volontiers négociés. Les entreprises devraient plutôt évaluer les effets de tout changement potentiel des attentes des personnes concernées, expliquer leurs politiques clairement et ostensiblement, et **dans certains cas** fournir aux personnes concernées des possibilités de refus [*opt-out*]. Lorsqu'un changement de contexte est radical et que les mesures de transparence sont insuffisantes, l'on peut s'appuyer sur un consentement exprès pour s'assurer que les personnes concernées acceptent une nouvelle utilisation de leurs données. Il n'est jamais simple de trouver le juste équilibre entre l'évolution des normes sociales et les droits individuels, mais **afin de permettre l'innovation et la croissance**

306 Traduction en français : « L'effet [du consentement *opt-in* systématique] a été de faire peser sur les individus des choix complexes et difficiles, qui nuisent aux interfaces utilisateur et entraîne une lassitude d'attention [*notice fatigue*]. Avec l'émergence de nouvelles technologies, les occasions de consentir augmentent jusqu'à perdre tout sens, et les consommateurs cochent des cases par réflexe afin d'utiliser la technologie. De plus, avec les progrès de l'« Internet des Objets » et la diminution de la prévalence des écrans pouvant proposer des choix, un consentement *opt-in* et immédiat pourrait tout simplement ne pas être possible. »
Le texte original en anglais a été maintenu dans le corps du texte car une partie du sens se perd à la traduction.

307 Cf. section 2.3.5.

308 Cf. section 5.6.2.

309 En italique dans le texte original.

> **dans l'économie européenne, les décideurs politiques doivent éviter les normes restrictives et formalistes**[310]. » (Corpus Lobbyplag, FPF1, 2013, p. 7)

Plus loin dans le document, cette approche par les contextes a servi à justifier un renforcement du critère de l'intérêt légitime comme condition de licéité du traitement de données à caractère personnel, au détriment du consentement (Corpus Lobbyplag, FPF1, 2013, p. 8).

Parmi les documents étudiés dans notre corpus, il s'agit de celui qui, du côté de la coalition industrielle, nous semble aller le plus loin dans une tentative de remise en cause du paradigme libéral de la vie privée. De telles tentatives ont été exceptionnelles, sinon marginales. Et même dans ce document, ses auteurs ne parviennent pas à renoncer tout à fait aux idées de « choix » et de « contrôle » individuels, comme en atteste cette citation :

> « Le Future of Privacy Forum soutient les mesures qui visent à offrir aux individus davantage de transparence, de choix et de contrôle sur leurs données à caractère personnel[311]. » (Corpus Lobbyplag, FPF1, 2013, p. 11)

Nous observons ainsi, que, de fait, l'essentiel des discours d'acteurs de la coalition industrielle font référence et valident une vision de ces droits inspirée du paradigme libéral de la vie privée, centrée sur l'autonomie de l'individu. Microsoft a par exemple affirmé son attachement à « l'autonomisation » (« *empowerment* ») et le « contrôle » (« *control* ») de ses utilisateurs dans l'usage qui est fait des données les concernant :

> « En tant qu'entreprise engagée pour le respect de la vie privée des utilisateurs, nous croyons en la nécessité de faire preuve de transparence avec nos clients quant à nos pratiques en matière de protection des données, et **nous travaillons dur à élaborer des innovations pour permettre à** [*empower*] **nos clients de disposer d'un choix et d'exercer un contrôle** sur leurs informations personnelles[312]. » (Corpus Lobbyplag, MICROSOFT1, 2013, p. 1)

---

310 Traduit de l'anglais. Texte original : « Some argue that soliciting express consent should be a prerequisite to *any* shift in existing boundaries. In reality, however, shifting contexts are not always readily negotiated. Rather, organizations should assess the effects of any prospective change on data subject expectations; convey their policies clearly and conspicuously; and **in certain cases** provide data subjects with an opportunity to opt out. When a change in context is radical and transparency measures inadequate to support it, express consent can be relied upon to ensure that data subjects are willing to accept a new data use. Finding the precise balance between evolving social norms and individual rights is never easy; yet **in order to permit innovation and growth in the European economy, policymakers should avoid restrictive formalistic standards**. »

311 Traduit de l'anglais. Texte original : « The Future of Privacy Forum supports measures to provide individuals with greater transparency, choice and control over their personal data. »

312 Traduit de l'anglais. Texte original : « As a company committed to user privacy, we believe in being transparent with our customers about our data protection practices and **we work hard to develop innovations that empower our customers to exercise choice and control** over their personal information. »
Texte mis en gras par l'auteur.

Cet argument selon lequel l'utilisateur doit garder le contrôle de l'utilisation de ses données a même été mobilisé, par exemple par Business Europe, pour justifier les demandes de la coalition industrielle d'avoir une définition souple du consentement[313] :

> « Nous ne soutenons pas les modifications de la définition du consentement, étant donné qu'elles rendront le processus trop lourd et prescriptif. Dans le cas de relations d'affaires [*business relations*] prolongées, ces exigences sont un fardeau administratif supplémentaire inutile.
> **Cela est susceptible de transformer le consentement en exercice de cochage de cases plutôt qu'en moyen pour les personnes concernées de contrôler leurs données**. Le nombre de formulaires et de cases à compléter ou cocher par les utilisateurs augmentera. Les services en ligne subiront des conséquences négatives, étant donné que les utilisateurs seront à un clic supplémentaire d'accéder au produit, aux services ou au contenu qui les intéresse. Les consommateurs doivent conserver la possibilité de fournir un consentement implicite, par exemple dans le processus d'inscription[314]. » (Corpus Lobbyplag, BUSINESSEUROPE1, 2012, p. 5)

Cette idée selon laquelle les dispositions sur le consentement proposées par la Commission européenne, et soutenues par les défenseurs de la vie privée, aboutirait à submerger l'utilisateur de demandes et à ainsi le « fatiguer » ou de le « lasser » au point de les vider de leur substance, a donné lieu à la création de la formule de « *click fatigue* », reprise par la délégation irlandaise au Conseil de l'UE :

> « Cela engendre le risque d'inonder les utilisateurs de cases à cocher et d'avertissements, et pourrait engendrer une expérience en ligne décousue et sans cesse interrompue[315]. » (Corpus Lobbyplag, FACEBOOK2, 2013, p. 19-20)

> « L'exigence systématique d'un consentement explicite peut engendrer des pratiques peu accueillantes pour les utilisateurs (« **lassitude de clic** » [*click fatigue*]), sans offrir aux

313 Cf. section 4.3.3.

314 Traduit de l'anglais. Texte original : « We do not support the changes in the definition of consent as they will make the process too cumbersome and prescriptive. In case of continued business relationships, these requirements are an unnecessary supplementary administrative burden.
This is likely to turn consent into a box-ticking exercise rather than a way for data subjects to control their data. The number of forms and tick boxes that users need to complete will increase. Online services will be negatively affected, as users will be an additional click away from accessing the product, services, content they are interested in. It must remain possible for consumers to provide implicit consent i.e. in the process of registration. »
Texte mis en gras par l'auteur.

315 Traduit de l'anglais. Texte original : « This carries the risk of inundating users with tick boxes and warnings and may result in an overly disrupted or disjointed internet experience. »

personnes concernées un meilleur niveau de vie privée[316]. » (Corpus Lobbyplag, TELEFONICA1, 2013, p. 8)

« L'exigence d'un consentement explicite dans tous les cas peut également avoir des conséquences indésirables, par exemple une forme de '**lassitude de clic**' qui pourrait de manière perverse mener les consommateurs à mettre en danger leurs données à caractère personnel. Elle peut également réduire la base statistique utilisée par les entreprises qui s'appuient sur des analyses de fréquentation web pour réaliser des gains d'efficacité ou améliorer leur mise en page et leur contenu destinés aux utilisateurs[317]. » (Position irlandaise, Conseil de l'UE, document 9897/12, p. 66)

Des acteurs de la coalition industrielle ont aussi insisté sur le fait que, selon eux, la popularité de services informatiques reposant sur l'exploitation de données à caractère personnel, par exemple pour personnaliser les contenus, démontrait qu'il y avait une demande pour de tels services. Dès lors, les interdire ou en « dégrader la qualité », comme le RGPD risquait de le faire selon la coalition industrielle, aurait aussi été, d'une certaine façon, ne pas respecter les désirs de l'utilisateur :

« En englobant toutes les formes de personnalisation, quelles que soient les conséquences possibles pour les utilisateurs, les nouvelles règles pourraient compromettre les efforts fournis par les entreprises pour offrir à leurs clients des produits et services « personnalisés » et dégrader la qualité des services offerts aux citoyens européens[318]. » (Corpus Lobbyplag, FBF1, 2012, p.3)

« Nous sommes convaincus que l'examen doit être effectué à la lumière d'un principe fondamental de l'UE, à savoir la notion de consommateur rationnel et informé. Tout règlement surprotecteur donnera lieu à une conception du consommateur comme vulnérable et incapable de mener sa vie sans la protection complète du gouvernement[319]. » (Corpus Lobbyplag, FEDIL1, 2012, p. 3)

316 Traduit de l'anglais. Texte original : « Systematically requiring explicit consent may lead to practices which are both user unfriendly (« **click fatigue** ») while not leading to a higher level of privacy protection for data subjects. »
Texte mis en gras par l'auteur.

317 Traduit de l'anglais. Texte original : « Requiring explicit consent in all cases may also trigger unintended consequences, e.g. a form of '**click fatigue**' which may, perversely, lead consumers to endanger their personal data. It may also result in a reduced statistical base for companies relying on web analytics to achieve efficiency gains or to provide improved layout and content for users. »
Texte mis en gras par l'auteur.

318 Traduit de l'anglais. Texte original : « By encompassing all forms of personalisation, whatever the possible impact on users, the new rules could compromise the effort made by companies to offer their customers "customised" products and services and degrade the quality of services offered to European citizens. »

319 Traduit de l'anglais. Texte original : « We believe that the review should be guided by a fundamental principal of the EU, namely the notion of the rational and informed consumer. Any over-protective regulation will convey a perception of a consumer who is vulnerable and ultimately unable to navigate through life without the encompassing protection of the government. »

Cet argument a donc été une façon d'utiliser l'idée de l'auto-détermination informationnelle pour dénoncer des dispositions perçues par la coalition industrielle comme paternalistes.

Du côté des ONG, Jens-Henrik Jeppesen, de CDT, a défini le « droit *à la* vie privée » de l'article 7 de la Charte des droits fondamentaux de l'UE comme étant « *the right to be left alone* » (« le droit d'être laissé tranquille »), une formulation synonyme et paronyme (en anglais) de celle utilisée par Louis Brandeis et Samuel Warren dans leur article 1890 dans la *Harvard Law Review* qui fut à l'origine de la formalisation juridique de ce droit (« *right to be let alone*[320] »).

De son côté, Joe McNamee d'EDRi a défini le droit *à la* vie privée comme « un concept plus large [que celui de protection des données personnelles] de protection de l'espace personnel des individus, de leur autonomie individuelle[321] ». Anna Walkowiak de la fondation Panoptykon répondit de façon presque identique en entretien. Pour elle aussi, le droit *à la* vie privée était « un concept plus large » (« *broader concept* ») que celui de droit *à la* protection des données à caractère personnel. Interrogée sur les raisons de l'engagement de son ONG en faveur de l'adoption du RGPD, elle répondit que « les informations sur les individus [étant] d'une grande importance[322] » en tant qu'« outils pour gouverner ces personnes et les contrôler[323] », il fallait « aider les gens à utiliser ces droits [*à la* protection des données], les renforcer[324] » (entretien avec Anna Walkowiak). Elle poursuivit en citant des œuvres de Michel Foucault, Zygmunt Bauman et David Lyon, des auteurs ayant contribué intellectuellement à l'évolution du paradigme libéral de la vie privée, à l'appui de ses propos[325]. Le nom même de cette association fait explicitement référence au « panoptique », construction architecturale inventée par Jeremy Bentham et qui a inspiré les travaux de Michel Foucault dans *Surveiller et punir* sur la discipline et le biopouvoir (voir : Simon, 2002).

Cette adhésion au paradigme libéral de la vie privée, et surtout l'idée de droit à l'auto-détermination informationnelle de l'individu, a malgré tout fait l'objet de critiques internes au sein de la coalition des défenseurs de la vie privée. Ainsi, selon Walter Hötzendorfer de l'ONG autrichienne Epicenter Works, l'individu ne devrait pas toujours avoir le droit de consentir à certains usages de ses données à caractère personnel car la vie privée a une dimension de bien commun. En entretien, il développa un parallèle entre celle-ci, et la vaccination :

> « Je dirais qu'il y a une raison pour laquelle personne ne peut décider seul de cela, parce qu'il y a une dimension sociétale. C'est comme pour les vaccins. Vous n'avez pas à être

320 Cf. section 2.2.
321 Traduction de l'auteur. Texte original : « […] privacy is a larger concept of the individual and protection of their personal space, their individual autonomy » (entretien avec Joe McNamee).
322 Traduction de l'auteur. Texte original : « Information about individuals is really important. »
323 Traduction de l'auteur. Texte original : « It's a tool to govern these persons, and to control her, her or him. »
324 Traduction de l'auteur. Texte original : « […] help people be able to use the rights, make them stronger [...] ».
325 Cf. fin de la section 2.2.

vacciné parce que vous êtes protégé, même si cela peut être votre choix. Il est obligatoire d'être vacciné pour protéger tous les autres[326]. » (entretien avec Walter Hötzendorfer)

Ainsi qu'il l'a expliqué en entretien, cette valeur collective de la vie privée découlerait de son caractère instrumental pour garantir des droits fondamentaux indispensables au bon fonctionnement de la démocratie, cette dernière étant un bien commun. Une idée similaire a été exprimée en entretien par Lionel Maurel, militant à la Quadrature du Net en France, pour qui « la vie privée […] est la condition d'exercice des libertés ».

Lionel Maurel a publié avec Laura Aufrère une tribune dans *Le Monde* sur le RGPD au moment de son entrée en application. Selon eux, la « dimension collective échappe pour l'essentiel au RGPD, car malgré ses réelles innovations, il reste empreint de la même philosophie « personnaliste » qui inspira dès 1978 la loi Informatique & Libertés en France. Dans cette approche, les données sont appréhendées à travers un prisme « individualiste » qui ne les saisit qu'en tant qu'elles se rapportent à un individu déterminé en permettant de l'identifier » (Aufrère et Maurel, 2018b). Or toujours selon ces mêmes auteurs : « cette approche repose en réalité sur une fiction juridique que les plateformes sont déjà en train d'exploiter : l'individu isolé, capable « d'auto-détermination » et érigé à ce titre en centre de gravité de la régulation » (Aufrère et Maurel, 2018b). Ils en appellent alors à la protection de droits non pas individuels, mais collectifs, des données à caractère personnel (Aufrère et Maurel, 2018a).

Cette idée d'une protection collective, et non pas individuelle, des données à caractère personnel se justifie également selon Lionel Maurel et Laura Aufrère par la valeur économique, exploitée par certaines entreprises comme Google et Facebook, du réseau de données à caractère personnel de leurs utilisateurs (Aufrère et Maurel, 2018a, 2018b). Cette prise en compte de la dimension économique de l'exploitation des données à caractère personnel des utilisateurs rappelle la proximité intellectuelle de ces auteurs avec les théories du *Digital Labour*[327]. Elle rappelle par certains côtés des préoccupations sur les dimensions collectives du droit *à la* vie privée qu'avait exprimées plusieurs décennies auparavant le juriste italien, proche du parti communiste, Stefano Rodotà, même si lui n'abordait pas la question de l'aliénation de la valeur produite par les sujets des données personnelles collectées (Rodotà, 1974).

Ces différences de point de vue ont pu aboutir à quelques désaccords sur l'action à mener.

Ainsi, à la suite de l'entrée en application du RGPD le 25 mai 2018, plusieurs organisations ou associations « à but non lucratif, qui [ont] été valablement constitué[es] conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le

326 Traduit de l'anglais. Texte original : « I will say that there is a reason why people cannot decide that solely on their own, because there is a societal dimension. It's like with vaccination. You shouldn't be vaccinated because you are protected, that may be your choice. You should be vaccinated to protect all the others. »

327 Cf. section 2.3.3.

cadre de la protection des données à caractère personnel les concernant » (art. 80 §1 du RGPD) ont cherché à mener des actions de groupe contre des entreprises qu'elles accusaient de ne pas respecter le droit *de la* protection des données à caractère personnel. C'est notamment dans le but de mener de telles actions en justice que Max Schrems, un militant autrichien qui avait déjà obtenu l'annulation par la CJUE de l'accord *Safe Harbor* sur l'échange de données à caractère personnel entre l'UE et les États-Unis[328] a fondé en 2017 l'association *None Of Your Business* (NOYB). En 2019, cette dernière, associée à la Quadrature du Net, a obtenu de la CNIL la condamnation de Google pour défaut de recueil valide du consentement des utilisateurs de son système d'exploitation Android[329].

D'autres projets de ce type ont vu le jour en Europe. En avril 2018, nous avions organisé avec le soutien financier de l'ISOC France un atelier à Paris, réunissant chercheurs, adhérents et employés d'association envisageant de lancer de tels recours collectifs après l'entrée en application du RGPD. Cet atelier était réparti entre une réunion en comité restreint entre les chercheurs et les acteurs d'ONG invités, et une restitution publique en soirée. L'objectif était de réfléchir à l'élaboration de méthodes permettant d'estimer le montant du préjudice à demander aux responsables du traitement contrevenant au RGPD, dans le cadre d'une action collective au civil, dans les États membres ayant choisi de permettre qu'une association « exerce [au nom de la personne concernée] le droit d'obtenir réparation visé à l'article 82 [du RGPD] » (art. 80 §1 du RGPD) (Castex et al., 2018).

Cette réunion a été l'occasion d'un débat entre la Quadrature du Net d'une part, et d'autre part les participants à l'initiative e-Bastille soutenue par l'ISOC France et la fondation Panoptykon, sur le point de savoir s'il fallait ou non demander le remboursement pécuniaire du préjudice moral subi au titre de la violation d'une ou plusieurs dispositions du RGPD. Pour les personnes représentant l'ISOC France ou la fondation Panoptykon, des recours collectifs permettant de demander le versement d'un dédommagement financier individuel multiplié par le grand nombre de personnes concernées représentées à travers des associations, était un moyen stratégique d'inciter les entreprises à se mettre en conformité. Pour la Quadrature du Net, à l'inverse, cela n'avait aucun sens de parler de préjudice individuel, le préjudice étant plutôt, pour les membres de cette association, collectif.

Revenant sur ce débat entre, en France, la Quadrature du Net et e-Bastille, lors d'une question à ce sujet, Lionel Maurel expliqua :

> « On avait des nuances avec eux sur pas mal de choses en fait. Nous ce qui nous gênait surtout, c'était le fait […] de demander des dédommagements individuels […]. Ce qui [est] le but d'e-Bastille […]. C'est aussi ce qu'a fait Max Schrems […]. Mais nous en fait comme il y a eu un grand débat sur la monétisation des données personnelles, droit de propriété sur les données personnelles, on n'a pas voulu s'engager dans cette voie, parce que symboliquement, il y a quelque chose qu'on a trouvé un peu dérangeant dans le fait

328 CJUE 6 octobre 2015 « Schrems contre DPC Irlande » Aff. C-362/14.

329 CNIL, Délibération de la formation restreinte n° SAN-2019-1 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société Google Inc.

> de demander une réparation qui se concrétise par un retour individuel. […] Même si c'est complètement différent juridiquement […] il y a une sorte d'isomorphie avec le fait de payer pour l'usage des données personnelles. […] Mais il y a d'autres choses que j'ai notées. Ils balançaient des stickers sur lesquels il y avait marqué : « protégeons « nos » données personnelles ». Et moi j'aime pas du tout ce genre de phraséologie. » (Entretien avec Lionel Maurel)

Ce type de « nuances » entre acteurs de la coalition de la « *privacy community* » contribue à expliquer le fait, qu'à l'heure actuelle, les acteurs de la Quadrature du Net considèrent EDRi et ses membres comme des alliés, sans adhérer pour autant à l'organisation.

Dire que l'engagement des militants de la « *privacy community* » s'explique exclusivement par le paradigme libéral de la vie privée est donc simplificateur et faux. Ce paradigme est un point de référence partagée, qui peut faire, et fait, l'objet de mises en débat en interne, alimenté par l'influence d'autres théories, comme celles sur le *Digital Labour* au sein de la Quadrature du Net, ou encore, si l'on parle du Cecil, une autre ONG française, des théories décroissantes de Jacques Ellul, qui a préfacé un livre de son président, André Vitalis (Vitalis, 1988)[330].

Toutefois, ces débats sont restés assez largement internes. L'emploi du mot « nuance » par Lionel Maurel semble souligner une volonté de ne pas se désolidariser des positions d'alliés malgré l'existence de tels débats, comme si ces désaccords ne touchaient pas à l'essentiel. Ainsi, ces derniers n'ont remis en cause ni la cohérence d'ensemble ni l'unité de la coalition des défenseurs de la vie privée. En entretien, Lionel Maurel a bien identifié NOYB et EDRi comme des alliés. Quant à Epicenter Works, l'ONG autrichienne dont fait partie Walter Hötzendorfer, elle est membre d'EDRi[331] et Christof Tschohl, son président, est membre du Conseil d'administration de NOYB[332]. Enfin, que ce soit sur les sujets évoqués ici ou sur la question du droit au déréférencement et de sa conciliation avec la liberté d'expression – point de désaccord entre EFF et la plupart des ONG européennes d'EDRi – Joe McNamee a insisté en entretien sur le fait qu'il ne se rappelle d'aucune occasion lors de laquelle une association membre d'EDRi ne s'est formellement opposée par un veto à la position de consensus au sein de l'organisation pendant le processus d'adoption du RGPD.

De plus, si le paradigme libéral de la vie privée a inspiré le droit à l'auto-détermination informationnelle, et se traduit d'un côté par l'importance accordée au consentement individuel comme base légale d'un traitement de données, et, de l'autre, par une définition individualiste de la notion de donnée à caractère personnel[333], une partie de la littérature qui s'y rattache

330 Cf. section 2.4.3.
331 Voir la liste actuelle des membres d'EDRi à l'adresse https://edri.org/members/ (page consultée le 30 mai 2019).
332 Voir la composition du Conseil d'administration de NOYB à l'adresse : https://noyb.eu/team/?lang=fr (page consultée le 30 mai 2019).
333 Cf. chapitre 6.

s'intéresse, comme nous l'avons vu[334], à explorer la dimension instrumentale du droit (même exercé individuellement) *à la* vie privée et *à la* protection des données pour garantir l'exercice de droits collectifs et le maintien d'un régime politique démocratique.

D'ailleurs, nous pouvons observer dans cet extrait du discours de Lionel Maurel un raisonnement pour justifier l'existence du droit *à la* vie privée très similaire au raisonnement de John Stuart Mill pour justifier la liberté individuelle dans *De la liberté* (Mill, 1989 [1859]) :

> « Y a pas de liberté d'expression possible s'il n'y a pas de réelle vie privée, […] s'il n'y a pas un espace où la conscience des individus peut rester protégée et où ils peuvent forger leurs opinions sans avoir la peur du jugement, et qu'ils ne puissent pas développer une personnalité, une opinion dissidente, un espace d'expérimentation de principes qui sont pas forcément les normes, et qui peuvent être soumis à jugement. La possibilité d'avoir cet espace-là est nécessaire pour avoir des opinions, et donc est nécessaire pour avoir ensuite une liberté d'expression. » (Entretien avec Lionel Maurel)

Or, le libéralisme de John Stuart Mill est, comme nous l'avons précédemment montré[335], une des principales sources d'inspiration du paradigme libéral de la vie privée.

Enfin, la conception collectiviste et critique à l'égard du caractère perçu comme individualiste du paradigme libéral de la vie privée, s'est effectivement traduite, après l'entrée en application du RGPD en mai 2018, par le refus de la Quadrature du Net de demander au civil la réparation du préjudice subi individuellement par les personnes concernées, au titre des articles 80 et 82 du RGPD, comme l'aurait permis le droit français. À la place, cette association a fait le choix d'introduire une plainte collective auprès de la CNIL, pour demander que soit prononcée une sanction pécuniaire administrative par une autorité publique, qui, versée au budget général de l'État, représenterait symboliquement une forme de dédommagement collectif. Mais il s'agit d'actions qui n'ont pu être menées qu'une fois le RGPD adopté et entré en application, donc après la conclusion de son processus d'adoption.

Pendant ce processus, la principale revendication, qui peut en définitive être rattachée à la critique du consentement individuel traduisant concrètement l'auto-détermination informationnelle, a été celle de l'exigence d'un renforcement des conditions de validité du consentement par scepticisme à l'égard de la base légale du consentement (voir : La Quadrature du Net, 2013), et la suppression de la possibilité d'invoquer son « intérêt légitime » pour traiter des données à caractère personnel sans le consentement libre, préalable, informé et spécifique de la personne concernée.

334 Cf. section 2.2.
335 Cf. section 2.2. et 3.6.

Sur ce thème du consentement, Lionel Maurel a expliqué pourquoi la Quadrature du Net soutenait l'inclusion dans le RGPD d'une définition sur le consentement « libre » différent des définitions et conditions du consentement demandées par la coalition industrielle :

> « En gros, tout le débat, c'était : est-ce qu'on peut vraiment faire confiance à l'individu pour contrôler ses données personnelles ? Est-ce que ça vaut la peine de se battre pour donner un droit de consentir à l'individu ? Ou est-ce que c'est de toutes façons un combat perdu d'avance ? Parce qu'il est tellement porté à accepter des traitements tellement intrusifs, que même si le consentement était recueilli de manière libre, éclairée, spécifique, *et cætera*, ça serait peut-être pas du tout un moyen de protection efficace […]. Et en fait, on a réussi à sortir de ce débat, parce que […] ce que défend la Quadrature c'est surtout la notion de consentement libre, et ça fait consensus chez nous parce que […] le consentement libre, contrairement à ce qu'on pense, c'est pas du tout une notion qui donne un blanc-seing à l'individu pour décider ce qu'il veut de ses données. Au contraire même. C'est-à-dire que là par exemple la condamnation qu'on a obtenue de Google, ce que ça dit, c'est que y a plein de gens qui ont donné leur consentement, qui l'ont peut-être voulu, mais leur consentement n'est pas valable, y compris contre leur volonté à eux. » (Entretien avec Lionel Maurel)

Toujours selon la même personne, expliquant la position de la Quadrature du Net :

> « Dans le droit des données personnelles, par exemple, il y a l'histoire de l'intérêt légitime. Ça c'était un gros débat dans le RGPD. Nous à la Quadrature notre position c'était que ce truc devait être viré complètement. » (Entretien avec Lionel Maurel)

Il faisait ici référence à l'article 6 paragraphe 1 sous f) de la proposition initiale comme du texte final qui, reprenant l'article 7 sous f) de la directive de 1995, devait permettre et permet avec son adoption aux responsables du traitement de collecter et d'utiliser des données à caractère sans le consentement de la personne concernée s'ils ont un « intérêt légitime » à le faire. C'est sur ce fondement que se base par exemple un moteur de recherche l'indexation des pages web contenant des données à caractère personnel sans demander leur accord préalable à chaque personne concernée[336]. Dans ces cas, une personne concernée se voyait accordé à l'article 14 de la directive de 1995, et aujourd'hui à l'article 21 du RGPD, un droit d'opposition au traitement de ses données, dans une logique d'*opt-out*, là où le mécanisme de consentement de l'art. 7 sous a) ou art. 6 §1 sous a) du RGPD répond à une logique d'*opt-in*.

La demande de supprimer l'intérêt légitime de la liste des bases légales de licéité d'un traitement se trouve également formulée dans un document qu'avait produit EDRi :

336 Voir : CJUE 13 mai 2014 « Google contre Espagne », Aff. C-131/12, pts. 73 à 75

Amendment 67
Proposal for a regulation
Article 6 – paragraph 1 – point f

Text proposed by the Commission	*Amendment*
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.	***deleted***

Figure 23 : *Proposition d'amendement 67, extraite d'un* position paper *d'EDRi, en page 52 du document EDRI2 du corpus Lobbyplag*

Selon cette ONG, sa proposition d'amendement se justifiait par le fait que le critère de l'intérêt légitime pourrait être une façon de contourner l'obligation de recueil du consentement :

> « L'ambiguïté du terme "intérêts légitimes" pourrait inciter les responsables du traitement à tenter de justifier la plus grande part possible de leurs traitements sur ce fondement, même s'ils ont la possibilité d'utiliser d'autres fondements, notamment le consentement[337]. » (Corpus Lobbyplag, EDRI2, 2012, p. 52)

Cet amendement n'a pas été retenue par le législateur européen, et l'intérêt légitime du responsable du traitement demeure aujourd'hui l'un des critères de licéité listés à l'article 6 paragraphe 1 du RGPD. Mais nonobstant l'échec de cette dernière revendication, le résultat de débats internes entre défenseurs de la vie privée sur le caractère individuel ou collectif du droit *à la* vie privée et *à la* protection des données à caractère personnel a finalement surtout abouti à un renforcement de l'une des principales mesures concrètes qui traduisent dans le texte du RGPD l'inspiration du paradigme libéral de la vie privée : le consentement. Au terme des « discussions » sur le RGPD, sous la pression des défenseurs de la vie privée, et en comparaison avec l'état du droit ayant précédé cette réforme, le consentement individuel s'en trouve donc considérablement renforcé.

337 Traduit de l'anglais. Texte original : « The vagueness of the term "legitimate interests" would encourage controllers to try to cover as much processing as possible under this ground, even though it could be covered under other grounds, notably consent, as well. »

4.7. Conclusion du chapitre

Les transformations d'ampleur du milieu technique consécutives à la diffusion des ordinateurs en réseaux n'ont pas eu les effets mécaniques sur le droit *de la* protection des données qui lui sont souvent attribués. Le RGPD, qui remplace la directive 95/46/CE, modifie la façon dont les responsables du traitement doivent se conformer au droit *de la* protection des données à caractère personnel par l'introduction de la logique de « *compliance* » et l'introduction d'obligations renforcées pour les traitements à « haut risque[338] ». Il poursuit l'européanisation de ce domaine du droit et des politiques publiques, et relève le seuil des sanctions administratives maximales en cas d'infraction à des niveaux qui se veulent dissuasifs. Dans l'ensemble, il reprend l'essentiel des définitions, principes, et droits pour les citoyens à l'égard des données les concernant, qui étaient déjà présents dans la directive de 1995, qui les a elle-même hérités de la Convention 108 et des Lignes directrices de l'OCDE. Le RGPD s'inscrit donc non pas en rupture, mais en parfaite continuité des développements juridiques en matière de protection de la vie privée et des données à caractère personnel en cours en Europe depuis le début des années 1970.

Du point de vue des arguments échangés dans la controverse qui a accompagné son processus d'adoption, les remises en cause du paradigme libéral de la vie privée par la coalition industrielle a été marginale, et celui-ci a continué à être un point de référence – malgré quelques « nuances » – pour les défenseurs de la vie privée[339]. Plutôt que de le remettre en cause, la coalition industrielle a eu recours à l'argument d'un nécessaire « meilleur équilibre » avec les objectifs de croissance contenus dans le référentiel néolibéral global et transversal aux politiques publiques de l'UE[340].

La coalition de la « *privacy community* » a répondu à cette demande d'« équilibre » avec le même argument de la confiance que celui que les défenseurs de la vie privée utilisaient déjà dans les années 1970[341] : sans confiance de la part des consommateurs et des citoyens, l'on ne peut espérer aucune croissance du marché des services informatiques et du « marché unique numérique » de la stratégie Europe 2020. La coalition industrielle ayant été convaincue par cet argument, ou l'ayant en tout cas concédé, les défenseurs de la vie privée parvinrent avec succès à articuler leurs préoccupations fondées pour l'essentiel sur le paradigme libéral, qui accorde une attention prioritaire aux droits fondamentaux et à la liberté individuelle, au paradigme global accordant la priorité à une « croissance » rendue possible par le passage à une « économie fondée sur les connaissances » d'inspiration néolibérale.

Depuis les années 1970, le référentiel global est passé d'un paradigme productiviste keynésien, où l'État planificateur était le principal consommateur de données à caractère personnel, à un paradigme néolibéral qui a inspiré de nombreuses dérégulations et privatisations, et dans lequel ce sont les entreprises qui, en situation de concurrence libre et non-faussée,

338 Cf. section 4.1.3.
339 Cf. section 4.6.
340 Cf. section 4.4.
341 Cf. section 3.8.

deviennent les moteurs de la croissance à condition d'être libérées du « fardeau » étatique[342]. Mais que ce soit dans le nouveau référentiel global ou dans l'ancien, l'usage de données à caractère personnel y est perçu comme de nature à procurer un bénéfice économique pour le bien commun. Avant, cela devait permettre à l'État planificateur de prendre des décisions plus rationnelles en faveur de la croissance. Aujourd'hui, cela doit permettre aux entreprises d'être plus efficaces, et de faire des découvertes leur permettait d'innover et d'offrir de nouveaux services marchands et de favoriser ainsi la croissance économique en contexte de « société fondée sur la connaissance » selon le langage de la stratégie Europe 2020 de la Commission européenne.

Le paradigme libéral de la vie privée a évolué depuis les années 1970 et 1980 en intégrant des apports des théories foucaldiennes sur la discipline et le pouvoir, tout en restant assez stable sur ses fondements libéraux utilitaristes. Quant à l'argument permettant d'articuler ce référentiel, partagé (dans l'ensemble) par la coalition des défenseurs de la vie privée, au paradigme global, il demeure avec succès celui de la nécessité de garantir la « confiance », qui continue à lui conférer le statut de référentiel sectoriel dans le sous-système de politiques publiques de protection des données de l'Union européenne.

La structure argumentative générale des controverses autour du droit *de la* protection des données à caractère personnel, dans le sous-système de politique publique de la protection des données, au niveau européen (Conseil de l'Europe puis CEE et UE) est donc restée remarquablement stable, ce qui contribue à expliquer la stabilité des dispositions juridiques en vigueur telles que rédigées dans la Convention 108, dans la directive 95/46/CE de 1995, et aujourd'hui dans le RGPD. Nous verrons dans le chapitre 6 si, et dans l'affirmative, de quelle façon, cette stabilité d'ensemble se traduit en particulier par une stabilité dans la rédaction de la définition juridique de la notion de « donnée à caractère personnel », ainsi que le suggèrent nos hypothèses 3 et 4.

Les arènes de délibération des standards techniques d'Internet et du Web ont également hébergé des discussions sur la protection de la « vie privée » qui se sont déroulées majoritairement en parallèle des « discussions » sur le RGPD. À l'inverse des institutions de l'UE et des groupes d'intérêt que nous venons d'étudier, elles sont surtout composées d'acteurs socialisés à l'informatique et à l'ingénierie. Dès lors, si l'hypothèse 1, selon laquelle il existe des conceptions différentes du droit *à la* vie privée et/ou *à la* protection des données à caractère personnel entre les juristes d'une part, et les informaticiens d'autre part, se vérifiait, nous pourrions nous attendre à ce que la la structure des débats, les référentiels en présence et les arguments échangés y soient différents de ceux que nous avons observés dans ce chapitre et dans le précédent. Or, comme nous allons maintenant le voir, même s'il existe en effet quelques différences (essentiellement lexicales) dues notamment à une structuration et une composition différentes des arènes, notre hypothèse initiale (l'hypothèse 1) en surestimait considérablement la portée.

342 Cf. sections 3.8., 4.4. et 4.6.

Chapitre 5 : La « *privacy* » dans la production des standards techniques du Web

5.1. Introduction

La conception libérale de la vie privée que nous avions identifiée et présentée dans le chapitre deux n'est qu'une façon parmi d'autres d'envisager la « vie privée » et la question des données à caractère personnel. Son rôle dans la construction de la protection des données comme problème public dans les années 1960 et 1970[1], puis lors des « discussions » sur le RGPD entre 2009 et 2016[2], lui a néanmoins conféré un statut paradigmatique particulier dans les politiques publiques européennes de protection des données à caractère personnel. Elle a également joué un rôle de ciment pour la coalition de cause des défenseurs de la vie privée, ou « *privacy community* ».

Les personnes qui, au sein des organismes de la gouvernance d'Internet, se mobilisent en faveur de la « *privacy* » et de sa protection par des standards techniques dont les dispositions sont, en cas de succès, répercutées sur les couches logicielles et matérielles des réseaux de communication électroniques, partagent-ils la même conception de la « vie privée » ? Ont-ils les mêmes valeurs, les mêmes discours et arguments, le même système de conviction que les défenseurs de la vie privée que nous avons étudiés dans les deux précédents chapitres ? Font-ils face aux mêmes arguments venant d'une coalition industrielle identique à celle qui participa aux « discussions » sur le RGPD ? Leur ont-ils opposé les mêmes contre-arguments, les mêmes stratégies d'articulation de leur référentiel au référentiel global ?

Comme les arènes de standardisation d'Internet sont, dans leur écrasante majorité, composées d'ingénieurs informaticiens, notre première hypothèse tendrait à nous faire supposer que la réponse à toutes ces questions est négative. De plus, la littérature sur les controverses nous apprend que lorsqu'elle passe d'une arène à une autre, une controverse a tendance à être transformée, reconfigurée (Dodier, 1999 ; Ollivier-Yaniv, 2018, à paraître). D'ailleurs, tant la nature des documents produits par les organismes de standardisation d'Internet que le vocabulaire qui y est employé paraissent provenir d'un tout autre monde que ce que nous observions sur les terrains présentés dans les deux précédents chapitres. « *Tracking* », « *fingerprinting* » sont tout aussi absents du RGPD que les mots « principe de limitation des finalités » le sont des standards de l'*Internet Engineering Task Force* (IETF) ou du *World Wide Web Consortium* (W3C).

1 Cf. chapitre 3.
2 Cf. chapitre 4.

Pourtant, à y regarder de plus près, les systèmes de convictions motivant les défenseurs de la vie privée du W3C, principal organisme de standardisation du Web (Sire, 2017), ne sont pas sans rappeler ceux que nous avons observés dans les discours des experts du Conseil de l'Europe, de l'OCDE, ou encore de la coalition de la « *privacy community* » dans les « discussions » sur le RGPD. Derrière des mots différents, il y a souvent un sens identique ou similaire. Ainsi, le terme d'« auto-détermination informationnelle » des juges du Tribunal constitutionnel fédéral de RFA devient « contrôle utilisateur » (« *user control* ») dans le vocabulaire des membres du *Privacy Interest Group* du W3C. Les mots sont différents, mais le sens, nous le verrons, est sensiblement identique.

La nature non-étatique et souvent informelle d'organismes comme l'IEEE, l'IETF ou le W3C, qui ne produisent pas de droit dur au sens de règles de droit positif assorties de mécanismes de sanction en cas d'infraction, font qu'il serait impropre de parler de « politiques publiques » *stricto sensu* pour parler de son action. Les contraintes matérielles et discursives qui pèsent sur les arènes du W3C, l'organisme sur lequel nous avons centré notre enquête de terrain, sont différentes de celles du Conseil de l'Europe, de l'OCDE, ou du sous-système de politiques publiques de l'Union européenne de protection des données. Si l'IETF ou le W3C sont un lieu de production d'action publique (au sens plus large, donc, que les « politiques publiques »), où sont rédigés des textes normatifs et performatifs qui sont une forme de « droit souple » intégrés à une *Lex Informatica* (Reidenberg, 1997), l'ACF et les théories cognitives des politiques publiques nous ont parues utiles mais incomplètes pour y étudier les controverses qui s'y déroulent. Des éléments issus de la littérature en sociologie des techniques et des sciences et en *Internet Studies* nous ont aidé à compléter notre cadre théorique général pour l'étude de ce terrain.

Le présent chapitre commence donc par une présentation des organismes de gouvernance d'Internet et par quelques éléments de théorie et de méthode nous ayant permis d'y enquêter. Nous décrirons ensuite avec plus de détails le *Privacy Interest Group* (PING) et le *Tracking Protection Working Group* (TPWG) du W3C, sur lesquels notre terrain s'est concentré, et qui résultent d'une histoire de la « *privacy* » au sein du W3C que nous exposerons pour comprendre l'historique des controverses actuelles. Puis nous détaillerons en quoi l'impératif de consensus propre au mode de gouvernance et de standardisation d'Internet impose des contraintes discursives particulières à la controverse que nous voulons étudier, qui doivent être prises en compte pour pouvoir procéder à l'analyse des discours observés sur le terrain, à la fin du chapitre.

5.2. Les arènes de la gouvernance d'Internet et les standards techniques

5.2.1. La gouvernance d'Internet

> « The Internet is governed[3]. » (DeNardis, 2014, p. 222)

Allant à l'encontre de nombreux préjugés sur l'Internet comme espace de liberté intrinsèquement anarchique et ingouvernable, Laura DeNardis démontre avec conviction qu'Internet fait bel et bien l'objet d'une gouvernance et ce, même si cette gouvernance n'est pas le fait d'une réglementation au sens habituel (et classiquement juridique) du terme :

> « Les points de contrôle de la gouvernance de l'Internet ne sont ni juridiques, ni confinés aux frontières de l'État-nation. Ils sont souvent matérialisés par la conception d'architectures techniques, par les décisions d'organes internationaux de la gouvernance de l'Internet, ou par les politiques d'entreprises privées, qui constituent ensemble des forces transcendantes en flux permanent et en conflit permanent avec les systèmes juridiques nationaux, les traités intergouvernementaux, et les normes culturelles régionales[4]. » (DeNardis, 2014, p. 222)

Il n'est pas inutile de se pencher sur la notion de « gouvernance » pour comprendre la distinction entre les modalités classiques et étatiques de gouvernement par la réglementation, que nous avons étudiées dans les chapitres analysant la politique publique européenne de protection des données à caractère personnel, et une « gouvernance » qu'il reste donc à définir.

L'usage du terme « gouvernance » est devenu très répandu, y compris dans le répertoire courant des hommes et femmes politiques. Il en existe de nombreuses acceptions, qui rendent une définition rigoureuse difficile (Chevallier, 2003). Il peut être utilisé comme synonyme de « gouvernement », mais c'est justement la distinction entre « gouvernement » et « gouvernance » qui nous intéresse. Pourquoi parler de « gouvernance » d'Internet et non de « gouvernement », au

3 Traduction par l'auteur : « L'Internet est gouverné. »

4 Traduit de l'anglais. Texte original : « Internet governance control points are not legal control points, nor are they confined within nation-state boundaries. They are often manifested through the design of technical architecture, the decisions of global institutions of Internet governance, or the policies of private companies, all globally transcending forces in constant flux and in constant tension with national legal systems, inter-governmental treaties, and regional cultural norms. »

sens non pas de l'institution, mais de l'action de gouverner ? La gouvernance est-elle une action de gouverner ? Dans l'affirmative, alors en quoi diffère-t-elle du gouvernement ?

Milton Mueller résume en une courte phrase la définition qu'en font James Roseneau et Ernst-Otto Cziempel (Rosenau et Czempiel, 2009 [1992]) :

> « Le terme de *gouvernance*[5] […] a gagné du terrain dans les relations internationales justement parce que c'est un terme plus faible que celui de *gouvernement*[6] *;* il dénote la coordination et la régulation par des acteurs interdépendants, en l'*absence*[7] d'une autorité politique globale supérieure[8]. » (Mueller, 2010, p. 8)

Sa généalogie remonte aux travaux de l'École de Chicago pour théoriser les mécanismes de coordination des activités économiques notamment pour parler de « gouvernance d'entreprise » (Chevallier, 2003). Popularisée à partir du tournant néolibéral des années 1980 marquant un reflux de l'État, « il servira à rendre compte des nouvelles formes d'organisation d'une société internationale de plus en plus fragmentée et hétérogène » (Chevallier, 2003, p. 205).

La gouvernance s'oppose à la bureaucratie classique décrite par Max Weber (Weber, 2003 [1921]), qui repose sur un principe hiérarchique, la rationalisation des processus administratifs, et une domination de type « légale-rationnelle ». Celle-ci repose également « sur une certaine conception du pouvoir, caractérisée par l'asymétrie, l'inégalité, l'unilatéralité, c'est-à-dire donnant la capacité à celui qui le détient d'imposer sa volonté au destinataire » (Chevallier, 2003, p. 206). C'est cette bureaucratie weberienne qui est désignée par « gouvernement » lorsque celui-ci s'oppose à la « gouvernance ». Elle est liée à la notion d'État comme « puissance suprême de domination » (Chevallier, 2003, p. 206).

Internet ne fait pas l'objet d'un gouvernement. Bien entendu, il existe des lois qui s'appliquent à des personnes dans le cadre de leurs activités en ligne, comme par exemple le RGPD. Mais comme le rappelle la formule « *Code is Law* » de Lawrence Lessig (Lessig, 2000), Internet et ses différentes applications (web, e-mails, services de voix sur IP, etc.) sont régulés plus par l'infrastructure matérielle et sa configuration (en particulier sa configuration logicielle, et donc des codes sources) que directement par des lois ou des décisions gouvernementales :

---

5 En italique dans le texte.
6 *Idem*
7 *Idem*
8 Traduit de l'anglais. Texte original : « The term *governance* […] gained currency in international relations precisely because it was weaker than *government* ; it denotes the coordination and regulation of interdependent actors in the *absence* of an overarching political authority. »

> « La coexistence de sources de normalisation technique et de sources traditionnelles législatives et juridiques donne naissance à une gouvernance internautique multi-acteur et multi-niveau, caractérisée par la présence de plusieurs centres de régulation de nature différente ainsi que par la juxtaposition de plusieurs « couches » normatives. » (Belli, 2016, p. 157)

La configuration de l'infrastructure matérielle de l'Internet engendre des effets sur la répartition du pouvoir entre différents acteurs. Françoise Massit-Folléa a par exemple montré comment le coût de l'accès aux points d'appairage connectant les différents réseaux constituant Internet entre eux et leur répartition géographique organisaient une hiérarchie entre fournisseurs d'accès à Internet (Massit-Folléa, 2014) au détriment des pays en voie de développement, ce qui renforce la dépendance de la périphérie à l'égard du centre du système-monde (Wallerstein, 2009).

Jonathan Zittrain parle de « points de contrôle » pour désigner des dispositifs techniques dont le contrôle permet de diriger le comportements des usagers des technologies informatiques (Zittrain, 2003). Les routeurs des fournisseurs d'accès à Internet permettant de diriger les paquets transitant sur Internet d'un réseau à l'autre jusqu'à son destinataire sont un exemple de points de contrôle. Un autre exemple est le serveur racine du système *Domain Name System* (DNS) qui permet à un internaute d'accéder à un site web en utilisant un nom de domaine (comme www.utc.fr) au lieu d'avoir apprendre à connaître l'adresse IP du serveur web du site en question (195.83.155.24). L'*Internet Corporation for Assigned Names and Numbers* (ICANN), une association à but non lucratif de droit californien, en assure un contrôle monopolistique de fait au niveau mondial (Belli, 2016).

La définition de la gouvernance d'Internet proposée à Laura DeNardis, à laquelle nous adhérons, est la suivante :

> « La gouvernance d'Internet porte généralement sur des technologies propres à l'Internet, et traite d'interopérabilité entre les appareils [*devices*] et de gestion des flux d'informations en réseau entre ces appareils[9]. » (DeNardis, 2014, p. 22)

5.2.2. Des standards techniques normatifs et performatifs

Romain Badouard, Clément Mabi et Guillaume Sire (Badouard, Mabi et Sire, 2016) rappellent que le régime de gouvernementalité propre à l'Internet ne se base pas uniquement sur

9 Traduit de l'anglais. Texte original : « Internet governance usually addresses technologies that are unique to the Internet and deal with interoperability among devices and the management of networked information flows between these devices. »

ces points de contrôle matériels, mais aussi sur des logiciels comme les Content Management Systems (CMS) ou les systèmes d'exploitation, qui, en définissant et en encadrant l'action des utilisateurs, forment un « architexte » qui encadre des pratiques communicationnelles (Souchier et Jeanneret, 2001). Bien qu'en informatique, le matériel (*hardware*) soit distingué du logiciel (*software*), il ne faut pas oublier que les logiciels sont des inscriptions machiniques agissantes sur un support matériel. Certains logiciels ont une incidence directe sur la circulation des contenus qui transitent par l'infrastructure de communication qu'est le réseau des réseaux.

Ainsi, une part importante de l'activité de la gouvernance d'Internet réside dans la délibération et l'adoption de documents qui décrivent de façon normative la façon dont les ordinateurs doivent communiquer entre eux pour être interopérables, c'est-à-dire compatibles.

Comme rappelé par Laura DeNardis : « Internet fonctionne parce qu'il se base sur un langage technique universel[10] » (DeNardis, 2014, p. 65). C'est la condition indispensable à ce que des ordinateurs de constructeurs divers puissent se transmettre des informations à travers plusieurs réseaux interconnectés, et pour que ces informations s'affichent de façon similaire et cohérente sur cette diversité de terminaux électroniques. Les logiciels, y compris ceux qui jouent un rôle d'architexte, qui n'obéiraient pas à l'important corpus de normes techniques définissant les modalités de cette transmission d'information, ne pourraient pas se connecter à Internet. Il a d'ailleurs existé un grand nombre de protocoles concurrents aux protocoles de base d'Internet que sont le *Transmission Control Protocol* (TCP) et l'*Internet Protocol* (IP), comme le X.25 du Minitel français. Les terminaux équipés pour utiliser ces protocoles concurrents ne peuvent pas se connecter à Internet.

Les différents logiciels capables de structurer des communications électroniques en TCP et en IP n'utilisent pas de *logiciel* TCP ou IP, mais respectent un strict cahier des charges qui est décrit dans des documents, dans des standards techniques. L'*Internet Engineering Task Force* (IETF) définit la notion de « standard » dans deux de ses *Requests For Comments* (RFC) : la RFC 2026, qui définit le processus d'adoption d'un standard, et la RFC 3935, qui fait office de charte à cette organisation, et dont la définition est un peu plus normative que la première :

> « En général, un standard Internet est une spécification stable et bien comprise, techniquement compétente, disposant d'implémentations multiples, indépendantes et interopérables, avec une expérience opérationnelle substantielle, bénéficiant d'un soutien public fort, et pouvant être reconnue comme utile dans tout ou partie de l'Internet[11]. »

10 Traduction de l'auteur. Texte original : « Internet works because it is based on a universal technical language. »

11 Traduit de l'anglais. Texte original : « In general, an Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all

(RFC 2026)

> « Standard : ce terme, tel qu'il est utilisé ici, décrit la spécification d'un protocole, d'un comportement système ou d'une procédure qui a un identifiant unique, et pour lesquels l'IETF s'est accordé à dire que « si vous souhaitez faire cette chose, voici la description de la manière dont vous devez le faire ». Cela n'implique pas de tentative de l'IETF d'imposer ou de surveiller leur utilisation – mais simplement : « si vous dites que vous faites cela selon tel standard, faites-le de cette manière ». L'avantage d'un standard pour l'Internet est dans son interopérabilité : plusieurs produits mettant en œuvre un standard peuvent travailler ensemble afin de proposer de précieuses fonctionnalités aux utilisateurs de l'Internet[12]. » (RFC 3935)

En d'autres termes, un standard, dans le contexte de la gouvernance d'Internet, est un instrument assimilable selon nous à une forme de droit souple, qui décrit de façon normative la façon dont doivent communiquer ensemble des ordinateurs afin de permettre à Internet de conserver ses propriétés d'interopérabilité. La sanction en cas d'infraction n'est pas de nature étatique, mais elle peut aboutir à une exclusion *de facto* du réseau de réseaux.

Une des applications d'Internet, le web, repose pour l'essentiel sur les standards techniques définis par le World Wide Web Consortium (W3C) (Sire, 2017), sauf en ce qui concerne le protocole *Hypertext Transfer Protocol* (HTTP) lui-même, qui est défini au sein de l'IETF dont la logistique est assurée par l'*Internet Society* (ISOC). Ce protocole, qui permet à un navigateur web de demander à un serveur web qu'il lui transfère le contenu d'une page, est codifié pour sa version 1.1 dans le document RFC 2616.

Les standards de l'IETF sont codifiés dans des documents appelés *Requests for Comments*, ou RFC, suivis d'un numéro qui suit un ordre chronologique. Le terme employé au W3C est celui de « recommandation », mais il s'agit du même type de document.

Les RFC suivantes sont quelques uns des exemples les plus connus de RFC décrivant des standards d'Internet :

---

parts of the Internet. »

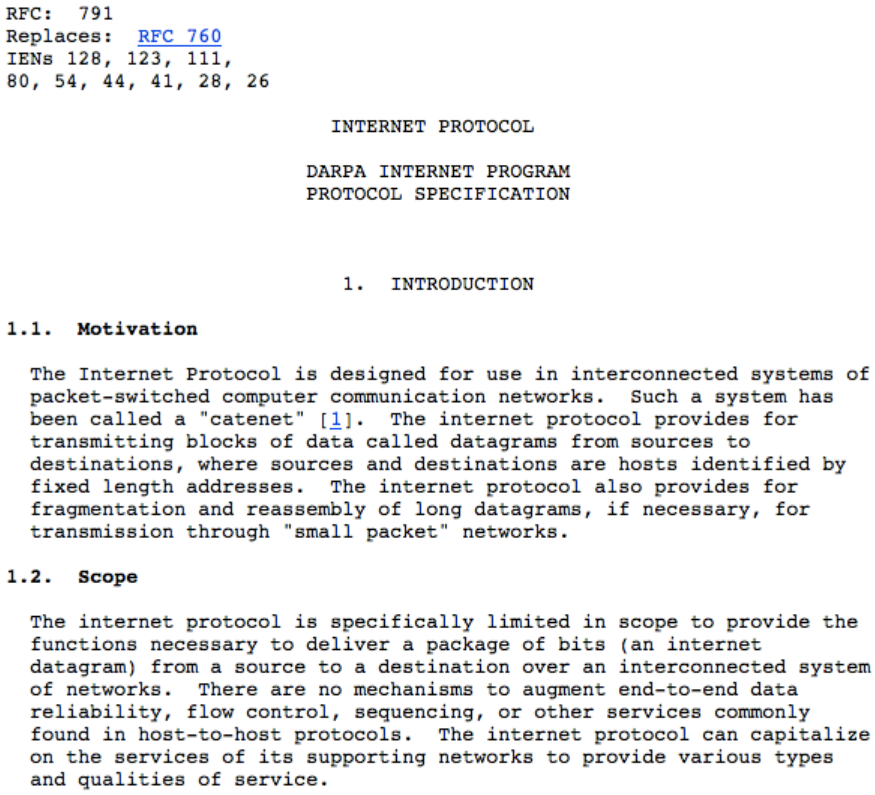
12 Traduit de l'anglais. Texte original : « Standard: As used here, the term describes a specification of a protocol, system behaviour or procedure that has a unique identifier, and where the IETF has agreed that "if you want to do this thing, this is the description of how to do it". It does not imply any attempt by the IETF to mandate its use, or any attempt to police its usage - only that "if you say that you are doing this according to this standard, do it this way". The benefit of a standard to the Internet is in interoperability - that multiple products implementing a standard are able to work together in order to deliver valuable functions to the Internet's users. »

RFC	Nom	Date	Description
RFC 20	ASCII format for Network Interchange	1969	Format standard d'encodage de l'alphabet latin sans signes diacritiques (utilisé par exemple le système d'exploitation MS-DOS)
RFC 768	User Datagram Protocol (UDP)	1980	Assurer la communication des paquets entre deux adresses IP
RFC 791	Internet Protocol version 4 (IPv4)	1981	Les adresses IPv4 sont des adresses qui permettent d'identifier un ordinateur sur un réseau. Par exemple, son propre ordinateur est toujours 127.0.0.1.
RFC 793	Transmission Control Protocol (TCP)	1981	Permet la communication entre deux adresses IP en s'assurant de la connection entre les deux ordinateurs
RFC 937	Post Office Protocol	1985	Un des protocoles de base permettant d'échanger des e-mails
RFC 959	File Transfer Protocol (FTP)	1985	Permet de télécharger des documents vers et depuis un ordinateur distant
RFC 1034 et RFC 1035	Domain Name System (DNS)	1987	Décrit le fonctionnement de la résolution des noms de domaine
RFC 1459	Internet Relay Chat Protocol (IRC)	1993	Protocole de messagerie instantanée en ligne, précurseur de services comme AIM ou Microsoft Messenger
RFC 2460	IPv6	1998	Nouvelle façon de former des adresses IP, pour faire face à la diminution des stocks d'adresses IP version 4 disponibles

Tableau 12 : *Tableau de présentation d’une sélection de RFC de l’IETF*

Ces standards techniques sont régulièrement mis à jour, une RFC pouvant en abroger ou en amender une précédente.

Du point de vue de sa forme, une RFC est un document qui décrit d'abord l'objectif de la norme (exemple avec la RFC 791 qui définit les adresses IP) :



RFC: 791
Replaces: RFC 760
IENs 128, 123, 111,
80, 54, 44, 41, 28, 26

INTERNET PROTOCOL

DARPA INTERNET PROGRAM
PROTOCOL SPECIFICATION

1. INTRODUCTION

1.1. Motivation

The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. Such a system has been called a "catenet" [1]. The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks.

1.2. Scope

The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system of networks. There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols. The internet protocol can capitalize on the services of its supporting networks to provide various types and qualities of service.

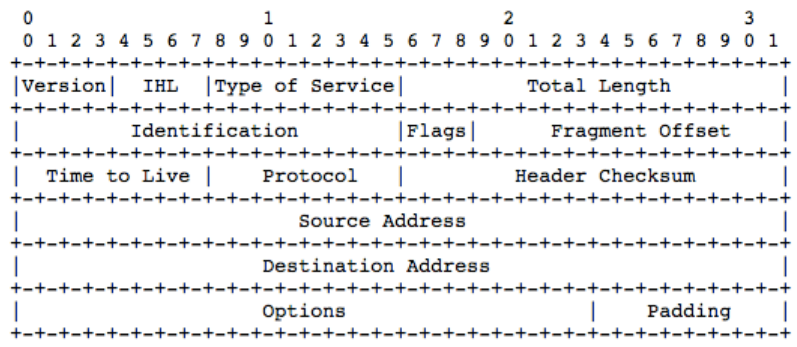
Figure 24 : *Premier extrait de capture d'écran de RFC 791 visible sur le site de l'IETF depuis la page https://tools.ietf.org/html/rfc791 (page web consultée le 10 mai 2018)*

Suit une description de la façon dont un protocole doit fonctionner (toujours extrait de la RFC 791) :

3. SPECIFICATION

3.1. Internet Header Format

A summary of the contents of the internet header follows:



Example Internet Datagram Header

Figure 4.

Note that each tick mark represents one bit position.

Version: 4 bits

The Version field indicates the format of the internet header. This document describes version 4.

IHL: 4 bits

Internet Header Length is the length of the internet header in 32 bit words, and thus points to the beginning of the data. Note that the minimum value for a correct header is 5.

Figure 25 : *Deuxième extrait de capture d'écran de RFC 791 visible sur le site de l'IETF depuis la page https://tools.ietf.org/html/rfc791 (page web consultée le 10 mai 2018)*

Ce n'est qu'en respectant cette description normative que deux ordinateurs pourront communiquer entre eux sur le réseau Internet. D'autres documents de l'IETF sont plutôt des déclarations politiques, et ne sont pas intégrés à des standards en tant que tel, comme par exemple la RFC 1087 « *Ethics and the Internet* » :

Network Working Group
Request for Comments: 1087

Internet Activities Board
January 1989

Ethics and the Internet

Status of this Memo

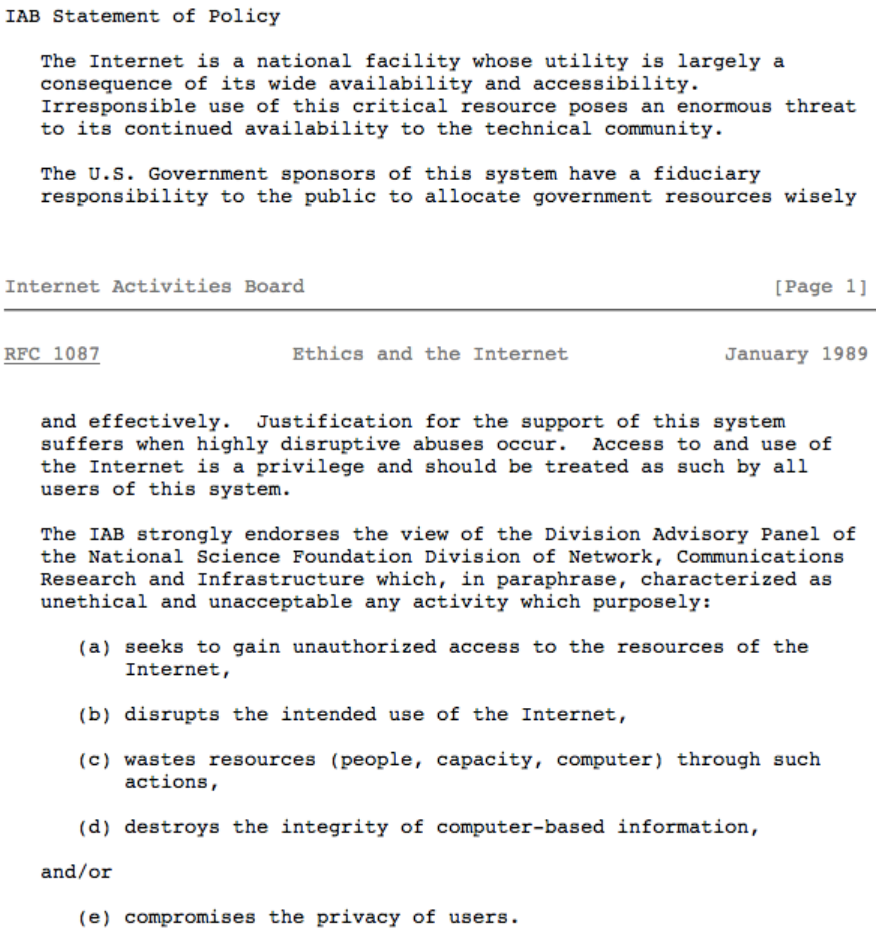
This memo is a statement of policy by the Internet Activities Board (IAB) concerning the proper use of the resources of the Internet. Distribution of this memo is unlimited.

Introduction

At great human and economic cost, resources drawn from the U.S. Government, industry and the academic community have been assembled into a collection of interconnected networks called the Internet. Begun as a vehicle for experimental network research in the mid-1970's, the Internet has become an important national infrastructure supporting an increasingly widespread, multi-disciplinary community of researchers ranging, inter alia, from computer scientists and electrical engineers to mathematicians, physicists, medical researchers, chemists, astronomers and space scientists.

As is true of other common infrastructures (e.g., roads, water reservoirs and delivery systems, and the power generation and distribution network), there is widespread dependence on the Internet by its users for the support of day-to-day research activities.

The reliable operation of the Internet and the responsible use of its resources is of common interest and concern for its users, operators and sponsors. Recent events involving the hosts on the Internet and in similar network infrastructures underscore the need to reiterate the professional responsibility every Internet user bears to colleagues and to the sponsors of the system. Many of the Internet resources are provided by the U.S. Government. Abuse of the system thus becomes a Federal matter above and beyond simple professional ethics.



IAB Statement of Policy

The Internet is a national facility whose utility is largely a consequence of its wide availability and accessibility. Irresponsible use of this critical resource poses an enormous threat to its continued availability to the technical community.

The U.S. Government sponsors of this system have a fiduciary responsibility to the public to allocate government resources wisely

Internet Activities Board [Page 1]

RFC 1087 Ethics and the Internet January 1989

and effectively. Justification for the support of this system suffers when highly disruptive abuses occur. Access to and use of the Internet is a privilege and should be treated as such by all users of this system.

The IAB strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure which, in paraphrase, characterized as unethical and unacceptable any activity which purposely:

(a) seeks to gain unauthorized access to the resources of the Internet,

(b) disrupts the intended use of the Internet,

(c) wastes resources (people, capacity, computer) through such actions,

(d) destroys the integrity of computer-based information,

and/or

(e) compromises the privacy of users.

Figure 26 : *Extraits de capture d'écran de RFC 1087 visible sur le site de l'IETF depuis la page https://tools.ietf.org/html/rfc791 (page web consultée le 11 mai 2018)*

Il existe une rhétorique particulière des documents de l'IETF, parfois reprise par d'autres arènes de standardisation. Ainsi, la RFC 2119, conjointement avec la RFC 8174, imposent un usage précis des termes anglais « MUST », « MUST NOT », « REQUIRED », « SHALL », « SHALL NOT », « SHOULD », « SHOULD NOT », « RECOMMENDED », « MAY », et « OPTIONAL », lorsque ceux-ci sont écrits en lettres majuscules. Utilisé par le RFC, ce lexique particulier est repris également dans un certain nombre de documents du W3C, comme le *Process Document* (W3C Process) mais pas par tous.

Voici un extrait de la RFC 2119 :

« 1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label[13]. » (RFC 2119)

Ces documents, qu'il s'agisse de standards de l'IETF ou encore de recommandations du W3C, sont des textes qui visent à décrire de façon normative la façon dont Internet (ou, pour le W3C, le web), *devrait* fonctionner. Ce corpus constitue, avec les choix de configuration des systèmes informatiques, ce que Joel Reidenberg appelle la *Lex Informatica* (Reidenberg, 1997) :

« Les capacités techniques et les choix de conception système imposent des règles aux participants. La création et la mise en œuvre de politiques d'information sont embarqués dans [*embedded in*] le design et les standards des réseaux ainsi que dans les configurations système. Même les préférences des utilisateurs et les choix techniques créent des règles locales par défaut supérieures [*overarching*]. Le présent article défend essentiellement l'idée que l'ensemble de règles qui s'appliquent aux flux d'information imposées par la technologie et les réseaux de communication forment une "Lex Informatica" que les décideurs publics doivent comprendre, consciemment reconnaître, et encourager[14]. » (Reidenberg, 1997, p. 554-555)

13 Traduction : « 1. DOIT Ce mot, ou les termes « EXIGE » ou « SERA », signifient que la définition est une condition absolue de la spécification.
2. NE DOIT PAS Cette expression, ou l'expression « NE SERA PAS », signifient que la définition est une interdiction absolue de la spécification.
3. DEVRAIT Ce mot, ou l'expression « EST RECOMMANDÉ », signifient qu'il peut exister des raisons valables, dans des circonstances précises, d'ignorer un élément en particulier, mais les implications dans leur ensemble doivent être bien comprises et soigneusement mesurées avant de choisir de procéder différemment.
4. NE DEVRAIT PAS Cette expression, ou l'expression « N'EST PAS RECOMMANDÉ », signifient qu'il peut exister des raisons valables, dans des circonstances précises, pour que le comportement soit acceptable ou même utile, mais que les implications dans leur ensemble doivent être bien comprises et soigneusement mesurées avant d'exécuter tout comportement décrit sous cette désignation. »
Traduction donnée à titre indicatif. Le texte original en anglais a été gardé dans le corps du texte car les termes « must », « should », « shall » ou encore « should » n'ont pas de traduction parfaite en français.

14 Traduit de l'anglais. Texte original : « Technical capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations. Even user preferences and technical choices create overarching, local default rules. This Article argues, in essence, that the set of rules for information flows imposed by technology and communication networks form a "Lex Informatica" that policymakers must understand, consciously recognize, and encourage. »

Les choix faits lors de la rédaction de ces conventions techniques qui permettent l'interopérabilité des logiciels et des matériels sur Internet conditionnent des possibilités d'action pour ses utilisateurs. Par exemple, le passage de la norme HTTP au HTTP Secure (HTTPS) avec la RFC 2818 permet le chiffrement des communications entre l'ordinateur du client (de l'internaute) et celui du serveur (contenant le site web) . Combiné avec d'autres outils, HTTPS permet de vérifier l'identité du site sur lequel le client se connecte. Cela permet de compliquer – sans pour autant rendre impossible – des attaques de type « *Man In The Middle* » qui permettent à un intermédiaire dans la chaîne de nœuds acheminant les paquets entre le client et le serveur de lire les échanges en clair (Callegati, Cerroni et Ramilli, 2009). Ce qui explique les efforts de la NSA pour affaiblir la fiabilité de ce protocole (Ball, Borger et Greenwald, 2013).

L'adoption d'un standard crée une forte dépendance au sentier, au sens de Paul Pierson (Pierson, 2000). En effet, une fois inscrits dans des standards, il devient très difficile et coûteux de faire évoluer le système (DeNardis, 2014, p. 65). Cela n'est pas propre, d'ailleurs, aux standards liés aux NTIC. Le clavier QWERTY, inventé en 1868, continue par exemple à être le standard dominant sur le marché alors même qu’une autre disposition inventée par August Dvorak a été conçue pour pouvoir taper plus vite (Lenert, 2004, p. 244). Pour revenir à Internet, Vinton Cerf et Robert Kahn inventèrent le TCP pour remplacer l'ancien *Network Control Protocol* (NCP) d'Arpanet et faciliter le développement des interconnexions qui devaient donner naissance à Internet au milieu des années 1970. Sa première publication remonte à 1974, dans la RFC 675. Il fallut attendre 1983 pour que le protocole TCP remplace définitivement le NCP (Bing, 2009, p. 27). Les tourments actuels du protocole IPv6, dont l'adoption généralisée se fait toujours attendre malgré les appels répétés de l'ICANN, de l'ISOC et d’autorités de contrôle comme l’Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) française, montre que cette dépendance au sentier est toujours très forte (Benhamou, 2019).

Mais même l'adoption initiale d'un protocole remplissant une fonction nouvelle n'est pas toujours une chose aisée, puisqu'elle repose sur l'adoption volontaire par un nombre maximal d'acteurs du système technique visé. L'histoire du protocole HTTP illustre bien cette double difficulté : difficulté d'adoption, puis dépendance au sentier.

Le terme « hypertexte » est une référence directe au même terme, employé par Ted Nelson décrivant son projet « Xanadu » dans *Computer Lib* (Nelson, 1983), lui-même inspiré du projet de « Memex » de Vannevar Bush (Bush, 1965), une machine qui devait permettre à un utilisateur de lier plusieurs contenus textuels de sorte à créer des « sentiers » (*trails*) permettant d'aller d'un texte à un autre.

C'est exactement ce que permet le lien hypertexte, qui, inséré dans le texte d'une page web, permet en un clic d'aller sur une autre page web. En allant de page en page, l'internaute navigue le long d'un « sentier » tracé pour lui par les multiples concepteurs des pages web qu'il

lit. À chaque clic sur un lien, le navigateur émet une requête HTTP transmise à l'ordinateur qui contient la page web demandée, la requête HTTP étant elle-même encapsulée dans un paquet TCP/IP pour permettre aux ordinateurs entre celui de l'utilisateur et le serveur de transférer les données aux bons destinataires.

Tim Berners-Lee inventa le protocole HTTP avec le web autour de l'année 1990 pour répondre à des besoins d'indexation et d'accessibilité de l'information de son employeur : le Centre européen de recherche nucléaire (CERN) (Berners-Lee, 1989). La plus ancienne version publiée, la version 0.9, date de 1991. Puis, sa normalisation fut confiée à l'IETF, qui publia en 1996 la RFC 1945. À cette époque, il existait d'autres protocoles semblables, eux aussi compatibles avec TCP/IP, comme le protocole Gopher, défini en 1993 dans la RFC 1436. Des travaux de Christopher Cal Lee montrent que le protocole HTTP a dépassé en utilisation celle du protocole Gopher à partir du milieu de l'année 1994. Le Web entama alors une croissance exponentielle, qui a progressivement éclipsé tous ses concurrents, comme le Minitel français.

Le protocole HTTP présente toutefois le défaut d'être peu sécurisé. Dès les années 1990, des efforts sont donc entrepris pour faire évoluer ce standard. C'est là qu'entre en jeu le HTTPS, qui permet le chiffrement de la communication entre le client et le serveur. Or, entre la publication du premier brouillon de RFC standardisant le protocole HTTPS en janvier 1998, l'adoption de la norme en mai 2000 (RFC 2818), et le moment où, en 2018, Google annonce que son navigateur Chrome affichera un message d'alerte de sécurité à chaque fois qu'un internaute va sur un site resté au protocole HTTP (Schechter, 2018), une vingtaine d'années se sont écoulées. Même aujourd'hui, il ne serait pas envisageable pour un fabricant de navigateur web de désactiver entièrement le protocole HTTP, car les sites web ne prenant pas en charge le HTTPS sont encore trop nombreux.

Cet exemple illustre les conditions particulières de réussite de la performativité des textes des standards d'Internet. Selon Luca Belli :

> « Bien que la *lex informatica* n'ait pas les caractéristiques formelles d'une loi, on se doit de remarquer son évidente valeur normative. D'une part, les protocoles et les standards exercent un effet régulateur sur les comportements des [internautes], tandis que, d'autre part, ils atteignent leur but de façon particulièrement efficace puisque la liberté de l'internaute est précisément délimitée par l'architecture cyberspatiale. Cela est dû au fait que […], le code qui met en œuvre la *lex informatica* est « auto-exécutoire », ce qui transforme la *lex informatica* en un vecteur normatif performatif, qui ne nécessite pas du support d'une entité tierce pour être appliquée. » (Belli, 2016, p. 143)

L'usage que fait Luca Belli du terme « lex informatica » diffère de celui de son inventeur, Joel Reidenberg, en introduisant une séparation utile, que nous reprenons à notre compte. Il existe en effet :

- La *Lex Informatica* à proprement parler, constituée par le corpus de textes à visée normative et reposant sur des mécanismes de performativité que sont les standards d'Internet ;
- Les codes sources des logiciels qui obéissent aux règles contenues dans la *Lex Informatica*, auxquels Lawrence Lessig fait référence lorsqu'il affirme que « *Code is Law* » (Lessig, 2000).

Lorsqu’un code source est compilé ou interprété, un processus automatique de transformation aboutit à un jeu d’instructions exécutables par le microprocesseur de l’ordinateur. Ces jeux d’instructions peuvent être représentés dans un langage appelé *Assembleur*, ou langage machine, dont la maîtrise est plus coûteuse en efforts et en temps que celle du langage dit de haut niveau dans lequel le code source du logiciel est rédigé. Il n’en demeure pas moins que le logiciel est d’abord un texte, contenant une série d’instructions. Un logiciel ne décrit pas une réalité ; son écriture transforme la réalité par la création de nouvelles possibilités d’action et d’un objet nouveau, inscrit sur support numérique. Écrire un code source, c’est effectuer un acte de parole.

Le logiciel porte en lui la promesse de la réalisation d’un jeu d’instructions écrites : l’affichage d’un texte, l’impression d’un document, la connexion à un serveur distant… Même si l’on écarte, par souci de simplification, la possibilité pourtant bien réelle d’une erreur de programmation, c’est-à-dire d’une mauvaise traduction en langage de programmation de l’intention du développeur, il faut prendre en compte le fait qu’un logiciel s’inscrit toujours dans un ensemble intertextuel plus large. Chaque code source dépend de « dépendances », c’est-à-dire de logiciels programmés par d’autres personnes, dont le fonctionnement n’est pas toujours maîtrisé par l’auteur du logiciel qui y fait appel. Les opérations de transformation du code source en code machine peuvent elles-mêmes être sources d’erreurs, sans parler du fait que le matériel est lui-même programmé pour réagir d’une certaine façon aux instructions transmises par un signal électrique. Tout cela est à prendre en compte dans la compréhension des mécanismes qui aboutissent à la félicité ou à l’échec du programme performatif d’un code source.

Ces codes sources obéissent à la *Lex Informatica*, qui définit des conventions facilitant la communication entre logiciels sous un format commun interopérable. Mais rien n’impose à un auteur de code source de respecter les injonctions écrites dans un document ayant vocation à devenir un standard officiel, et il arrive que des normes concurrentes coexistent.

L’écriture d’un document de standardisation technique est un acte de langage, un performatif au sens de John Austin (Austin, 1970), d’un type particulier. Son élaboration suit une

procédure particulière, décrite dans le cas du W3C dans son *Process Document*. Son écriture est polyphonique, mais chaque document se voit attribuer un rédacteur qui est *in fine* celui qui tient la plume, qui accepte les propositions des uns ou des autres ou les rejette.

Même quand l'ensemble de la procédure officielle de rédaction et de maturation d'un document est respectée, et qu'un document finit par cheminer jusqu'au statut de Recommandation W3C ou de RFC de l'IETF, rien ne garantit son succès réel. Les implémentations d'une recommandation, si elles sont nécessaires pour qu'un document parvienne à ce stade de maturité officielle, peuvent être trop rares, marginales, pour qu'obéir au document soit incontournable pour tout acteur souhaitant que le logiciel dont il écrit le code source soit adopté par un large public. Comme le souligne de façon générale John Austin au sujet des conditions de félicité des énoncés performatifs, il faut que la procédure soit réalisée de bonne foi par *l'ensemble* des participants (Austin, 1970, p. 70) pour qu'un énoncé performatif fonctionne. Ici, c'est au moins presque tous les acteurs (ou l'ensemble des acteurs dominants lorsqu'ils existent) qui agissent sur le fonctionnement d'un système socio-technique visé par une RFC ou une recommandation du W3C qui doivent adopter un comportement en adéquation avec ce document, avant que celui-ci puisse véritablement devenir de fait (puisque ce n'est jamais de droit) une norme contraignante.

Ce n'est qu'à partir du moment où des développeurs se mettent à rédiger des programmes et sites web qui respectent les règles d'écriture et de procédure dictées dans un document comme une recommandation du W3C, et que le logiciel ainsi produit est diffusé suffisamment largement pour que le respect de la recommandation soit nécessaire à l'opérabilité avec un large écosystème, que l'on peut parler de félicité de son caractère performatif. Il existe bon nombre d'exemples de RFC ou de recommandations qui ne deviennent jamais des standards, comme par exemple la recommandation *Platform for Privacy Preferences* (P3P) du W3C, sur laquelle nous reviendrons en section 5.4.2. Quant à l'IPv6, dont la RFC 2460 date de 1998, elle ne s'est toujours pas imposée, vingt ans plus tard, comme un véritable standard dans le domaine des communications électroniques, faute de véritable mise en œuvre par les différents acteurs du marché.

Le parcours vers le succès d'une RFC de l'IETF ou d'une recommandation du W3C est semé d'embûches. Un document de standardisation comme une RFC est loin de se muer systématiquement en standard. À l'IETF comme au W3C, nous avons vu que le processus d'adoption des recommandations exige, pour qu'un standard soit officiellement adopté, qu'il existe des implémentations concrètes du document, c'est-à-dire des logiciels rédigés en conformité avec les règles édictées par ce document. Une RFC, ou de tout autre document visant à standardiser le fonctionnement d'Internet, est donc performatif au sens de John Austin. Mais il ne faut pas négliger qu'il l'est également au sens de Judith Butler (Butler, 2010), car cette performativité est le fruit d'un travail itératif et progressif de construction sociale de sa légitimité en tant que standard, qui confère à un document un caractère d'autorité suffisant pour convaincre

les différents acteurs présents sur le marché qu'il concerne d'investir des moyens dans sa mise en œuvre.

5.2.3. Les arènes de la gouvernance d'Internet

Internet est le fruit de la puissance du complexe militaro-industriel des États-Unis d'Amérique et de la contre-culture associée au mouvement hippie (Bing, 2009 ; Tréguer, 2019 ; Turner, 2008). Les travaux de Jon Bing comme de Fred Turner soulignent en effet l'importance, pour le financement, des préoccupations du Département de la Défense des États-Unis, prêt à financer la création d'un réseau de communication capable de résister à une attaque nucléaire soviétique. Mais pour l'inspiration, le rôle de personnes comme Joseph Carl Robnett Licklider, qui imaginait dans les années 1950 et 1960 un « *Intergalactic Computer Network* », et devint en 1962 le chef de l'Information Processing Techniques Office de la *Defense Advanced Research Projects Agency* (DARPA), fut aussi très important.

La contre-culture américaine décrite en détail par Fred Turner dans son ouvrage sur les utopies de la Silicon Valley était réticente à l'idée de la centralisation du pouvoir. Elle était influencée par une idéologie libertaire (Turner, 2008) et par un imaginaire positif de la communauté scientifique idéale et autonome (Caloque-Bergès, 2018 ; Flichy, 2001). Lorsqu'il fallut que les ingénieurs en charge du projet Arpanet se mettent d'accord sur des protocoles de communication capable de faire fonctionner ce réseau, ancêtre de l'Internet, une forme nouvelle de processus de prise de décision émergea, qui caractérise aujourd'hui encore, au moins en théorie, les arènes de standardisation d'Internet. C'est cette même idéologie qui a inspiré, bien des années plus tard, un texte appelé la *Déclaration d'indépendance du Cyberespace*, rédigé par John Perry Barlow et qui illustre une volonté de s'émanciper de la réglementation étatique :

> « Gouvernements du monde industriel, vous géants las de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit. Au nom du futur, je vous demande à vous du passé de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté là où nous nous rassemblons[15]. » (Barlow, 1996)

En 1968, un groupe de travail informel fut créé pour répondre à ce besoin : le *Network Working Group* (NWG). Steve Crocker, l'un de ses participants, rédigea la première RFC. Datée du 7 avril 1968, il propose une description du logiciel faisant fonctionner les *Interface Message*

15 Traduit de l'anglais. Texte original : « Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. »

Processors (IMP), qui étaient les ancêtres de nos routeurs actuels sur le réseau Arpanet (Bing, 2009, p. 24). Ce document résumait des discussions qu'il avait eu avec plusieurs collègues. Le courrier électronique existait déjà, mais ne permettait que de s'envoyer des courriers entre utilisateurs d'un même ordinateur (MIT CTSS PROGRAMMING STAFF NOTE 39). C'est donc par courrier traditionnel que la première RFC fut distribuée aux autres participants du NWG, afin de recueillir leurs commentaires critiques et suggestions d'amélioration du programme décrit par Steve Crocker. De là l'origine de la formule de « *Request For Comments* ».

Le paragraphe introductif de la RFC 1 permet de comprendre l'état d'esprit dans lequel elle a été rédigée :

> « Introduction
>
> Le logiciel pour le réseau ARPA existe en partie dans les IMP et en partie dans les HOST respectifs. BB&N a spécifié le logiciel des IMP et il relève de la responsabilité des groupes HOST de s'accorder sur le logiciel HOST.
>
> Au cours de l'été 1968, des représentants des quatre premiers sites se sont rencontrés plusieurs fois pour débattre du logiciel HOST et d'expérimentations initiales sur le réseau. De ces débats a émané un groupe de travail composé de trois personnes : Steve Carr de l'Utah, Jeff Rulifson du SRI et Steve Crocker de l'UCLA, qui se sont rencontrés à l'automne et à l'hiver. La réunion la plus récente a eu lieu dans l'Utah la dernière semaine de mars. Bill Duvall du SRI, qui avait récemment commencé à travailler avec Jeff Rulifson, était également présent.
>
> De manière assez indépendante, Gerard DeLoche de l'UCLA a travaillé sur l'interface HOST-IMP.
>
> Je présenterai ici certains des points d'accord atteints et certains des problèmes soulevés. Très peu des éléments que je présente ici sont définitifs et des réactions sont attendues[16]. » (RFC 1)

16 Traduit de l'anglais. Texte original : « Introduction
The software for the ARPA Network exists partly in the IMPs and partly in the respective HOSTs. BB&N has specified the software of the IMPs and it is the responsibility of the HOST groups to agree on HOST software.
During the summer of 1968, representatives from the initial four sites met several times to discuss the HOST software and initial experiments on the network. There emerged from these meetings a working group of three, Steve Carr from Utah, Jeff Rulifson from SRI, and Steve Crocker of UCLA, who met during the fall and winter. The most recent meeting was in the last week of March in Utah. Also present was Bill Duvall of SRI who has recently started working with Jeff Rulifson.
Somewhat independently, Gerard DeLoche of UCLA has been working on the HOST-IMP interface.
I present here some of the tentative agreements reached and some of the open questions encountered. Very little of what is here is firm and reactions are expected. »

Dès la fin de l'année 1969, les RFC furent distribués sur le réseau Arpanet (Bing, 2009, p. 24). En 1973, 35 nœuds sont reliés entre eux sur ce réseau, et une première interconnexion entre ce réseau et un autre existe : le réseau Alohanet de l'université de Hawaii (Bing, 2009, p. 25). Cette première interconnexion fit entrevoir ce qui allait devenir plus tard l'Inter-net, c'est-à-dire l'interconnexion mondiale entre un nombre toujours croissant de réseaux pouvant communiquer entre eux grâce à des protocoles communs. Des interconnexions avec des réseaux informatiques norvégiens et britanniques allaient suivre rapidement (Bing, 2009, p. 28).

Maintenir l'interopérabilité entre un nombre croissant de réseaux matériellement hétérogènes devenait une tâche de plus en plus complexe, ce qui a amené le NWG à s'adapter pour demeurer capable de centraliser l'effort de coordination nécessaire à cette fin.

En 1972, lors de l'*International Computer Communication Conference*, où se tint la première démonstration au public d'Arpanet (Bing, 2009, p. 26), le NWG devint l'*International Network Working Group* (INWG), auquel participèrent notamment des ingénieurs français du projet Cyclades comme Louis Pouzin. Le but de cette organisation était de discuter informellement de futurs standards techniques, avant de les soumettre à une organisation comme l'*International Organization for Standardization* (ISO) (Russell et Schafer, 2014, p. 893). C'est dans le cadre de cette organisation que furent formalisés le TCP, dans la RFC 793, et l'IP, dans la RFC 791. Les deux avaient été le fruit d'une collaboration entre Bob Kahn et Vinton Cerf dans les années 1970 (Bing, 2009), inspirés par les travaux de l'équipe du projet Cyclades (Russell et Schafer, 2014). Comme souvent, et comme nous l'avons déjà vu avec l'exemple du HTTP, les protocoles TCP et IP avaient déjà fait l'objet de publications, et des prototypes avaient été mis en opération dès 1977, soit quatre ans environ avant la publication des RFC correspondantes (Bing, 2009, p. 27).

Le but de des participants à l'INWG était d'assurer l'interconnectivité du nombre croissant de réseaux informatiques, pour assurer, grâce à cet Inter-net, une connectivité universelle. Ce projet n'était donc pas dépourvu d'une portée utopique décrite en détail dans les travaux de Patrice Flichy (Flichy, 2001) et Fred Turner (Turner, 2008). Matériellement, Internet se définit dès lors comme étant tout ensemble de réseaux informatiques comportant des ordinateurs capables de communiquer entre eux grâce aux protocoles TCP et IP. Cela fit de ces protocoles, et des arènes où ils furent mis en délibération, le « centre magnétique » d'Internet (DeNardis, 2014, p. 67).

Le besoin de structurer la réflexion sur l'évolution du développement d'Internet, et d'éviter que tout ne repose sur les épaules d'une seule personne, Vinton Cerf, entourée de quelques conseillers, inspira la création d'un *Internet Configuration Control Board* (ICCB) en 1979, dirigé par David Clark, du MIT. Cet ICCB devient l'*Internet Advisory Board* en 1984 puis l'*Internet*

Activities Board (1986) et enfin l'*Internet Architecture Board* (IAB) en 1992. L'*Internet Architecture Board*[17] existe toujours de nos jours.

L'*Internet Architecture Board* devint peu à peu l'organisation qui, *de facto*, mais sans aucun mandat légal ou autre mécanisme contraignant, devint l'autorité chargée d'approuver les standards techniques d'Internet, sur la base non pas de votes majoritaires parmi ses membres, mais de la recherche du consensus. Plusieurs groupes appelés « *task forces* » sont sous son autorité, qui se stabilisèrent après quelques évolutions en 1990 (RFC 1160; Russell, 2006) pour former aujourd'hui :

- L'*Internet Engineering Task Force* (IETF), fondée en 1986, chargé de travailler sur les RFC à court terme ;
- L'*Internet Research Task Force* (IRTF), chargée de réflexions à plus long terme, et fondé en 1989.

Chaque « *Task Force* » est dirigée par un « *Steering Group* », composé des « *Area Directors* » de chaque « *Task Force* ». Chaque *Area Director* est en charge d'un secteur de l'activité de sa Task Force. Il existe donc une hiérarchie au sein de l'*Internet Architecture Board*, comme de l'IETF. Le processus d'élection, assez informel et relevant plutôt de la coutume, fut peu à peu codifié à partir d'octobre 1996 (RFC 2027), et mêle des mécanismes de co-optation à des mécanismes de vérification de l'existence d'un consensus assez complexes. Le processus, actuellement codifié dans les RFC 7437, 7776 et 8318, s'est encore complexifié, et inclut également des éléments de tirage au sort.

Entre la naissance du NWG et aujourd'hui, l'idée d'une coopération avec l'ISO pour la finalisation des RFC en standards officiels a fait long feu, en raison d'un conflit ouvert entre les informaticiens impliqués dans le projet Internet et l'ISO. En 1977, l'ISO proposa une architecture concurrente à Arpanet (et à l'Internet naissant) : l'*Open Systems Interconnection* (OSI) (Russell, 2006). Internet et l'OSI partageaient l'objectif de proposer une alternative ouverte et interopérable à des architectures réseaux propriétaires comme la *System Network Architecture* de la compagnie IBM (Russell, 2006, p. 52). Mais l'inspiration philosophique derrière l'OSI et Internet, tout comme leurs modèles de gouvernance, étaient très différents. Contrairement au modèle informel de l'INWG, une organisation informelle sans existence juridique, l'ISO est une organisation officielle, bénéficiant à partir des années 1980 du soutien officiel du Département de la Défense des États-Unis, l'institution qui avait été à l'origine du projet Arpanet.

Des participants à l'INWG comme Jon Postel, co-inventeur de l'*Internet Protocol*, critiquèrent le processus de prise de décision de l'ISO comme étant trop théorique, trop abstrait, et pas assez concret (Cohen et Postel, 1983). D'autres critiquèrent l'ISO comme étant

17 Nous n'utilisons pas l'abréviation (IAB) de l'*Internet Architecture Board*, pour éviter la confusion avec l'*Interactive Advertisement Bureau*

« prescriptive » là où l'INWG était « descriptif ». Selon un de ces participants, David Mills, dans un entretien de 2004 cité par Andrew Russell :

> « Les standards d'Internet tendaient à être ceux qui avaient été écrits pour les implémenteurs. Les standards internationaux étaient rédigés comme des documents auxquels on devait obéir[18]. » (Interview de David Mills citée par Russell, 2006, p. 53-54)

Ces différences de fonctionnement pointent une caractéristique des arènes de standardisation d'Internet où sont délibérés les standards de la *Lex Informatica*. L'ISO, et avec elle, le projet OSI (voir : ISO/IEC 7498-1:1994), suivaient un modèle prescriptif *top-down*, inspiré de la réglementation au sens classique du terme, et par la philosophie de la primauté de la loi sur la coutume des pays de droit continental. Au contraire, le NWG, puis l'INWG et aujourd'hui l'IETF et le W3C exigent, pour qu'un standard soit adopté, qu'il existe des implémentations, même expérimentales, de ce standard (RFC 2026 ; W3C Process). Le but y est donc de construire sur la pratique, sur la coutume, tout en invitant les participants à délibérer ouvertement dans le double but d'aboutir à un consensus qui favorise l'adoption de la norme à l'échelle du technique auquel elle s'applique pour en améliorer la qualité technique. Comme le montre Luca Belli dans ses travaux de recherche, ce processus participatif constitué par la « communauté technique » informelle de ses participants est fondé sur des idéaux proches de ceux de l'agir communicationnel et de la délibération démocratique de Jürgen Habermas, sans pour autant que ce dernier ait été une source d'inspiration pour les fondateurs des arènes de standardisation d'Internet (Belli, 2016, p. 141 ; Habermas, 1987). Le fait qu'il n'y ait aucun mécanisme contraignant est même conçu comme un gage de qualité, l'idée étant que seuls les meilleurs standards seraient volontairement mis en œuvre par les acteurs d'Internet (Alvestrand et Wium Lie, 2009).

Cette philosophie fut résumée lors d'une présentation faite par David Clark à la conférence annuelle de l'IETF de 1992. En réaction à un processus ISO perçu comme une menace pour l'espace de liberté et de créativité de l'IETF, il prononça les fameuses phrases : « Nous rejetons les rois, les présidents et le vote. Nous croyons en le consensus global et le code qui fonctionne[19]. », qui se trouvent sur une des diapositives de sa présentation à cette conférence, toujours disponible en ligne :

18 Traduction de l'auteur. Texte original : « Internet standards tended to be those written for implementers. International standards were written as documents to be obeyed. »

19 Traduction de l'auteur. Texte original : « We reject kings, presidents and voting. We believe in : rough consensus and running code »

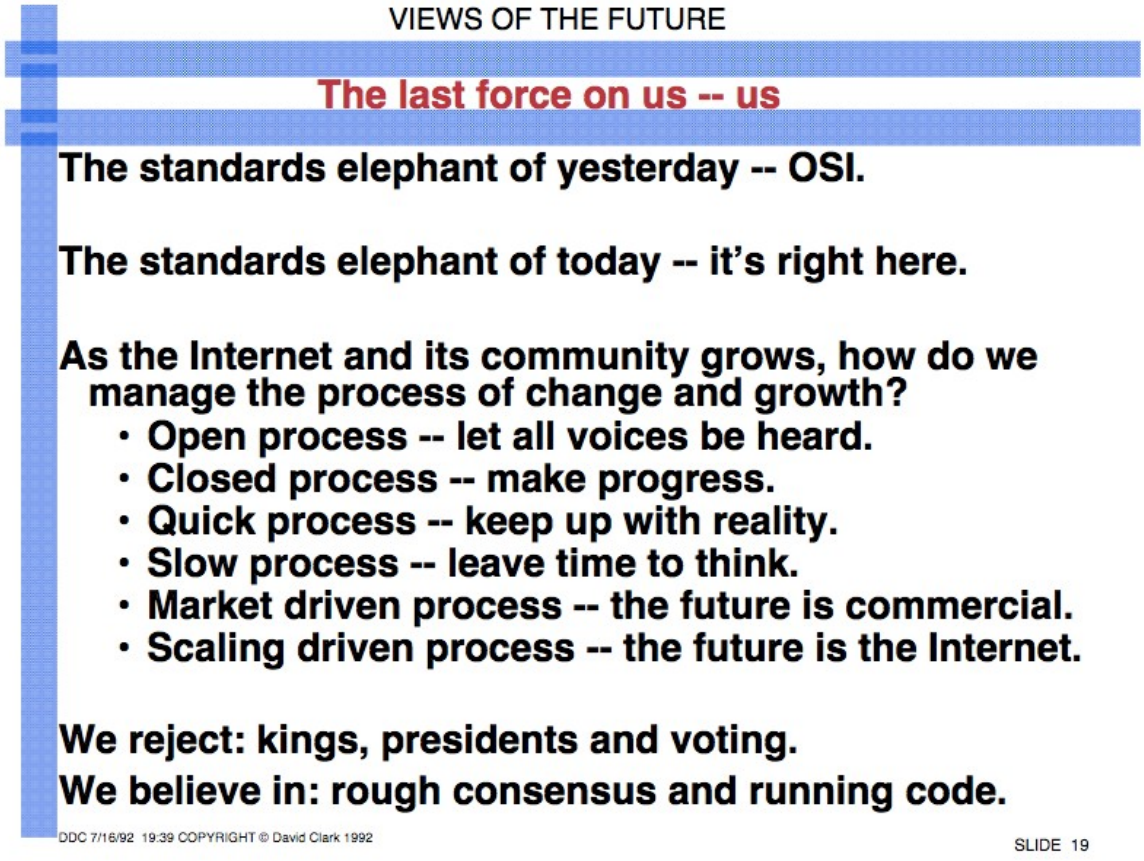


Figure 27 : *Extrait de la présentation de David Clark lors de l'IETF 24 en 1992* (Clark, 1992, p. 19)

Cette profession de foi est reprise aujourd'hui dans un document appelé dans sa traduction française « Le Tao de l'IETF : Guide destiné aux nouveaux participants à l'Internet Engineering Task Force », et qui est une sorte de charte fondatrice rétrospective de l'IETF :

> « À bien des égards, l'IETF repose sur les croyances de ses participants. L'une des « croyances fondatrices » est incarnée dans une citation sur l'IETF de David Clark : « Nous rejetons les rois, les présidents et le vote. Nous croyons en un consensus approximatif et un code qui fonctionne ». Une autre citation qui est devenue une croyance communément répandue à l'IETF vient de Jon Postel : « Soyez conservateur dans ce que vous envoyez et libéral dans ce que vous acceptez ». » (Hoffman, 2012)

Formellement, l'IETF n'existe toujours pas, au sens où il ne s'agit ni d'une association, ni d'une entreprise, ni d'une institution publique, ni de quelque autre organisme détenant la personnalité juridique que ce soit. L'*Internet Society* (ISOC) est une association qui a été fondée pour apporter un soutien logistique à l'*Internet Architecture Board*, à l'IRTF et à l'IETF. Selon Vinton Cerf, l'un de ses fondateurs :

> « L'Internet Society a été formée par un certain nombre de personnes impliquées depuis longtemps dans l'Internet Engineering Task Force (IETF). En conséquent, l'une de ses principales raisons d'être était de fournir un cadre institutionnel [*institutional home*] et un soutien financier au processus des Standards Internet[20]. » (Cerf, 1995)

Fondée en 1992, cette association est depuis 1996 en charge du support administratif, financier et en ressources humaines de l'IETF (Contreras, 2016, p. 8), selon une relation initialement codifiée dans la RFC 2031.

Deux facteurs allaient durant cette période des années 1980 et 1990 consolider la place d'organisations comme l'*Internet Architecture Board* et l'IETF.

Le premier est que ces innovations sont advenues dans un moment de retrait de l'État dans le bloc occidental, qui correspond au tournant néolibéral entamé dans les années 1980 (Hall, 1986 ; Jobert, 1994). Cela a joué un rôle très important dans la trajectoire du développement d'Internet (Mueller, 2010), avec la fin progressive des monopoles nationaux des grandes compagnies de télécommunications d'abord aux États-Unis puis dans le reste du monde occidental, ou en France la création des radios et télévisions libres, soit en d'autres termes, le reflux de la mainmise de l'État sur les télécommunications (Tréguer, 2019). D'abord en 1980, la *U.S. Federal Communications Commission* adopta une politique de dérégulation des réseaux télématiques, qu'elle distingua des réseaux téléphoniques classiques, eux réglementés. Puis, à partir du milieu des années 1990, et notamment sous l'impulsion de la politique de l'administration Clinton, Internet s'est ouvert à des usages commerciaux qui ont notamment permis une prolifération de fournisseurs d'accès à Internet commercialisant l'accès à leurs réseaux TCP/IP privés connectés via ces protocoles au reste d'Internet. Ces derniers permettent à des particuliers ou à des entreprises de brancher leurs propres réseaux domestiques sur le leur pour avoir accès à l'ensemble d'Internet (Mueller, 2010).

Le deuxième facteur est que les réformes sur le droit d'auteur aux États-Unis, puis la possibilité de breveter certains logiciels, ont ouvert la voix à la privatisation des standards faisant fonctionner Internet. Il devint alors nécessaire pour l'IETF et ses fondateurs de développer une

20 Traduit de l'anglais. Texte original : « The Internet Society was formed by a number of people with long-term involvement in the Internet Engineering Task Force (IETF). As a result, one of its principal rationales was to provide an institutional home for and financial support for the Internet Standards process. »

politique de brevets permettant à l'ensemble des acteurs d'Internet ayant besoin de mettre en œuvre les standards d'Internet et du web de le faire et, si possible, de le faire gratuitement. Cela s'applique aussi au W3C et aux autres organismes de ce type (Contreras, 2016). Les lois sur la propriété intellectuelle ont donc eu pour effet de forcer une forme institutionnelle de coopération pour éviter le morcellement d'Internet en un kaléidoscope de réseaux publics et privés fondés sur des protocoles propriétaires incompatibles entre eux.

Il existe pléthore d'autres organisations de normalisation technique pertinentes dans la gouvernance d'Internet. Par exemple, le développement de la norme WiFi est assuré par un groupe de travail de l'*Institute of Electrical and Electronics Engineers* (IEEE), le groupe IEEE 802.11. La norme Open Document Format à laquelle obéissent les fichiers de la suite LibreOffice, elle est le fruit de discussions ayant lieu au sein du consortium *Organization for the Advancement of Structured Information Standards* (OASIS), qui avait été fondé en 1993 sous le nom SGML Open. Quant au Javascript, son développement se partage entre le socle fourni par l'ECMAScript de l'*European Association for Standardizing Information and Communication Systems* (ECMA International) et certaines recommandations de W3C qui le complètent.

Enfin, aucun panorama, aussi succinct soit-il, des arènes de la gouvernance d'Internet ne serait complet sans qu'il ne soit fait mention de l'*Internet Corporation for Assigned Names and Numbers* (ICANN).

L'ICANN, une association de droit californien, est responsable d'une des ressources les plus rares et les plus critiques d'Internet : les adresses IP (et non le protocole, dont l'IETF a la charge) et les noms de domaine (Belli, 2016).

Le *Domain Name System* (DNS) est un protocole standardisé par l'IETF. Pour fonctionner, il faut que des ordinateurs, des serveurs DNS, détiennent des tables de correspondance mises à jour entre des listes d'adresses IP et des noms de domaine (comme « google.fr », « yandex.ru », etc). Il existe plusieurs systèmes DNS concurrents à celui qui est administré par l'ICANN, mais l'ICANN détient un quasi-monopole de fait, qui bénéficie du soutien de l'*Internet Architecture Board* (voir la RFC 2826). Si entre 1998 et 2016, cette fonction lui fut déléguée par le *Department of Commerce* des États-Unis , l'ICANN a finalement pris son indépendance formelle par rapport au gouvernement des États-Unis lors de l'expiration du contrat (ICANN, 2016), y compris pour l'exercice de ces missions de nommage et d'adressage.

Pour pouvoir enregistrer des noms de domaines dans ce système DNS monopolistique, chaque *registrar* national, comme en France l'Association française pour le nommage Internet en coopération (AFNIC) doit signer un contrat avec l'ICANN, qui est de fait un contrat d'adhésion (Belli, 2016).

En matière de protection de la vie privée, il y a eu bien des tensions entre certains *registrars* (organismes à qui est délégué l'enregistrement des noms de domaine) et l'ICANN, et

entre les autorités européennes de protection des données et l'ICANN[21]. L'essentiel de ces tensions reposent sur le rôle du registre WHOIS, géré lui aussi par l'ICANN, et qui est une forme de cadastre des noms de domaine, permettant à l'origine à tout le monde de voir le nom et l'adresse des détenteurs des noms de domaine, et ce, sans aucune protection, même lorsqu'il s'agissait de particuliers.

L'ICANN n'a toutefois pas pour fonction d'éditer des standards d'Internet, mais de gérer certaines de ses ressources critiques, ce qui n'est pas tout à fait la même chose. De plus, ce n'est pas une arène de mise en délibération de questions relatives à la vie privée *en général*, ni un lieu où sont discutés des standards renforçant la protection de la vie privée, et encore moins un lieu où sont évalués les risques que certains standards représentent en matière de protection de la vie privée. L'ICANN ne fait donc pas partie de notre enquête sur la standardisation techno-politique de la « vie privée » dans les arènes de la gouvernance d'Internet.

5.2.4. Les standards techno-politiques d'Internet

Contrairement à une impression répandue, les organismes comme le W3C ou l'IETF ne sont pas des arènes « purement techniques », au sens où les délibérations qui s'y déroulent seraient déconnectées des implications économiques, politiques et sociales des standards adoptés.

Lorsque Lawrence Lessig affirme avec emphase que « *Code is Law* », il donne pour exemple le fait que le code informatique détermine le degré d'anonymat auquel un internaute peut accéder. Il évoque ainsi le fait que le protocole IP, n'étant pas conçu pour identifier des personnes, complique le pistage des personnes physiques sur Internet et leur identification formelle, y compris dans des situations d'enquêtes judiciaires (Lessig, 2000). Si, depuis la parution de l'article de Lawrence Lessig en 2000, un grand nombre de techniques qui se sont depuis répandues doivent nous amener à remettre en cause l'idée que les individus sont difficiles à pister sur Internet, la conclusion fondamentale selon laquelle le code informatique a des effets de régulation sociale comparables en bien des aspects au droit – qu'il soit de droit continental ou de *Common Law* – reste valable.

Les codes sources dont Lawrence Lessig parle dans son article doivent obéir, pour se compiler en des logiciels capables de communiquer entre eux sur Internet, à des standards. Il s'en suit que si le code fait (d'une certaine manière) loi, alors les standards qui fixent un cadre à ces

21 Voir par exemple la lettre de Jacob Kohnstamm, président du Groupe de travail de l'Article 29 (Kohnstamm, 2012b) envoyée le 26 septembre 2012 au président de l'ICANN pour exiger la mise en conformité de cet organisme au droit européen de la protection des données à caractère personnel. La lettre rappelle un avis adopté en 2003 (avis 2/2003 du G29), et des échanges de courriers en 2006 et 2007 n'ayant pas aboutis. Cet échange sera suivi de plusieurs autres courriers du G29 en 2014, puis en 2018.
Voir aussi l'affaire ayant opposé EPAG, un *registrar* allemand, à l'ICANN (Oberlandesgericht Köln. 3 septembre 2018. « ICANN gegen EPAG ». Aff. 19W 32/18)

codes qui constituent la *Lex Informatica* font aussi (d'une certaine manière) loi, à un degré plus élevé de la pyramide des normes de l'informatique que les codes sources. Dès lors, comme le rappelle Laura DeNardis :

> « Les standards intersectent avec l'intérêt public, à la fois en raison de la nature critique de l'interopérabilité dans les infrastructures publiques et parce qu'ils peuvent constituer des instruments [*enactments*] de gouvernance en eux-mêmes[22]. » (DeNardis, 2014, p. 76-77)

En déterminant la façon dont fonctionnent les réseaux de communication, ils ont des effets sur les conditions d'exercice de la liberté d'expression (DeNardis, 2014, p. 77). Le débat sur la neutralité du Net est l'illustration d'une controverse sur ce que sont les conditions équitables d'accès à l'infrastructure matérielle permettant de diffusion d'une information sur Internet. Ceux sur l'*Encrypted Media Extension* (EME), plus récents, ont porté sur la question de savoir s'il fallait intégrer un système de gestion des droits d'auteur sur le web (Sire, 2017). Sur le plan économique, il existe une compétition entre entreprises pour savoir quels seront les standards adoptés (DeNardis, 2014, p. 77). Les coûts d'adaptation d'une norme technique à une autre étant élevés, une entreprise a intérêt à imposer sa façon de fonctionner comme étant le standard adopté. En 2008, Microsoft imposa son standard Open XML, qui correspond au format .docx de sa suite Office, à l'ISO, face à son concurrent Open Document Format d'OpenOffice (Lamonica, 2008), au terme d'un processus très controversé auquel se sont mêlées des accusations de corruption de certains organismes nationaux de standardisation membres de l'ISO et ayant participé au vote (Calore, 2007 ; Lamonica, 2008). Pour donner un exemple plus récent, le groupe de travail *Web Payments* du W3C développe des standards qui sont d'un intérêt direct pour un grand nombre de champs de l'action publique, des paiements à la finance en passant par la lutte contre le blanchiment et le financement du terrorisme.

Les controverses au sein des arènes de standardisation d'Internet se structurent alors autour de ce que Guillaume Sire, s'inspirant de la terminologie de ces deux mêmes auteurs (Bijker, 1995 ; Lenert, 2004), appelle une « ligne de conflit », définie comme « un sujet divisant les acteurs qui œuvrent à la mise au point d'un même artefact, et dont l'opposition aura des effets sur ce qu'est ou ce que n'est pas cet artefact » (Sire, 2017, p. 49).

Un exemple de projet de standard ayant fait controverse est la recommandation *Battery Status API*. Rédigée par des membres du groupe de travail *Device and Sensors Working Group* du

22 Traduit de l'anglais. Texte original : « Standards intersect with the public interest both because of the critical nature of interoperability in public infrastructures and because they can be enactments of governance themselves. »

W3C, sa section introductive décrit son objectif comme étant de permettre aux sites et applications web d'adapter des fonctionnalités à l'état de charge d'une batterie. La désactivation de certaines fonctions non-essentielles et gourmandes en énergie lorsque le statut de charge est faible permettrait ainsi une meilleure « expérience utilisateur », selon les termes des auteurs de la recommandation.

Łukasz Olejnik, Gunes Acar, Claude Castelluccia et Claudia Diaz (2015) ont montré que cette nouvelle fonctionnalité pouvait permettre de faciliter l'identification des internautes, et présentait ainsi un risque en matière de vie privée. Après avoir rappelé que l'API[23] ne prévoit pas de mécanisme systématique de demande d'autorisation à l'internaute pour que soit transmise au serveur l'information sur l'état de charge de la batterie, ils montrent que l'appel de la méthode navigator.getBattery() sur un navigateur web Firefox démarré à partir du système d'exploitation GNU/Linux renvoyait un nombre décimal ayant la précision d'une variable dite à double précision, c'est-à-dire ayant une précision de 16 chiffres significatifs après la virgule (voir IEEE754:2008). Cela n'était pas le cas sous Windows, Mac OS X ou Android.

La raison de cette différence, qui illustre à quel point chaque brique logicielle et matérielle d'un système sociotechnique complexe comme Internet est dépendant d'une myriade d'autres briques, est qu'à la réception d'une demande navigator.getBattery(), Firefox, sous Linux, faisait appel à UPower. Ce dernier est un outil installé par défaut avec le système d'exploitation qui permet à n'importe quel autre logiciel d'accéder à l'état de charge de la batterie. L'analyse du code source de ce logiciel libre permet de voir qu'il permet un accès très précis à l'état de charge de la batterie.

Une valeur d'une telle précision, lue à distance à intervalles courts et réguliers, permet de connaître de façon fiable le profil de la batterie : à quelle vitesse se décharge-t-elle ? Ce profil est alors un élément de plus qu'un ordinateur distant peut connaître sur l'appareil de l'internaute, permettant de le réidentifier (Olejnik et al., 2015).

La publication de cette vulnérabilité a entraîné un certain nombre de conséquences, dont la plus immédiate a été la limitation par Firefox de la précision de la valeur renvoyée par la méthode navigator.getBattery() à deux chiffres après la virgule. La section de la recommandation W3C Battery Status API a également été mise à jour (Olejnik, Englehardt et Narayanan, 2017).

C'est pour traiter ce type de cas qu'un certain nombre d’acteurs du W3C, parmi lesquels Łukasz Olejnik, Arvind Narayanan ou encore Nick Doty, que nous retrouverons parmi les principaux acteurs du projet *Do Not Track* du W3C, ont appelé à l'inclusion systématique dans chaque recommandation du W3C ou dans chaque RFC de l'IETF d'une étude d'impact résumée dans une section sur la protection de la vie privée (Doty, 2015 ; Olejnik, Englehardt et Narayanan, 2017). Une telle section s'inspirerait des « *Security Considerations* », devenues

23 API désigne en anglais une *Application Programming Interface*, soit, en français, une interface de programmation applicative. C’est un ensemble normalisé de méthodes permettant à un logiciel de fournir des services à un autre logiciel. Par exemple, dans le *Battery Status API*, il s’agit d’une description de la façon dont un logiciel, le serveur web, peut demander à un autre logiciel, le navigateur, des informations sur l’état de charge de l’ordinateur sur lequel il tourne.

obligatoires avec l'adoption de la RFC 1543 en octobre 1993, et dont la RFC 3552 adoptée en juillet 2003 détaille des exigences de fond et de forme. Malgré une qualité variable et souvent décrite comme médiocre, de telles « considérations », depuis le début des 1990, et de façon stable, presque 100 % des RFC comportement au moins le terme « security », alors que les meilleures années, seul entre 20 % et 25 % des RFC publiées comportaient le terme « privacy » (Doty, 2015). Il existe toutefois des standards, tant de l'IETF que du W3C ou même d'autres organismes, qui comportent volontairement une telle section, parfois, comme dans le cas du *Battery Status API*, sous la pression d'acteurs militants présents dans ces arènes.

Cet exemple que nous venons de développer montre qu'un projet *a priori* très technique et éloigné de toute considération politique, comme la façon de communiquer à un serveur web une donnée numérique sur un état de charge de batterie, peut provoquer une controverse à laquelle participent des personnes pouvant venir de l'extérieur du projet controversé, et qui participent en raison d'un engagement politique.

En plus de tels exemples de standards qui suscitent un intérêt qui dépasse le cercle restreint d'ingénieurs engagés dans l'IETF ou le W3C et dont la démarche de standardisation se veut strictement technique, il existe aussi des groupes au sein de ces arènes qui sont dédiés à la recherche de solutions à des problèmes politiques par la production de standards techniques. Le groupe *Web Accessibility Initiative* du W3C publie par exemple des lignes directrices sur la façon d'améliorer l'accessibilité des sites web pour des personnes en situation de handicap (DeNardis, 2014, p. 77). D'autres projets de standardisation technique cherchent à « standardiser la vie privée » (DeNardis, 2014, p. 77). Laura DeNardis cite plusieurs exemples de projets allant dans ce sens : le projet *The Onion Routeur* (TOR), le projet P3P, ou encore la RFC 3041, remplacée depuis par la RFC 4941. Ces deux dernières RFC décrivent un mécanisme qui réduit le risque que les adresses IPv6 attribuées à un appareil soient toujours identiques, sur tous les réseaux auquel il se connecte, afin de compliquer son identification et donc de protéger la vie privée de son propriétaire (RFC 4941, section 1).

Nick Doty, qui participe au *Tracking Protection Working Group*, et Deirdre Mulligan, qui a participé au projet P3P depuis son tout début, ont défini la notion de de « standard techno-politique » (*« techno-policy standard »*) à partir de tels exemples :

> « Un petit nombre de groupes de travail W3C ont été constitués [*chartered*] spécialement pour réfléchir aux liens entre les questions techniques et les questions de politiques publiques [*policy*], définissant ce que l'on pourrait appeler un "standard techno-

politique”[24]. » (Doty et Mulligan, 2013, p. 141)

Leur définition du concept, très empirique, nous a paru un peu courte pour avoir des contours clairs. Nous proposons donc de la développer et de la préciser, en définissant un standard techno-politique comme : tout texte à vocation performative qui définit le fonctionnement d'un ensemble de logiciels faisant système et dont la vocation première est de résoudre un problème préalablement perçu et défini par ses auteurs comme de nature politique. Les logiciels permettant le bon fonctionnement d’Internet sont un exemple d’un ensemble de logiciels faisant système.

Les standards définis par le *Web Payments Working Group* du W3C ont des impacts sociaux et économiques, mais ils ne sont pas conçus par leurs auteurs comme ayant une mission principalement politique. Selon notre définition, il s'agit « simplement » d'un standard qui permet de normaliser la façon dont des ordres de paiement sont transmis sur le web, via des interfaces intégrées dans des navigateurs web. *A contrario*, la RFC 4941 a pour but affiché d'améliorer la protection de la vie privée des internautes (RFC 4941, p. 6), les recommandations du groupe de travail P3P du W3C devaient permettre à un internaute d'exprimer par l'intermédiaire de l'interface de son navigateur des règles de confidentialité (W3C P3P 1.1), et le standard *Accessible Rich Internet Applications* (WAI-ARIA) cherche à résoudre (au moins en partie) le problème de l'accessibilité du web pour les personnes handicapées (W3C ARIA 1.1).

La RFC 6973, qui définit la façon dont les autres RFC doivent traiter la question de la protection de la vie privée, est aussi un standard techno-politique selon notre définition, puisque :

- Elle cherche bien à résoudre un problème conçu comme politique : la garantie de l'exercice du droit à la vie privée sur Internet ;
- Il s'agit d'un texte qui fonctionne selon les principes d'un énoncé performatif ;
- Elle vise à encadrer la façon dont les autres RFC, qui décrivent normativement la façon dont des systèmes logiciels doivent fonctionner pour communiquer entre eux, doivent être rédigées ;
- Ce faisant, elle cherche bien à résoudre par de l’ingénierie logicielle un problème construit comme politique.

Les standards techno-politiques et leurs implémentations entrent dans la catégorie des *Privacy Enhancing Technologies* (PET's), qui sont un des instruments de l'action publique en matière de protection des données personnelles et de la vie privée (Bennett et Raab, 2003).

24 Traduit de l’anglais. Texte original : « A small number of W3C working groups have been chartered specifically to consider interlinking technical and policy issues, defining what we might call a “techno-policy standard”. »

Le projet de résoudre un problème politique par la standardisation technique et donc, au bout du compte, par de nouveaux artefacts techniques, entre dans le cadre de ce qui est critiqué vivement par Evgeny Morozov comme étant dans ses mots du « solutionisme » (Morozov, 2015). Il est certain qu'apporter des solutions purement techniques à un problème politique s'avère dans bien des cas un leurre qui relève souvent de la croyance en l'efficacité forte des projets des concepteurs médiés par leurs artefacts techniques auprès d'usagers passifs. Mais l'objet de notre étude n'est pas, ici, d'évaluer l'efficacité d'une action publique qui passe par de tels standards. Deirdre Mulligan et Nick Doty ont déjà tenté pour cela de définir un cadre d'évaluation (Doty et Mulligan, 2013).

Notre travail a consisté à étudier les représentations de la vie privée et du droit *à la* vie privée qui circulent dans des arènes de standardisation techno-politique.

Comme le niveau de connaissances en informatique requis pour participer de façon pertinente aux travaux des arènes de standardisation d'Internet, et pour y être reconnu comme un interlocuteur crédible par les autres participants, est très élevé, à de rares exceptions près, tous les participants y sont des informaticiens. La composition de ces arènes est donc très différentes de celles du Conseil de l'Europe, de l'OCDE et des « discussions » sur le RGPD que nous avons étudiées, fréquentées, elles, par des gens socialisés au droit et à la politique, mais rarement à l'ingénierie informatique. Cela nous a permis de chercher, à travers le cas du *Privacy Interest Group* du W3C, des éléments de réponse à des questions comme : les informaticiens de l'IETF ou du W3C ont-ils la même définition de la vie privée et du droit *à la* vie privée que les juristes du Conseil de l'Europe ou des institutions de l'UE ? À quels auteurs font-ils référence ? Quels arguments utilisent-ils ? Sont-ils confrontés aux mêmes contre-arguments que des acteurs évoluant dans les arènes institutionnelles de l'UE ?

Les arènes de standardisation technique sont souvent présentées, tant par nombre des acteurs qui y participent ou par des observateurs extérieurs, comme indépendantes de tout ce qui relève du droit étatique. La fameuse déclaration d'indépendance du cyberespace de John Perry Barlow, que nous avons déjà citée, illustre bien ce sentiment. Or, étudier les arènes de standardisation techno-politique permet aussi d'observer, d’évaluer dans quelle mesure des normes juridiques ou l'action des États y influencent les discussions. Nous en avons donc profité pour interroger cet imaginaire typiquement partagé par les acteurs de la standardisation technique d’Internet (Flichy, 2001) auquel certains travaux universitaires, comme ceux de Pierre Lévy sur la « noosphère », ont offert un important écho (Lévy, 2000).

Ainsi, est-il vrai que, par nature, des textes juridiques comme la récente California Consumer Privacy Act de 2018, le RGPD ou encore l'Acte additionnel de la CEDEAO A/SA 1/01/10 du 16 février 2010 relatif à la protection des données personnelles ne peuvent s’appliquer à Internet ? Ces textes juridiques ont-ils au moins une influence sur la façon dont se déroulent les

discussions sur les standards d'Internet, ou assiste-on à une absence totale de référence à des règles de droit dur dans les discussions ?

Il y a un grand nombre d'arènes que nous aurions pu choisir pour servir de terrain empirique à notre étude. Voici par exemple un tableau non-exhaustif d'arènes où sont discutées des standards techno-politiques relatifs à la protection des données à caractère personnel et à la protection de la vie privée :

Organisation	**Arène**	**Documents**
W3C	Techical Architecture Group	Self-Review Questionnaire: Security and Privacy
	Privacy Interest Group	Fingerprinting Guidance for Web Specification Authors
		Privacy Considerations for Web Protocols
		Specification Privacy Assessment (SPA)
	Tracking Protection Working Group	Tracking Compliance and Scope
		Tracking Preference Expression (DNT)
	Platform for Privacy Preferences (defunct)	The Platform for Privacy Preferences 1.0 (P3P1.0) Specification
IETF		RFC 1087 – Ethics and the Internet
		RFC 6973 – Privacy Considerations for Internet Protocols
		RFC 7258 – Pervasive Monitoring Is an Attack
		RFC 3041 – Privacy Extensions for Stateless Address Autoconfiguration in IPv6 RFC 4941 – Privacy Extensions for Stateless Address Autoconfiguration in IPv6

	Mailing list on pervasive monitoring (perpass)	
	IETF Privacy and Security Program	
	IETF Geographic Location/Privacy (geopriv)	RFC 3693 – Geopriv requirements RFC 4745 - Common Policy: A Document Format for Expressing Privacy Preferences RFC 6280 - An Architecture for Location and Location Privacy in Internet Applications etc.
OASIS	OASIS Privacy Management Reference Model (PMRM) TC	Privacy Management Reference Model and Methodology (PMRM) Version 1.0
	OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC	Privacy by Design Documentation for Software Engineers Version 1.0
IRTF	Privacy and Security Research Group (defunct)	
	Human Rights Protocol Considerations Research Group	
IEEE	IEEE 802 EC Privacy Recommendation Study Group (defunct)	P802E – Recommended Practice for Privacy Considerations for IEEE 802 Technologies
	IEEE Global Initiative on Ethics and Autonomous and Intelligent Systems	IEEE Ethically Aligned Design v1
	IEEE P 7006 – WG-PDAI – Personal Data AI Agent Working Group	Standard for Personal Data Artificial Intelligence (AI) Agent (qui ne semble pas encore être publiée à la date du 23 juillet 2018)
Kantara Initiative	Kantara Identity and Privacy Incubator	
ICANN	PDP Privacy & Proxy Services Accreditation Issues Working Group	
ISO	ISO/IEC JTC 1/SC 27 IT	ISO 29134:2017 on PIA's

	Security techniques	La série ISO 27000 sur la sécurité ISO 29190:2015 on processes with regards to privacy ISO 27018 on cloud computing
	ISO/IEC JTC 1/SC 27/WG 5 Identity management and privacy technologies	

Tableau 13 : *Aperçu non-exhaustif des arènes de standardisation techno-politique de la vie privée*

Le *Privacy Interest Group* (PING) et sa liste de discussion *public-privacy*, point de départ de notre enquête de terrain, rassemblent depuis 2010 des gens qui, au sein du W3C, ont un intérêt pour le sujet de la protection de la vie privée. Le *Human Rights Protocol Considerations* (HRPC) de l'IRTF héberge bien des discussions sur la protection de la vie privée, mais son champ s'étend à d'autres domaines, comme la liberté d'expression et la lutte contre la censure ou encore la liberté d'association (RFC 8280).

Le W3C PING semble donc être, aujourd'hui, le seul groupe de travail parmi les principales arènes de standardisation d'Internet à avoir pour mandat de s'intéresser à la vie privée en général (au contraire du TPWG, entre temps d'ailleurs disparu), mais aussi en particulier (au contraire du HRPC). Et contrairement au groupe P3P du W3C, il s'agissait d'un groupe encore actif au moment où nous avons mené notre enquête de terrain.

Notre étude a cependant inclus, là où cela s'est avéré nécessaire, des éléments provenant d'autres arènes. En raison de la façon dont le W3C PING et le TPWG étaient liés, nous avons par exemple été amenés à intégrer à notre étude de terrain des débats sur la définition de la notion de « *tracking* » qui n'ont pas été hébergées par le PING. Nous avons également étudié ce qui avait précédé le PING, au sein du W3C, et qui permet d'en expliquer la création, comme, en particulier, les controverses autour de travaux sur la géolocalisation qui ont commencé en 2008, ou l'héritage du groupe P3P. Chacun de ces détours a été incité par leur évocation dans des échanges d'e-mails sur la liste de discussion public du PING, ou dans des entretiens que nous avons réalisés. L'étude du PING s'est ainsi révélée être un excellent point de départ pour comprendre et cartographier les discussions sur la vie privée au niveau du W3C dans son ensemble.

5.3. Le World Wide Web Consortium (W3C)

Le *World Wide Web Consortium* (W3C) est l'organisme informel issu de la coopération entre plusieurs universités qui est chargé d'héberger l'activité de production des standards techniques du Web.

Le *World Wide Web*, souvent désigné comme le « Web », est la combinaison d'un protocole (le HTTP) et d'un langage informatique (le *HyperText Markup Language*, ou HTML) compatibles avec le protocole TCP/IP et permettant, via une connexion à Internet, de récupérer depuis des ordinateurs distants auxquels se connecte l'internaute des pages mises en forme contenant des contenus multimédias (texte, image, son). Les liens hypertextes pointent vers des ressources qui sont identifiés suivant la convention de l'*Uniform Resource Locator* (URL), comme http://nomdedomaine.com/index.html. Les pages web, sont rédigées en HTML. À l'origine, le HTML permettait la description et la mise en forme des pages, à l'aide de balises placées dans le texte. Par exemple :

```
<b>Exemple</b>
```

s'affiche[25] en gras :

Exemple

La balise <a> permet elle de créer un lien hypertexte. Par exemple :

```
<a href = "http://www.utc.fr">UTC</a>
```

commande l'affichage d'un texte (« UTC ») qui, si l'internaute clique dessus avec le curseur de sa souris, lui permet de demander à son navigateur d'aller charger la page web d'accueil située sur le serveur identifié dans le système DNS par le nom de domaine utc.fr, qui correspond à l'adresse IP : 195.83.155.24.

Ces pages sont requêtées, interprétées et affichées par des logiciels spéciaux : les navigateurs web. Le premier navigateur web, développé par Tim Berners-Lee à l'époque où il travaillait encore pour le Centre européen de recherche nucléaire (CERN), date de 1990. Il fut éclipsé rapidement par Mosaic, qui lui-même inspira Netscape Navigator, dont le code source servit de base au développement de la suite Mozilla puis du navigateur Mozilla Firefox.

Côté serveur, un logiciel, le serveur web, tourne en permanence et répond à toutes les requêtes envoyées sur un port logique, généralement le port 80, auquel le navigateur envoie ses requêtes HTTP[26]. Le système de port logique est un système qui permet à un même ordinateur d'avoir plusieurs services (web, e-mail, transfert de fichiers par FTP...) simultanément, chaque

25 C'est toujours le cas, bien que cette écriture ne soit plus considérée comme correcte dans les version récentes du HTML.

26 Ou le port 443 pour le HTTPS.

logiciel serveur ne répondant qu'aux requêtes reçues sur son propre port. Le serveur web reçoit du navigateur un certain nombre d'informations, dont l'adresse IP d'origine de la requête. Comme nous le verrons en étudiant l'importance au sein du W3C des discussions sur le « *fingerprinting* » (les empreintes digitales numériques), cette caractéristique de base du fonctionnement du Web engendre des risques en matière de protection de la vie privée. Le premier serveur web, httpd, a été développé au CERN par Tim Berners-Lee. Aujourd'hui, Apache, de la Fondation Apache, et *Internet Information Services* (IIS) de Microsoft sont les principaux serveurs web sur le marché.

Pour que tous les sites web s'affichent de la même façon sur tous les navigateurs et sur tous les ordinateurs, il est nécessaire qu'ils obéissent à des normes communes implémentées correctement. Or, en l'absence de référence commune, les navigateurs avaient commencé, dans les années 1990, à interpréter le HTML chacun à leur façon, ou à accepter des balises que les autres navigateurs ne connaissent pas.

Cet épisode de concurrence par les standards entre navigateurs web connut deux principaux épisodes dans les années 1990 : la « guerre » entre NSCA Mosaic et Netscape Navigator, puis la guerre entre Microsoft Internet Explorer et Netscape (Windrum, 2004). L'idée était d'exploiter sa position dominante sur le marché pour créer et imposer de nouvelles balises HTML que les navigateurs concurrents sont dans un premier temps incapables d'afficher. Cette stratégie joua à l'avantage de Microsoft, qui utilisa sa position dominante sur le marché des systèmes d'exploitation pour augmenter considérablement, dans la seconde moitié des années 1990, la diffusion de son navigateur, installé par défaut avec Windows, alors que Netscape Navigator devait être installé à part par l'utilisateur, et a fini par disparaître.

L'objectif du W3C est d'éviter ce type de morcellement du Web en créant un espace de délibération entre ses membres pour générer un consensus sur des standards communs, tout en ayant une politique de propriété intellectuelle mettant les acteurs basant leurs produits sur ces standards à l'abri de poursuites fondées sur le droit de la propriété intellectuelle (Contreras, 2016).

Le W3C a été fondé en octobre 1994 au MIT avec le soutien du CERN, de la DARPA et de la Commission européenne (Contreras, 2016 ; DeNardis, 2014 ; LCS, 1994). Dirigé par Tim Berners-Lee depuis sa création, il est le fruit de la collaboration entre le MIT et l'Institut national de recherche en informatique et automatique (INRIA), le CERN ayant dû abandonner son rôle dans le développement du web à cause de contraintes budgétaires imposées par la construction du Grand collisionneur de hadrons (Connolly, 2000). Le rôle de l'INRIA fut repris par l'*European Research Consortium for Informatics and Mathematics* (ERCIM), basé à Sophia Antipolis, en 2003. D'autres universités ont depuis rejoint le consortium : l'université Keio au Japon en 1996,

puis l'université Beihang, de Chine, en 2013. Ces universités sont les hôtes du W3C, c'est-à-dire qu'elles financent les postes administratifs des employés du W3C.

Au début, Tim Berners-Lee avait proposé à l'IETF de standardiser le HTTP et le HTML. Le HTTP est d'ailleurs toujours maintenu par l'IETF, et une première proposition de version 2 du HTML a même été proposée en 1995 à l'IETF par Tim Berners-Lee et Daniel Connolly dans la RFC 1866. Cependant, pour diverses raisons, il fut décidé de confier les standards du web, à l'exception du HTTP, au W3C. Notons au passage que les standards de ce consortium sont formellement appelés des « recommandations ». Informellement, à la fois dans les e-mails échangés sur les listes de diffusion et dans les entretiens réalisés dans le cadre de la présente recherche, les participants parlent aussi de « spécifications » (« *specifications* » ou « *specs* ») ou de « standards » comme synonymes du terme officiel du W3C « recommandation ».

Le modèle de financement et de participation du W3C est différent de celui de l'IETF. Au lieu de reposer essentiellement sur la participation d'individus, le W3C a pour membres des personnes morales, qui s'acquittent d'une cotisation, dont le montant varie en fonction de la nature de l'organisation, de ses revenus et de la richesse du pays où elle a son siège (W3C, non daté (b)). Chaque organisation membre envoie une ou plusieurs personnes pour participer à un ou plusieurs groupes.

Les groupes sont aujourd'hui de trois types :

- Les *Working Groups* sont des groupes qui disposent d'une charte et dont l'objectif est de développer un nouveau standard (ou d'en mettre à jour) ;
- Les *Interest Groups* sont des groupes de travail transversaux sur des thématiques comme la sécurité, l'accessibilité, l'internationalisation ou encore la protection de la vie privée ;
- Les *Community* et *Business Groups* sont des groupes qui ne sont pas officiellement approuvés par le W3C mais dont le W3C héberge sur ses propres ressources des espaces de discussion en ligne.

Ces groupes sont chapeautés par deux groupes permanents :

- Le *Technical Architecture Group* (TAG), créé en 2001, qui coordonne les activités techniques entre les différents groupes de travail et définit une stratégie de long terme sur l'avenir du web ;
- L'*Advisory Board* (AB), crée en 1998, qui sert de direction collégiale au W3C et édite notamment le « Process Document » (W3C Process), document qui précise les étapes à respecter pour faire adopter une nouvelle recommandation officielle du W3C.

L'*Advisory Committee* (AC) est une sorte d'assemblée générale, qui se réunie deux fois par an, et où chaque membre désigne un représentant (Alvestrand et Wium Lie, 2009). Un président directeur-général (*Chief Executive Officer*, CEO), actuellement Jeffrey Jaffe, est en charge de la direction administrative du W3C.

Une particularité du W3C par rapport à l'IETF est le recours au vote. Le consensus absolu n'est pas nécessaire pour adopter une recommandation, même s'il est préféré. Certains des membres du TAG sont élus, d'autres nommés par l'AB. Les membres de l'AB sont élus par les membres.

Entre la proposition initiale et l'adoption de la recommandation officielle, un texte passe à travers plusieurs étapes (W3C Process) :

1. D'abord est publié le premier brouillon public (*First Public Working Draft*)
2. Sont ensuite publiés un ou plusieurs documents de travail (*Working Drafts*)
3. Le document de travail devient ensuite une recommandation candidate (*Candidate Recommendation*)
4. Puis elle devient une proposition de recommandation (*Proposed Recommendation*)
5. Puis elle devient une recommandation officielle, publiée (*Published Recommendation*)
6. Ensuite, elle peut être éditée ou amendée (*Edited or Amended Recommendation*)

Un schéma, disponible en ligne sur le site du W3C, récapitule graphiquement ce processus :

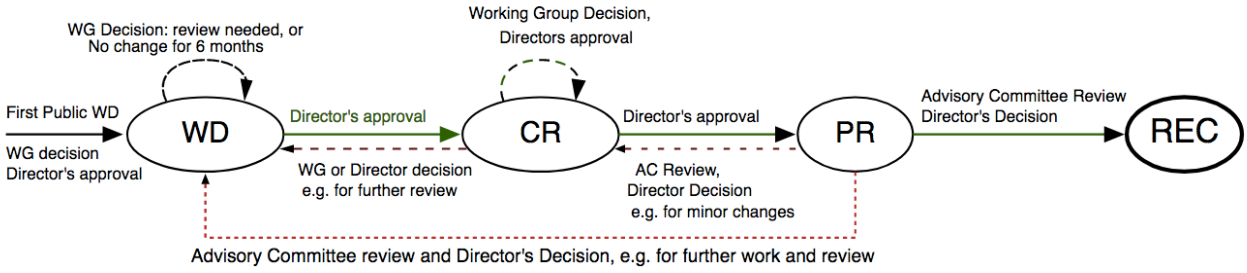


Figure 28 : *Le schéma de la procédure d'adoption d'une Recommandation du W3C (extrait du document W3C Process)*

Pour franchir chacune de ces étapes, une recommandation doit prouver son fonctionnement en disposant d'implémentations fonctionnelles, et recueillir l'approbation à la fois de la majorité de l'AC (donc des voix des membres), mais aussi celle du directeur, Tim Berners-Lee. Une procédure existe pour permettre de remettre en cause une décision du directeur (Sire, 2017), mais celle-ci n'a toujours pas été mise en œuvre. Comme pour d'autres projets[27], il existe au sein du W3C une fonction de « dictateur bénévole » (Russell, 2003 ; Sire, 2017).

Les discussions au sein des *working groups* ont lieu à travers plusieurs canaux de communication :

- Il existe des opportunités d'échanges de vive voix lors des « *Face to Face Meetings* » (F2F), qui ont lieu notamment lors du *Technical Plenary and Advisory Committee* (TPAC) annuel ou lors de conférences *ad-hoc* organisées par un groupe en particulier ;
- Il y a des réunions régulières en ligne, par téléphone, vidéoconférence, ou dans des salons de tchat fonctionnant sur le protocole *Internet Relay Chat* (IRC) ;
- Il existe des listes de diffusion d'e-mails, généralement publiques, dont le Process Document prévoit qu'elles ne peuvent qu'exceptionnellement être réservées aux membres, sans que nous ayons pu évaluer la fréquence d'utilisation de ces listes non-publiques par rapport aux listes publiques ;
- Il est possible d'utiliser des logiciels de *wiki* ou encore de *bug tracking* ou d'autres outils collaboratifs, dont l'usage varie d'un groupe à l'autre.

Au sein des groupes, certaines des décisions passent par un recours au vote. Cela fut le cas pour l'adoption de la version 1.1 de la recommandation P3P, par exemple, où un vote a eu lieu sur la *mailing-list* public-p3p-spec[28]. Cependant, là encore, si chaque groupe demeure libre d'adopter ses procédures dans sa propre *Decision Policy*[29], le *Process Document* montre que comme à l'IETF, le consensus est préféré au vote majoritaire pour la gestion des dissensus au sein des groupes :

> « Les groupes devraient privilégier les propositions suscitant les objections les plus faibles. Ces propositions sont préférées à celles soutenues par une large majorité mais qui suscitent des objections fortes de la part d'un petit nombre de personnes. Lorsqu'il est nécessaire de prendre une décision pour trancher un dissensus, il est attendu que le Président [*Chair*] doive notamment avoir connaissance des participants travaillant pour la même organisation Membre, ou des organisations membres liées, et mesurer leurs

27 Guido Van Rossum, l'inventeur du langage de programmation Python, est ainsi appelé depuis 1995 « Benevolent Dictator for Life » en raison du rôle qu'il joue dans le développement de ce langage (van Rossum, 2008).

28 Voir l'e-mail de Lorrie Cranor à la mailing-list public-p3p-spec du 27 octobre 2006.

29 Voir par exemple, pour le TPWG : W3C TPWG, 2012.

contributions en conséquence[30]. » (Section 3.3.1. du document W3C Process)

Chaque groupe est constitué de plusieurs types de participants.

Il peut avoir un ou plusieurs présidents (*chair*), qui, selon la section 5.1 du Process Document, sont nommés par le directeur du W3C, Tim Berners-Lee. Le président peut être le représentant d'un membre, un salarié du W3C[31], ou un expert invité par le directeur. Le président propose une charte pour le groupe et une feuille de route, peut inviter des experts à participer au groupe, maintient le contact avec le secrétariat (*staff*) du W3C, prépare les communiqués de presse, et doit s'assurer du bon déroulement des délibérations, c'est-à-dire du fait que celles-ci aboutissent à un consensus productif (Le Hégaret, s. d.). Il nomme également les éditeurs (*editor*), qui sont en charge de coordonner la rédaction des projets de recommandations sur lesquels le groupe travaille.

Chaque groupe se voit assigner un ou plusieurs salariés du W3C, à temps plein ou à temps partiel : ce sont les *Team contacts*, qui jouent à la fois un rôle de secrétariat et de coordination avec les autres groupes et la direction du W3C.

Le reste des participants sont les représentants envoyés dans le groupe par les membres, c'est-à-dire les personnes morales (associations, entreprises, établissements publics...) qui payent leur cotisation au W3C, ainsi que des experts invités, qui participent à titre individuel, mais sont cooptés et ne peuvent donc pas adhérer de leur propre chef.

Les documents officiels du W3C affichent un idéal de transparence des discussions. Cet idéal permet en pratique d'accéder à un grand nombre de documents en ligne, utiles pour analyser les échanges au sein des arènes du W3C. Dans les faits, il arrive malgré tout bien souvent que la phase de délibération publique n'intervienne qu'après une première phase de réflexion. Par exemple, HTML a d'abord été produit par le CERN puis formalisé pour faire l'objet d'une délibération publique. Le standard P3P a d'abord été le fruit d'un travail mené par le *Center for Democracy and Technology* (CDT) avant d'intégrer le W3C[32]. Cela découle du fait qu'il est nécessaire d'arriver avec un premier texte (*First Public Working Draft*) pour que soit créé un groupe de travail. Or, le niveau de transparence de cette phase de pré-standardisation est tout à fait variable, et il faut garder à l'esprit que l'imposition d'un standard développé en interne à l'ensemble d'une industrie procure à son inventeur un avantage compétitif important sur le marché. Ce contexte permet de mieux comprendre les ressources financières et humaines investies par de certaines entreprises (ou associations dans le cas de Mozilla) pour développer des

30 Traduit de l'anglais. Texte original : « Groups should favor proposals that create the weakest objections. This is preferred over proposals that are supported by a large majority but that cause strong objections from a few people. As part of making a decision where there is dissent, the Chair is expected to be aware of which participants work for the same (or related) Member organizations and weigh their input accordingly. »

31 C'est-à-dire un salarié d'une des universités hébergeant le W3C, affecté au W3C.

32 Cf. section 5.4.2.

navigateurs qui sont des logiciels complexes à maintenir, sensibles du point de vue de la sécurité, distribués gratuitement, et donc en général à perte.

L'autre motivation pour un membre du W3C de développer un navigateur est que cela lui confère un poids très largement prépondérant sur les autres acteurs.

Il faut en effet nuancer la portée pratique de l'idéal affiché de consensus horizontal délibératif en raison du poids disproportionné de ces membres qui contrôlent les logiciels appelés « *user agents* » dans le jargon du W3C. Ces « *user agents* », généralement des navigateurs web, outillent l'internaute dans sa navigation du web. Il est conçu et perçu, nous y reviendrons, comme devant permettre l'expression d'une agencéité de l'internaute. Or, pour qu'une recommandation du W3C ne reste pas lettre morte, il est indispensable que le standard soit mis en œuvre au moins par les principaux navigateurs web.

A ce sujet, un conflit majeur éclata au début des années 2000 entre Tim Berners-Lee et Ian Hickson, un ingénieur ayant travaillé chez Netscape (qui produisait le navigateur Navigator) puis pour Opera (qui édite toujours le navigateur Opera Browser) puis pour Google (qui a sorti son navigateur Chrome en 2008). Ian Hickson souhaitait produire une nouvelle version du HTML qui offre des fonctionnalités d'animation et d'interactivité le rendant substituable à Flash : le HTML 5. Tim Berners-Lee préféra orienter la discussion vers l'amélioration de l'interopérabilité autour du XTHML 2.0. Face au refus du directeur du W3C de créer le groupe de travail sur le HTML, Ian Hickson parvint à convaincre Apple, Mozzila, Opera puis Google, qui tous, étaient ou sont devenus des développeurs de navigateurs web, de créer une arène concurrente échappant au contrôle du W3C : le *Web Hypertext Application Technology Working Group* (WHATWG), aux procédures nettement plus souples que celles du W3C. En effet, le HTML du WHATWG est un standard « vivant », mis à jour régulièrement, au fil de l'eau, alors que le W3C fonctionne avec des versions incrémentales. L'avantage affiché de la façon de fonctionner du WHATWG est la réactivité et la vitesse d'innovation, là où celle du W3C est de favoriser l'interopérabilité en lassant entre chaque version le temps à chaque acteur de se mettre au niveau. Cela explique pourquoi, bien que le W3C ait finalement créé un groupe de travail HTML 5, qui a abouti entre temps à une recommandation officielle, et que donc le sujet initial de conflit ait disparu, le WHATWG n'ait toujours pas réintégré le W3C. Il y a donc aujourd'hui potentiellement deux versions concurrentes du HTML, et ce sont *in fine* aux producteurs de « *user agents* » de décider celle qu'ils préfèrent, sans que le W3C (ou tout autre organisme) n'ait de pouvoir contraignant sur ceux-ci (Sire, 2017).

Notre étude s'est focalisée sur l'arène du *Privacy Interest Group* (PING), dont la liste de discussion publique *public-privacy* a été crée le 19 juillet 2010. Sa charte date de juillet 2011

(W3C PING Charter), et sa première réunion, par téléconférence, a eu lieu le 19 avril 2012 (« *kick-off meeting* »).

Cette confusion autour de la date de création du PING illustre la difficulté à circonscrire temporellement et matériellement les limites des arènes du W3C. L'arène est-elle constituée par la décision institutionnelle ? Si c'est le cas, laquelle : celle de créer une liste de discussion ? Celle d'octroyer une charte officialisant le groupe ? Celle de réunir une réunion de lancement ? Par ailleurs, vu qu'il y a une différence, les membres d'un groupe sont-ils ceux qui sont listés sur la page web de présentation du groupe, ou bien ceux qui participent à la liste de discussion, ou bien aux réunions ? Nous aurons l'occasion de revenir sur ces interrogations dans le sous-chapitre suivant, dans lequel nous allons nous attarder sur une présentation détaillée du PING, de son fonctionnement, et de son interaction avec d'autres groupes du W3C.

Avant cela, nous commencerons par étudier quelques éléments sur le *Platform for Privacy Preferences Working Group* (P3P WG) afin de comprendre la façon dont les membres du W3C se sont saisis initialement de la question de la vie privée, et de retracer l'origine du parcours d'un certain nombre d'acteurs qui, à l'instar par exemple de Rigo Wenning, contribuent à être actifs dans ces arènes. Puis, en raison de sa contiguïté thématique, nous avons dû nous intéresser à certains des débats qui ont eu lieu au sein du *Tracking Protection Working Group* (TPWG), et en particulier aux débats autour de la définition du terme « tracking », qui fut un débat, en creux, sur la définition du terme « privacy ». Le PING n'ayant pas souhaité que soit débattue cette définition, et les groupes PING et TPWG étant constitués pour une part significative des mêmes personnes, il a été indispensable de décentrer un peu la focale du PING pour intégrer certaines discussions ayant eu lieu au sein du TPWG.

5.4. Les activités liées à la protection de la « vie privée » au W3C

5.4.1. Identifier les arènes de mise en débat de la « *privacy* » au cours du temps

Officiellement, le *Privacy Interest Group* (PING) a été créé en 2011 (W3C PING Charter). De 2011 à fin 2018 ou début 2019[33], il a coexisté avec le le *Tracking Protection*

33 La date exacte est difficile à établir. En effet, la charte du TPWG n'ayant pas été prolongée, ce groupe ne s'est pas réuni lors du TPAC d'octobre 2018 à Lyon. Officiellement, le groupe a tout de même continué à exister jusqu'à l'annonce de sa fermeture officielle le 17 janvier 2019 (*public-tracking*, e-mail de xueyuan du 17 janvier 2019). Le groupe a tout de même publié la dernière version d'une de ses spécifications, *Tracking Compliance and Scope*, le 22 janvier (W3C TCS). Au 9 janvier 2020, le dernier e-mail échangé sur la liste *public-tracking*, datait du 21 mai 2019 (*public-tracking*, e-mail de Mike O'Neill du 21 mai 2019)

Working Group (TPWG) (W3C TPWG Charter). Mais ces deux arènes ne sont pas les seules à avoir des discussions sur la « *privacy* » dans l'histoire du W3C. Pour comprendre leur formation, nous nous sommes intéressé à l'origine des premières discussions sur la protection de la « vie privée » au sein du W3C.

Grâce à des scripts réalisés sous Python et au traitement de données structurées dans des tableaux au format CSV importés dans le tableur de la suite LibreOffice, nous avons pu générer un graphe qui montre l'évolution au cours du temps de l'utilisation en valeur absolue du terme « *privacy* » dans 56 listes de discussion du W3C que nous avons téléchargées :

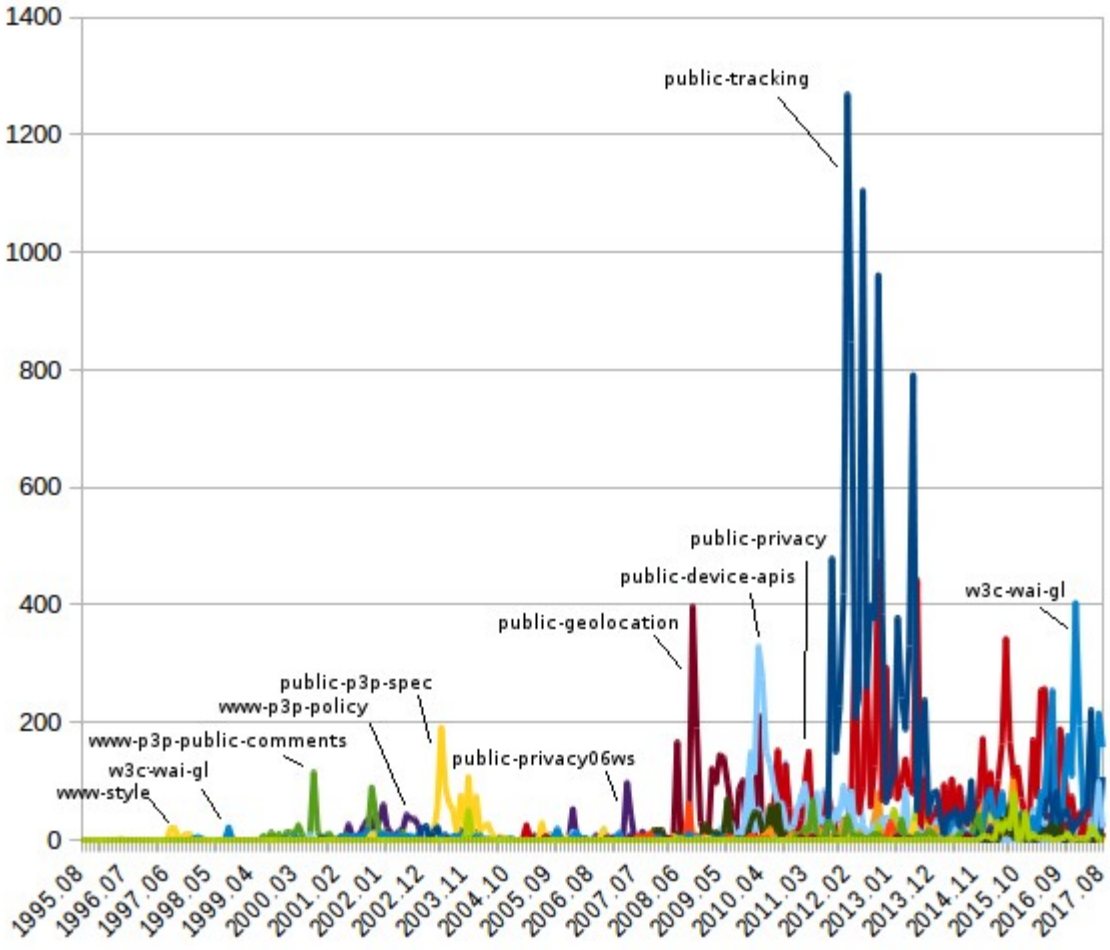


Figure 29 : *Nombre d'occurrences du mot « privacy » en valeur absolue entre août 1995 et octobre 2017 sur les* mailing-lists *téléchargées*

Le schéma ci-dessus nous permet de voir la fréquence d'emploi du mot « *privacy* », mais aussi la circulation de celui-ci entre les différents groupes du W3C. Il montre que quatre périodes sont à distinguer :

- Dans un premier temps, entre 1995 et 1997, voire la toute fin des années 1990, il n'y a pratiquement aucune activité autour de la « privacy[34] » ;
- Puis, de la fin des années 1990 au milieu des années 2000, nous observons le développement d'une activité sur la « privacy » uniquement dans les listes de discussion liées au projet *Platform for Privacy Preferences* (P3P) ;
- Cette activité est ensuite retombée au milieu des années 2000 ;
- Puis, à partir de 2008, nous observons d'abord le développement de discussions sur la « privacy » dans *public-geolocation* et *public-device-apis*, puis l'apparition de discussions sur *public-privacy* et *public-tracking*, respectivement les listes de discussion de PING et du TPWG, pendant que d'autres listes non-spécialisées sur le sujet continuent à discuter de « privacy ».

Nous nous intéresserons dans un premier temps au projet P3P[35], qui fut la première occasion pour le W3C de se saisir de la problématique de la protection de la « vie privée ». Un certain nombre d'acteurs, comme Rigo Wenning, Matthias Schunter ou encore Deirdre Mulligan étaient déjà actifs dans le projet P3P, et ont poursuivi leurs activités au sein d'autres groupes de travail, comme le TPWG ou le PING.

Nous verrons ensuite comment, après l'échec du projet P3P et une période où il n'a pratiquement plus été question de « vie privée » au sein du W3C, des controverses sont nées autour de projets de recommandations sur la communication des objets connectés, qui remit la question de la « vie privée » à l'agenda du W3C[36]. Deux groupes aux missions différentes ont alors été créés : PING[37] et le TPWG[38].

5.4.2. L'échec du projet *Platform for Privacy Preferences* (P3P)

Platform for Privacy Preferences (P3P) était un projet de standard techno-politique du W3C qui devait permettre à un internaute d'exprimer via son « *user agent* », c'est-à-dire son navigateur, ses préférences en matière de protection de sa vie privée. Il a été lancé par l'association *Center for Democracy and Technology* (CDT) avant d'intégrer le W3C avec l'appui de son fondateur, Tim Berners-Lee.

34 Le premier pic, dans www-style, a été ignoré car il correspond en fait à l'utilisation par quelques personnes de signatures PGP faisant apparaître les termes « PGP for Personal Privacy » en signature d'e-mails sans rapport thématique avec la vie privée (voir par exemple : www-style, e-mail de Liam Quinn du 1er juillet 1997).
35 Cf. section 5.4.2.
36 Cf. section 5.4.3.
37 Cf. section 5.4.4.
38 Cf. section 5.4.5.

CDT est une association états-unienne fondée en décembre 1994 (CDT, 1997). Sa mission est alors d'œuvrer pour la promotion des droits humains sur Internet. Selon un de ses membres que nous avons interrogé, sa mission originelle était de faire en sorte que l'architecture technique d'Internet se développe dans un sens favorable à l'exercice des libertés en ligne (entretien avec Joseph Hall).

L'*Internet Privacy Working Group* (IPWG), créé avec le soutien de CDT et de la *Federal Trade Commission*, est l'arène qui a vu la naissance du P3P (Berners-Lee, 1997). Il avait été mis en place par l'association CDT, qui a soumis formellement ses propositions au W3C en octobre 1997 (CDT, 1997). Ce groupe de travail réunissait des représentations d'associations comme CDT, *Consumers Union*, la *National Consumers League*, l'*Electronic Frontier Foundation*, des entreprises de l'industrie de l'informatique comme Microsoft, IBM, America Online, ou encore TrustE (devenue entre temps TrustArc, spécialisée dans les technologies de la vie privée) et des entreprises du secteur du marketing ou de la finance (*American Association of Advertising Agencies*, Experian, Citicorp *Credit Services*...). Certains des participants demeurent aujourd'hui actifs dans ce milieu, comme Deirdre Mulligan, ou encore David Singer.

Tim Berners-Lee a soutenu la proposition de CDT de créer un groupe au sein du W3C dédié à la rédaction d'une recommandation pour le standard P3P (Berners-Lee, 1997). Sa création fut officiellement annoncée le 23 mai 1997 (W3C, 1997).

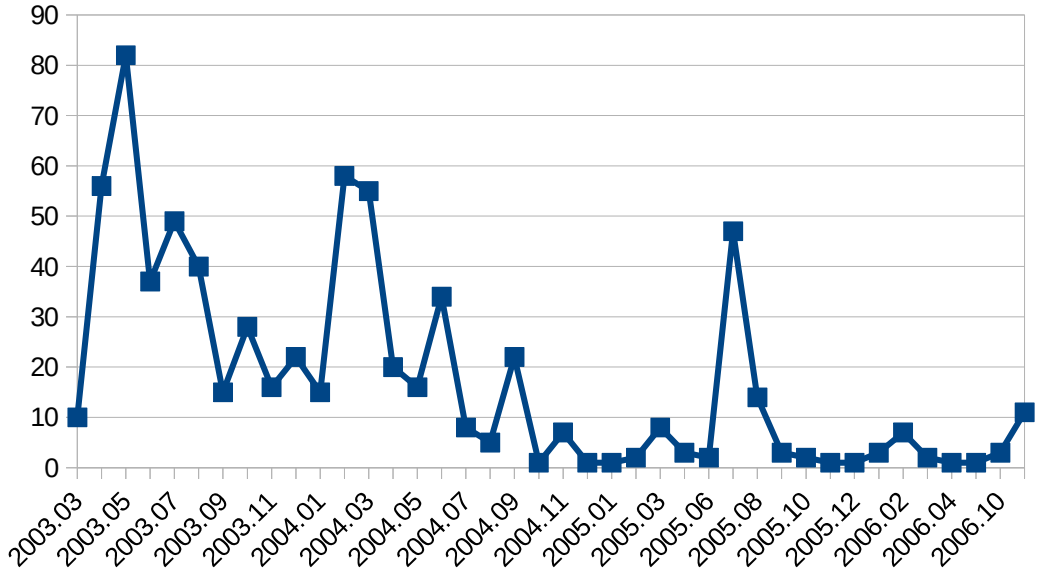
Techniquement, le projet P3P s'inspirait d'un autre projet : PICS, pour *Platform for Interest Content Selection* (Bennett et Raab, 2003, p. 151). Ce système avait pour but d'ajouter des métadonnées, des données de description, aux documents (pages, images...) web pour permettre aux navigateurs d'opérer un filtrage du contenu en fonction de critères déterminés par l'utilisateur. L'objectif était notamment de permettre de filtrer les contenus pornographiques, comme le rappelle un des enquêtés interrogés :

> « Pour comprendre le P3P, il faut commencer par PICS […]. Donc à l'époque les seuls, disons, […] en 97, […] qui faisaient de l'argent sur Internet ce n'était pas les GAFA mais les pornographes. Et […] il y avait partout, un peu partout dans les États, il y avait des efforts pour filtrer Internet […]. Et donc y avait le mouvement pour dire : tiens, pourquoi, puisque le principe de l'Internet, c'est que le réseau en lui-même, il est stupide, mais qu'il transporte, et que les terminaux sont intelligents, […] pourquoi pas avoir des terminaux qui peuvent déterminer que c'est images à caractère pornographique, et donc que je ne veux pas voir ? […] Mon navigateur est intelligent, et il les écarte. […] L'idée a transporté dans la vie privée […]. » (Entretien avec Rigo Wenning)

Une première démonstration de prototype est faite auprès de la Federal Trace Commission le 11 juin 1997 par Tim Berners-Lee. Voici à quoi ressemblait alors le prototype P3P dans Internet Explorer :

Figure 30: *Capture d'écran d'une boîte de dialogue P3P dans* Internet Explorer[39]

Le premier brouillon (« *draft* ») de recommandation P3P fut publié le 19 mai 1998. La première version officielle date du 16 avril 2002 (W3C P3P 1.0). Cependant, dans la pratique, P3P ne fut que très peu implémenté dans les navigateurs ou par les développeurs de sites web, coupant l'herbe sous le pied au projet. Progressivement, et malgré quelques pics d'activité, la discussion ralentit jusqu'à s'interrompre presque complètement à partir de septembre 2005 :



39 Image extraite de : https://web.archive.org/web/19980213181407/http://www13.w3.org:80/Talks/970612-ftc/ftc-mast.html (page visitée le 11 mai 2018)

Figure 31 : *Évolution du nombre de mails envoyés par mois sur la liste de discussion* public-p3p-spec[40].

En juillet 2005, à la suite de la découverte d'une erreur dans la première recommandation, la discussion reprit temporairement. Après une nouvelle année d'inactivité, les discussions reprirent pour publier une dernière version de P3P[41], la version 1.1 (W3C P3P 1.1), datée du 13 novembre.

L'e-mail du 22 novembre 2006 de Susan Lesch, salariée d'une des universités constituant le consortium du W3C, annonçant au nom de Tim Berners-Lee la fermeture du groupe P3P, marqua l'abandon définitif du projet P3P (public-p3p-spec, e-mail de Susan Lesch du 22 novembre 2006).

L'idée derrière de P3P, qui consistait à proposer une façon standardisée pour un utilisateur de communiquer ses préférences en matière de vie privée à un serveur, a été reprise dans d'autres projets. PRIME et PRIMELIFE[42], puis SPECIAL EU[43], des projets auxquels Rigo Wenning, recruté en 1999 par le W3C pour travailler sur P3P, a participé, s'en sont inspirés. Le projet de norme *Do Not Track*, permettant à l'utilisateur d'un navigateur web de signifier au site qu'il est en train de visiter qu'il ne souhaite pas être tracé, était une forme d'expression lisible par la machine simplifiée à l'extrême mais inspirée de la philosophie de P3P.

5.4.3. L'essor de l'Internet des objets et les controverses sur la « vie privée »

Les objets connectés sont des objets dotés d'un ordinateur qui leur permet de communiquer entre eux ou d'échanger des données sur Internet. Ensemble, ces objets, comme par exemple des téléphones, des montres, ou encore des voitures, constituent ce qui est généralement désigné comme l'Internet des objets. Équipés de capteurs, comme des gyroscopes, des accéléromètres ou encore des antennes GPS, ces objets sont autant de points de production de données qui, souvent, peuvent fournir des indications sur leurs utilisateurs. Ainsi, un téléphone portable connecté (un *smartphone*) peut stocker et transmettre un historique de coordonnées GPS qui permet de connaître de façon détaillée les déplacements de la personne qui le porte.

40 0,7 % des courriers sont ignorés à cause d'erreurs de lecture.
41 Voir l'e-mail de Lorrie Cranor, *chair* du groupe P3P, envoyé le 27 octobre 2006 et annonçant la demande de la direction du W3C de publier une version finale de la recommandation avant la fermeture du groupe.
42 Voir : http://primelife.ercim.eu/ (page consultée le 20 décembre 2019).
43 Voir : https://www.specialprivacy.eu/ (page consultée le 20 décembre 2019).

Les objets connectés se sont considérablement développés à partir de la fin des années 2000. Le W3C créa des groupes de travail dont la mission était de standardiser la façon de communiquer entre un objet connecté et un serveur web. La liste de discussion du futur groupe de travail sur la géolocalisation (*Geolocation Working Group*) a été crée en mai 2008. Son but est de rédiger une recommandation décrivant la façon dont un appareil pourrait communiquer à un serveur ses données de géolocalisation. En 2009, un autre groupe fut créé : le *Device APIs & Policy Working Group*, devenu en 2001 le *Devis APIs Working Group*. Ce dernier rédige des descriptions d'interfaces permettant à des sites web d'accéder à des informations sur le matériel du terminal. Typiquement, la *Battery Status API*, que nous avons déjà évoqué, a été développé par ce groupe, de même que par exemple l'API qui permet l'accès aux données du gyroscope et de l'accéléromètre.

Comme nous l'avions vu avec le schéma montrant l'évolution du nombre d'occurrences du mot « privacy » à travers le temps et les différentes listes de discussion du W3C, le groupe de travail travaillant sur l'API de géolocalisation a été le premier à voir revenir, en 2008, un pic d'activité pour ce terme. Selon l'une des personnes du PING avec qui nous avons réalisé un entretien, cela est dû au fait que les données de géolocalisation, une des premières générées par des capteurs connectés accessibles à des applications ou sites web, sont des données particulièrement sensibles, qui ont ravivé les discussions sur la protection de la vie privée au sein du W3C :

> « Je crois qu'il y avait juste un sentiment général, dans le monde de la standardisation, selon lequel la vie privée était en train de devenir un sujet de plus en plus pertinent, et qu'il y avait un écart entre son importance et les outils dont la communauté était équipée pour s'attaquer au [*address*] problème. […] De mon côté, j'avais travaillé très tôt sur la géolocalisation et je pense qu'il y avait un certain intérêt autour d'un sujet comme la géolocalisation. La géolocalisation est une question qui touche de façon viscérale le sens de la vie privée de certaines personnes. Et c'était l'un des premiers capteurs accessibles, largement accessibles aux logiciels, particulièrement aux logiciels Web. Donc le sujet de la vie privée en matière de géolocalisation [*geolocation privacy*] a attiré beaucoup d'attention médiatique, et […] je crois que c'est une des choses qui ont conduit à cet intérêt[44]. » (Entretien W3C5)

44 Traduit de l'anglais. Texte original : « I think there was just a general sense in like the standard setting space that privacy was just becoming a more relevant topic, and that there was a gap in how important it was and how equipped the community was to address it. […] For me I had done that early work on geolocation and I think that there was a fair amount of interest around a topic like geolocation. Geolocation is something that really gets in a visceral way to some people's sense of privacy. And it was one of the first sensors that was accessible, that was widely accessible to software, particularly web software. So you got a lot of press coverage on geolocation privacy, and […] I think that's another thing that sort of drove that interest. »

Quelques jours après la création de *public-geolocation* – la liste du groupe de travail sur la géolocalisation – Alec Bernston, de Microsoft, s'alarma des risques que le projet de recommandation allait selon lui engendrer pour la vie privée des utilisateurs (*public-geolocation*, e-mail d'Alec Berntson du 6 juin 2008). Il proposa de préciser une règle d'*opt-out* par défaut pour les utilisateurs, l'obligation d'afficher une alerte lorsque des données sont transmisses via l'interface de géolocalisation, d'inclure la possibilité pour l'utilisateur de définir un niveau de brouillage de la précision des données, et de rendre obligatoire la journalisation des accès aux données de géolocalisation. Nick Doty, qui allait jouer un rôle de premier plan dans le PING, contribua à la discussion en insistant sur la nécessité, selon lui, de demander systématiquement l'autorisation aux utilisateurs avant de recueillir via la *Geolocation API* ses coordonnées de géolocalisation (*public-geolocation*, e-mail de Nick Doty du 8 avril 2009).

Doug Schepers, employé du W3C, rappela cependant que, traditionnellement, c'est aux développeurs de navigateurs de se préoccuper des aspects d'interface utilisateur :

> « Cependant, je suis réticent à l'idée de trop édicter de règles sur les fonctionnalités de l'interface utilisateur [*UI: user interface*]… la décision revient habituellement plutôt à l'agent utilisateur [*UA: user agent*].
>
> L'équilibre entre sécurité et désagrément est toujours délicate à trouver[45]. » (*public-geolocation*, e-mail du 8 juin 2008)

Selon l'argument de ce dernier, les règles pour la protection de la vie privée n'auraient donc pas eu leur place dans la recommandation du W3C, car cela ne serait pas de sa responsabilité. Pour le contrer, l'association CDT, par l'intermédiaire de John Morris, se mêla à la discussion, pour rappeler au groupe de travail l'existence de discussions similaires et synchrones dans une autre arène : le groupe de travail Geopriv de l'IETF, où les discussions avaient débouché sur la conclusion que : « toute information sur la localisation DOIT être liée inextricablement aux règles sur la vie privée qui s'appliquent à l'information sur la localisation[46]. » (*public-geolocation*, e-mail de John Morris du 23 octobre 2006).

Finalement, la recommandation produite par le groupe contient bien un paragraphe intitulé « *Security and Privacy Considerations* » qui comprend l'obligation pour les *user agents* de recueillir le consentement de l'internaute avant de transmettre ses données de géolocalisation et ce, via une interface utilisateur (W3C Geolocation API).

---

45 Traduit de l'anglais. Texte original : « However, I am reluctant to dictate too much along the lines of UI features... traditionally, that's been mostly left to the UA to decide.
It's always a delicate balance between security and annoyance. »

46 Traduction de l'auteur. Texte original : « any piece of location information MUST be inextricably bound together with the privacy rules that apply to the location info ».

Des discussions similaires ont eu lieu dans le *Devive APIs & Policy Working Group*. Alissa Cooper et John Morris de CDT, avec l'aide de Frederick Hirsch de Nokia, éditèrent en 2010 un document appelé « *Device API Privacy Requirements* » dont le but est de servir de guide pour l'évaluation en matière de vie privée de chaque projet de recommandation du groupe (W3C Device API Privacy).

Avec ces controverses, pour la première fois, des discussions importantes ont eu lieu au sein du W3C au sujet de la protection de la « vie privée » en dehors des groupes dont cela est la mission principale. Depuis, des discussions ont régulièrement lieu à ce sujet dans un grand nombre de groupes de travail. La création du *Privacy Interest Group*, que nous allons maintenant présenter, ont eu pour effet de consolider la présence de discussions sur le sujet au sein de l'ensemble de l'organisation.

5.4.4. Le rôle et le fonctionnement du *Privacy Interest Group*

Contrairement au groupe P3P, et contrairement au TPWG avec lequel il a coexisté de 2011 à 2019, le *Privacy Interest Group* (PING) n'est pas un « groupe de travail » (« *Working Group* »), mais un « groupe d'intérêt » (« *Interest Group* »). Dans la terminologie du W3C, cela signifie que, comme par exemple le *Web Accessibility Initiative Interest Group* qui s'intéresse aux problématiques d'accessibilité, il n'a pas pour mission de produire des recommandations, mais d'alimenter par son expertise, sa réflexion et ses conseils le travail des « groupes de travail » qui, eux, en rédigent.

Du point de vue de ses participants, le PING structure une communauté de personnes partageant le même intérêt pour la protection de la vie privée :

> « Avoir le Groupe d'Intérêt était une sorte de : oh, soudain, ces personnes ont […] une sorte de façon organisée de penser le sujet de la vie privée et de soulever des questions à ce sujet, de travailler dessus[47]. » (Entretien W3C5)

> « Je pense que, de façon générale, nous tendons à constituer une petite communauté intéressée par la vie privée, qui s'en soucie, vous savez[48]. » (Entretien avec Joseph Hall)

47 Traduit de l'anglais. Texte original : « Having the Interest Group was just sort of: oh suddenly those people have […] some organised way of thinking about privacy and raising issues about it, and working on it. »

48 Traduit de l'anglais. Texte original : « I think generally we tend to be a little privacy interested community, that sort of cares, you know. »

Même si tout le monde n'en donne pas la même définition, ou si les motivations de l'engagement pour le groupe peuvent varier, tous partagent un engagement en faveur de la protection de la vie privée :

> « Le consommateur qui achète sur un site Internet ne sait pas clairement de quel type d'informations un site web dispose à son sujet […]. Je voulais utiliser cet alliage parfait [*perfect storm*] de ma situation [*where I was*], des personnes pour lesquelles je travaillais et des personnes dont j'étais entouré, pour ouvrir le débat sur la manière de rendre cela plus transparent[49]. » (Entretien avec Sid Stamm)

> « Je pense que c'est une sorte de […] lieu d'expression et repaire [*outlet*] pour des personnes déjà très impliquées dans la standardisation technique. Il s'agit de personnes travaillant pour de grandes entreprises technologiques [*big tech companies*], qui […] participent en permanence à différents groupes travaillant sur différentes fonctionnalités… certaines d'entre elles avaient depuis toujours réfléchi à la vie privée mais manquaient d'un cadre, d'une direction [*didn't have a good direction*], pour ça[50]. » (Entretien W3C5)

> « Et concernant mon travail sur la vie privée… je dirais que je traverse une sorte de purgatoire pour tous les péchés de ces années passées à développer des formats, des API et des protocoles présentant des risques pour la vie privée et la sécurité[51]. » (Entretien avec Frank Dawson)

L'e-mail de Susan Lesch annonçant au nom de Tim Berners-Lee, sur la liste de discussion publique *public-p3p-spec*, la fermeture du groupe de travail, annonçait déjà la création future d'un Privacy Interest Group :

> « Après le grand succès de l'atelier Ispra, la communauté a besoin de discuter davantage

49 Traduit de l'anglais. Texte original : « It's not clear to consumers who purchase something at a website what kind of information a website has about them […]. So I just kind of wanted to use that perfect storm of where I was, who I was working for, the people I was surrounded with, to start a discussion about how we can make that more transparent. »

50 Traduit de l'anglais. Texte original : « I think in some ways it's kind of an […] outlet for people who are already deeply involved in the technical standard-setting. These are people from big tech companies that are […] constantly participating in different groups working on different features … there are some of those people who have always been thinking about privacy and didn't have a good direction for it. »

51 Traduit de l'anglais. Texte original : « And my work on privacy... I sort of say I'm in purgatory pain for the sins of all those previous years of developing formats, API's, and protocols that had privacy and security risks. »

avant de se lancer dans de nouveaux travaux. L'Activité Vie Privée [*Privacy Activity*] s'attend donc à proposer un Privacy Interest Group constitué [*chartered*] pour discuter de prochaines étapes concrètes et maintenir une communauté de haut niveau sur la vie privée au sein de la W3C.[52] » (*public-p3p-spec*, e-mail de Susan Lesch du 22 novembre 2006)

Cette promesse a mis du temps à se concrétiser. Entre temps, en 2007, un *Policy Language Interest Group* (PLING) fut créé. Son objectif était à la fois plus large et plus spécifique que celui du PING actuel, puisqu'il ne s'agissait que de travailler sur des façons standardiser d'exprimer des « politiques » (« *policies* »), mais pas uniquement sur des questions de « *privacy* ». Son existence fut éphémère, puisqu'il disparut en 2011, et surtout, elle a correspondu à la période pendant laquelle, entre 2006 et 2008, le W3C n'a connu que très peu de discussions et activités liées à la protection de la vie privée.

La liste de discussion *public-privacy* fut créée le 19 juillet 2010[53]. PING obtint sa charte en juillet 2011 (W3C PING Charter). La première réunion officielle du PING a eu lieu le 19 avril 2012, sous la co-présidence de Tara Whalen et de Christine Runnegar (*public-privacy*, e-mail de Christine Runnegar du 13 avril 2012).

La première section de la Charte du PING définit ainsi sa mission :

« Afin d'accroître la prise en charge de la protection de la vie privée dans les standards du Web, le Privacy Interest Group (PING) s'intéressera de manière très large aux enjeux de la vie privée sur le Web et aux méthodes pour répondre de façon systémique aux inquiétudes soulevées par les questions de vie privée sur le Web dans le processus de standardisation.

Le groupe envisagera et discutera toute question relative à la vie privée et affectant les utilisateurs du Web. Cela peut inclure, sans s'y limiter, des questions concernant : le pistage en ligne [*online tracking*], les données de localisation, de santé et financières, les initiatives d'administration électronique [*eGovernment*], ainsi que le réseautage social et l'identité en ligne. Lorsque cela sera approprié, le groupe fera des recommandations sur des points pour lesquels le W3C devrait entamer un processus de standardisation relatif à des questions de vie privée, et pourra développer des prototypes, ou initier ce type de travail au sein du groupe.

De plus, le Groupe d'Intérêt [*Interest Group*] développera et documentera des lignes directrices, des modèles [*patterns*], des processus et des bonnes pratiques pour traiter [*for addressing*] les considérations de vie privée [*privacy considerations*] dans les standards du Web. Le Groupe d'Intérêt pourra fournir un lieu d'expertise [*locus of expertise*] pour

52 Traduit de l'anglais. Texte original : « After the very successful completion of the Ispra Workshop, there is a community that needs more discussions before starting further work. So the Privacy Activity expects to propose an Privacy Interest Group chartered to discuss concrete next steps and to maintain the high level community around privacy in W3C. »

53 Voir le premier e-mail sur la liste, envoyé par Thomas Roessler le 19 juillet 2010.

aider (proactivement ou réactivement) la réflexion sur des questions relatives à la vie privée émergeant dans d'autres travaux de standardisation du W3C[54]. » (W3C PING Charter)

Alors que le TPWG a repris le projet, abandonné avec l'échec de P3P, de créer un standard techno-politique de protection de la « vie privée » des internautes, PING se spécialisa dans un autre type d'activité : devenir le lieu de concentration d'une expertise sur le sujet au service des groupes de travail du W3C. Comme l'expliquaient certains enquêtés en entretien :

« Le conseil a toujours existé. Donc auparavant, c'était le groupe P3P qui était bourré d'experts vie privée qui faisait du conseil à côté. […] Ce qu'on voit en 2010 […] et j'ai aussi supporté, encouragé ce développement, c'est [la séparation de] la discussion générale sur la vie privée et sur la vision de la vie privée sur Internet des avancées techniques concrètes. » (Entretien W3C8)

« Je crois que nous avons essayé de faire du Privacy Interest Group une sorte de cabinet de conseil [*consultancy*] pour les autres groupes. Et je crois que nous avons atteint un succès mitigé, mais il y a tout de même eu un certain nombre d'interactions. Un groupe dira par exemple : 'tiens, nous travaillons sur une nouvelle fonctionnalité avec probablement un problème relatif à la vie privée, nous préférerions en avoir connaissance plutôt tôt que tard. Alors allons en discuter avec le Privacy Interest Group et voyons ce que nous pouvons faire'.[55] » (Entretien W3C5)

Il existe des discussions sur la nature de cette activité de conseil. Pour Frank Dawson, ingénieur chez Nokia, et rédacteur du document du PING « *Specification Privacy Assessment* » (W3C SPA), chaque document de travail du W3C ayant vocation à devenir une recommandation

54 Traduit de l'anglais. Texte original : « In order to improve the support of privacy in Web standards, the Privacy Interest Group (PING) will broadly investigate ongoing Web privacy issues and methods of systematically addressing privacy concerns during the standardization process.
The group will consider and discuss any privacy issues that affect users of the Web. This may include, but is not limited to, issues related to: online tracking; location, health and financial data; eGovernment initiatives; and online social networking and identity. Where appropriate, the Interest Group will recommend areas where W3C should begin recommendation-track standards work on privacy issues and may prototype or initiate such work within the group.
Additionally, the Interest Group will develop and document guidelines, patterns, processes and best practices for addressing privacy considerations in Web standards. The Interest Group may provide a locus of expertise to help consider (proactively or reactively) privacy issues that arise in other W3C standards work. »

55 Traduit de l'anglais. Texte original : « I think we try to make the Privacy Interest Group almost kind of like a consultancy for other groups. And I think we've got mixed success with that, but there has been quite a bit of interaction where some other group says: oh, we're working on a new feature, we probably think there is some privacy issue, we'd like to know about it earlier rather than later. So let's gonna talk to the Privacy Interest Group. And we can sort of figure it out. »

devrait être soumis de façon obligatoire à un processus d'évaluation d'impact complet[56], inspiré de ce qui est devenu l'article 35 du RGPD, et qui pourrait être réalisé par ou avec l'aide du PING :

> « Nous avons donc pensé […], si on regarde les standards en cours d'élaboration : pourquoi est-ce qu'on n'exigerait pas une évaluation d'impact vie privée [*privacy impact assessment*] de ces standards, comme nous pourrions l'exiger de la part d'entreprises et de leur technologie ? Pourquoi n'existe-t-il pas d'approche systématique d'évaluation de l'impact de ces standards sur la vie privée[57] ? » (Entretien avec Frank Dawson)

L'engagement des membres du PING en faveur de la protection de la « vie privée » est souvent supérieur à celui de leurs employeurs. Dans ces conditions, il n'est pas toujours facile d'obtenir d'y consacrer une part importante de son temps de travail. Plusieurs enquêtés, dont Frank Dawson lui-même, ont ainsi fait remarquer que le caractère volontaire voire bénévole de la participation au PING rendait difficile le fait de dégager suffisamment de temps de travail pour réaliser efficacement des évaluations d'impact complètes dans des délais qui conviennent à la temporalité des groupes de travail produisant des recommandations :

> « Il y a eu un engagement, au moins de la part du Directoire [*Board*] du W3C, que tous les standards devraient passer par le PING dans le cadre de leur processus de publication. […] Et ensuite, ils deviennent très frustrés parce qu'ils disent : notre planning prévoyait une publication pour hier et vous êtes tous trop lents dans votre examen. Il s'agit d'une participation volontaire.[58] » (Entretien avec Frank Dawson)

> « Tout ceci est basé sur un travail bénévole. Si vous voulez qu'un travail soit fait, il faut en quelque sorte persuader les membres du groupe de travail de travailler réellement. Et étant donné que c'est volontaire, ce n'est pas chose aisée. […] Vous allez donc évidemment être

56 Le TAG du W3C a, depuis l'entretien, modifié son questionnaire sur la sécurité et la vie privée de 2015 (W3C TAG Security and Privacy 2015) pour y ajouter une obligation pour tous les groupes de travail d'y répondre avant que leurs recommandations ne soient adoptées (W3C TAG Security and Privacy 2019). Cette modification a eu lieu notamment à l'initiative de Łukasz Olejnik, membre du PING élu membre du TAG en janvier 2018. Comme elle est intervenue après que nous avons terminé notre enquête de terrain sur le W3C, nous ne pouvons toutefois pas juger la portée de cette obligation. Notons par ailleurs que contrairement au document édité par Frank Dawson, ce questionnaire ne se présente pas non plus comme une procédure complète d'évaluation d'impact.

57 Traduit de l'anglais. Texte original : « So we thought […], if you look at standards that are being developed, why do we not require a privacy impact assessment of those standards in the same way that we could of companies and their technology? Why isn't there a systematic approach to evaluating the privacy impact in the standards? »

58 Traduit de l'anglais. Texte original : « There has been a commitment at least of the W3C Board that all standards should go through PING as part of their publication process. […] And then they get very frustrated, because they say: our schedule for publication was yesterday and you all are so slow in reviewing. It's a voluntary participation »

> approché par des gens qui veulent que vous examiniez leurs spécifications. […] Mais ces personnes veulent obtenir de bons conseils, et les obtenir dans des délais raisonnables.[59] » (Entretien W3C10)

Une autre limite importante à la portée du travail du PING est que ses avis, et même le simple fait de demander son avis, sont facultatifs.

Cela n'a pas empêché le PING de développer des guides destinés à aider les autres groupes de travail à rédiger des recommandations qui protègent la « vie privée » des utilisateurs du Web. Il existe un document qui propose une méthode pour évaluer si et de quelle manière une nouvelle recommandation peut augmenter la surface d'empreinte digitale numérique (*digital fingerpint*[60]) d'un navigateur (W3C Fingerprinting Guidance). Selon Nick Doty, son rédacteur :

> « Il peut arriver qu'une seule API souhaite ajouter une fonctionnalité en particulier et que cela seul puisse faire une différence énorme en termes de fingerprinting[61]. » (Entretien W3C5)

Régulièrement, une nouvelle recommandation est publiée, qui permet, une fois mise en œuvre par les navigateurs, de transmettre de nouvelles informations aux navigateurs. Ce fut le cas par exemple de la *Battery Status API*, dont nous avons déjà parlé[62], et qui permet à un serveur distant de connaître l'état de charge de la batterie et, si ces données sont assez précises, de générer un profil de cette batterie (Olejnik et al., 2015).

Un autre document donne des indications aux groupes de travail sur la façon de rédiger une section sur la protection de la vie privée (W3C Privacy Considerations). Ce type de documents sert aussi à cadrer la méthode commune de travail au sein de PING pour évaluer les

---

59 Traduit de l'anglais. Texte original : « All of this is based on volunteer labour. If you want there to be any work done at all, you sort of need to be able to persuade the people who have signed up for the interest group to actually do work. And that's not a small thing given that it's all volunteer labour. […] So clearly, you're going to be approached by folks who want you to do reviews of their specs. […] But all those, they want to receive good advice, and they want to receive good advice in a timely fashion. »

60 Le *fingerprinting* est une technique qui vise à identifier de façon unique un internaute en se fondant sur les informations techniques transmises par le navigateur au serveur web visité, comme les préférences linguistiques, la version du navigateur, ou encore le système d'exploitation utilisé. L'*Electronic Frontier Foundation* (EFF) a mis en place un site web appelé Panopticlick qui permet de tester à quel point l'empreinte digitale numérique d'un internaute est unique, à partir de l'ensemble des données qui lui sont transmises par le navigateur : https://panopticlick.eff.org/ (page consultée le 9 janvier 2020).

61 Traduit de l'anglais. Texte original : « It sometimes happens that a single API wants to add a particular feature and that that alone could make a huge difference for fingerprinting. »

62 Cf. section 5.2.4.

projets de recommandations qui lui sont soumis[63]. Car bien que le PING ne soit pas parvenu à atteindre l'objectif que Frank Dawson aurait voulu qu'il atteigne, par la mise en place d'évaluations d'impact complètes et systématiques, ce groupe est effectivement devenu un lieu reconnu d'expertise et de conseil sur la protection de la vie privée dans la standardisation du Web. Par exemple, le 28 avril 2018, Léonie Watson, du *Web Platform Working Group*, a envoyé un e-mail sur la *mailing-list public-privacy* pour obtenir une évaluation en matière de protection de la vie privée du projet de version 5.3 du HTML (*public-privacy*, e-mail de Léonie Watson du 26 avril 2018). D'autres projets, comme *Web Audio API* et *Ambient Light API* ont fait l'objet d'une même démarche.

Nous avons voulu voir quelle était la centralité du PING dans l'écosystème des groupes du W3C. Nous avons choisi comme indice de cette centralité la participation des personnes qui échangent sur *public-privacy* à d'autres listes de discussion, liées à d'autre groupes, et vice-versa, la participation des participants à ces autres listes à *public-privacy*.

Nous avons réalisé une cartographie à l'aide de scripts Python et de Gephi à partir de l'ensemble des e-mails des *mailing-lists* que nous avons téléchargées. Chacune est représentée par un nœud. Les liens entre les nœuds représentent le nombre de personnes qui participent aux deux *mailing-lists*. Cette cartographie est approximative, puisqu'en particulier, comme nous l'avons vu en section 1.2.5.3, certaines personnes utilisent plusieurs adresses e-mail. De plus, certains groupes ont des *mailing-lists* accessibles seulement à leurs membres. Il existe quelques cas d'envoi de spam, et, pour finir, tous les groupes n'ont pas été actifs aux mêmes époques. Or, l'image ci-dessous concatène toute l'histoire des échanges de mails publics sur les *mailing-lists* du W3C téléchargées en un seul schéma.

Le graphique ci-dessous permet de visualiser que PING occupe effectivement une place très centrale, bien plus que ne l'était la liste de discussion du PLING, qui l'a précédée, ou même celle du TPWG :

63 Entretien W3C1.

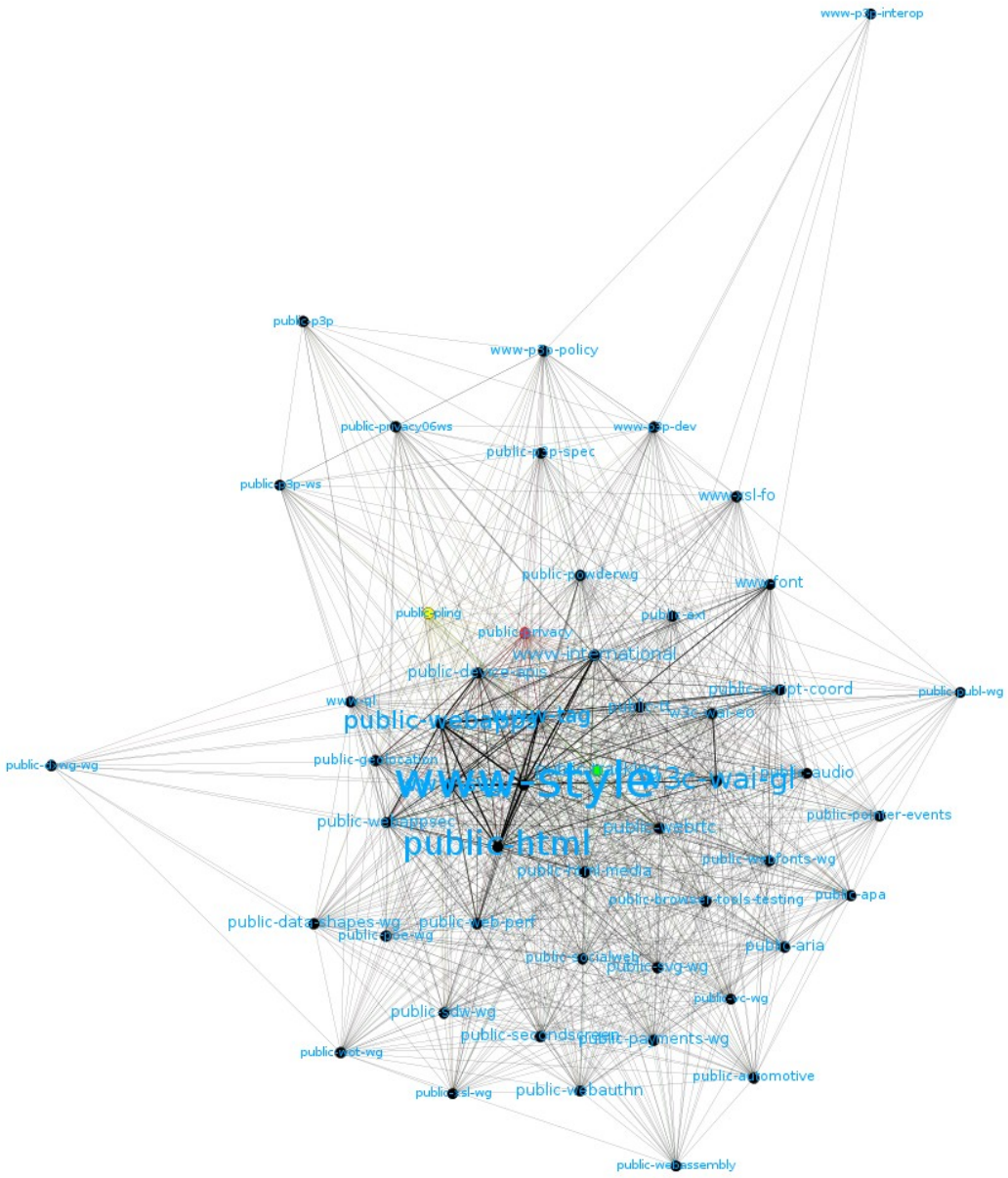


Figure 32 : *Schéma des liens interpersonnels entre listes de diffusion du W3C.* Public-pling *est en jaune,* public-privacy *en rouge et* public-tracking *en vert. La taille du texte donne une indication sur le nombre total d'e-mails échangés sur la mailing-list représentée par le nœud.*

Notons que le W3C PING entretient des relations avec d'autres groupes de standardisation d'Internet qui ont une mission dans le domaine de la protection de la vie privée. Les relations avec l'IETF, qui a sa *mailing-list ietf-privacy*, sont particulièrement fortes. Le document *Fingerprinting Guidance for Web Specification Authors* (W3C Fingerprinting Guidance) cite explicitement la RFC 6973 (Cooper et al., 2013). Hans Tschofening est co-auteur des deux

documents. Enfin, en 2010 et en 2014, deux rencontres réunissant l'*Internet Architecture Board*, l'IETF et le W3C ont eu lieu sur le thème de la « *privacy*[64] ».

Surtout, tant que le TPWG existait, le PING a entretenu de très étroites relations avec lui. Au-delà même de la composition officielle de ces groupes, qui montre qu'en 2016, 43 membres du TPWG sur 70, soit près des deux-tiers, étaient aussi membres du PING, les participants à la liste *public-privacy* ont aussi souvent participé à *public-tracking* et vice-versa, sans être forcément membres des deux groupes. Une controverse engagée sur une liste pouvait se poursuivre sur l'autre, et les discussions d'une liste avaient souvent une incidence sur l'autre liste. Cela s'explique par le fait que bien que leurs missions précises aient été différentes, avec un PING qui fournit de l'expertise et du conseil pour améliorer les recommandations écrites par d'autres et un TPWG qui travaillait sur un projet de standardisation techno-politique, les deux groupes avaient un même objectif commun : améliorer la protection de la « vie privée » des internautes utilisant des outils techniques fondés sur les standards du W3C.

5.4.5. Le *Tracking Protection Working Group* et le projet *Do Not Track*

Le *Tracking Protection Working Group* (TPWG) est un groupe qui, de 2011 à 2019, a tenté de produire un standard technique autour d'un projet dénommé *Do Not Track* (DNT). L'objectif de ce dernier était de créer un mécanisme qui permette à un internaute d'indiquer à un site web sur lequel il se connecte son désir d'être ou de ne pas être pisté à travers un choix configurable dans l'interface graphique de son navigateur web.

La première formulation d'une idée désignée par la formule « *Do Not Track* » émane d'une note rédigée ensemble par plusieurs associations, dont CDT et l'*Electronic Frontier Foundation*, et transmise à la FTC en vue d'une réunion à Washington D.C. les 1 et 2 novembre 2007 (Schwartz et al., 2007). Les auteurs de ce *position paper* y invitaient la FTC à établir une liste nationale « *Do Not Track* ». Cette liste serait fondée sur le même principe que le registre « *Do Not Call* », qui est la liste rouge, aux États-Unis, des personnes ne souhaitant pas faire l'objet de démarchage téléphonique. L'idée fut reprise par le président de la FTC lors d'une audition au Sénat de 2009[65] (Leibowitz, 2010).

64 Cf. la chronologie des actions en matière de « *privacy* » dans les arènes de standardisation technique d'Internet en annexe 10.

65 Le rapport ne mentionne pas de « *Do Not Track* » mais, selon des témoignages, cette formule aurait été évoquée à l'oral par le président de la FTC sans être rapportée à l'écrit. Voir : (Soghoian, 2011).

Toujours en 2009, Christopher Soghoian et un ingénieur de la fondation Mozilla que nous retrouvons au TPWG et au PING, Sid Stamm, ont créé un premier prototype d'extension pour le navigateur web Firefox mettant en œuvre cette idée.

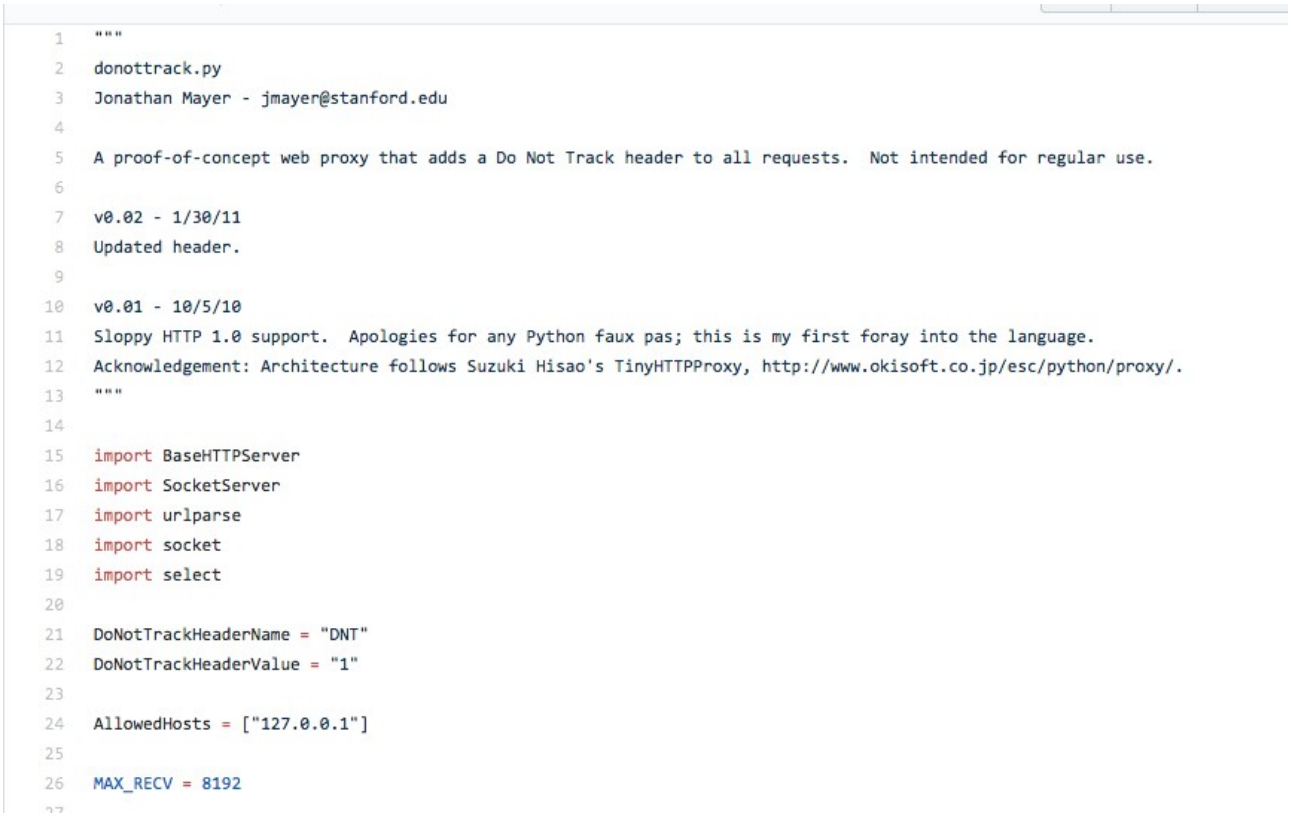
Lorsqu'un navigateur souhaite accéder à un site web, il émet une requête, qu'il transmet au serveur web. Cette requête est un texte qui comprend certaines informations, formatées dans un format lisible par le serveur. Celui-ci renvoie alors la page web, précédée d'un en-tête, qui est un texte lisible par le navigateur et qui lui permet d'indiquer un certain nombre d'informations.

L'idée était simple : au lieu que chaque site web permettant à l'internaute de choisir de ne pas être tracé enregistre ce choix par un cookie qui n'est pas reconnu par les autres sites, il serait plus simple qu'il existe une expression unifiée de consentement à être tracé. Ceci peut se faire à travers une reconfiguration des navigateurs web, dont l'interface pourrait proposer une case à cocher dans l'outil de configuration du navigateur. Cette information serait transmise à travers le HTTP (RFC 1945 et RFC 2616) en ajoutant des informations dans de nouveaux champs dans lesquels seraient renseignés la préférence éventuelle d'un internaute de ne pas être « tracé ».

Dès août 2010, David Singer de chez Apple aborde le sujet du DNT dans un e-mail sur la mailing-list *public-privacy* (public-privacy, e-mail de David Singer du 2 août 2010).

Jonathan Mayer, chercheur à l'université de Stanford, qui par la suite fut très actif dans le TPWG, rédigea peu de temps après un logiciel en Python permettant d'ajouter cette information aux requêtes HTTP émises depuis l'ordinateur de l'internaute. Cette information, désormais notée « DNT:1 », opèrait une simplification du signal initialement proposé par Sid Stamm et Christopher Soghoian (Soghoian et Stamm, 2009), qui, elle, distinguait l'expression de la volonté de ne pas voir affichées de publicités comportementales de celle de ne pas être tracé. Une première version de son script fut mise en ligne sur Github fin 2010[66].

66 Voir son dépôt sur le site Github à l'URL : https://github.com/jonathanmayer/Do-Not-Track/commit/615f4faacede47567adc6fa43edb972aa6cc2636 (page consultée le 20 avril 2020)



```
"""
donottrack.py
Jonathan Mayer - jmayer@stanford.edu

A proof-of-concept web proxy that adds a Do Not Track header to all requests.  Not intended for regular use.

v0.02 - 1/30/11
Updated header.

v0.01 - 10/5/10
Sloppy HTTP 1.0 support.  Apologies for any Python faux pas; this is my first foray into the language.
Acknowledgement: Architecture follows Suzuki Hisao's TinyHTTPProxy, http://www.okisoft.co.jp/esc/python/proxy/.
"""

import BaseHTTPServer
import SocketServer
import urlparse
import socket
import select

DoNotTrackHeaderName = "DNT"
DoNotTrackHeaderValue = "1"

AllowedHosts = ["127.0.0.1"]

MAX_RECV = 8192
```

Figure 33 : *Apparition du signal « DNT:1 » dans le code source d'un logiciel développé en Python en janvier 2011 par Jonathan Mayer. Capture d'écran réalisée à partir de la page https://github.com/jonathanmayer/Do-Not-Track/blob/master/proxy/donottrack.py le 11 mai 2018*

C'est autour de ce signal DNT:1 que sont construits aujourd'hui les projets de recommandations du TPWG (W3C TPE et W3C TCS), partiellement implémentés par certains navigateurs web, comme Firefox. Voici par exemple une requête HTTP (effectuée le 11 mai 2018) typique, envoyée par le navigateur Firefox au serveur web utc.fr pour charger sa page d'accueil :

```
Host: www.utc.fr

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:61.0)
Gecko/20100101 Firefox/61.0

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate, br

DNT: 1

Connection: keep-alive
```

```
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

L'activation du signal « DNT: 1 » se faisait dans Firefox par le biais de cette interface :

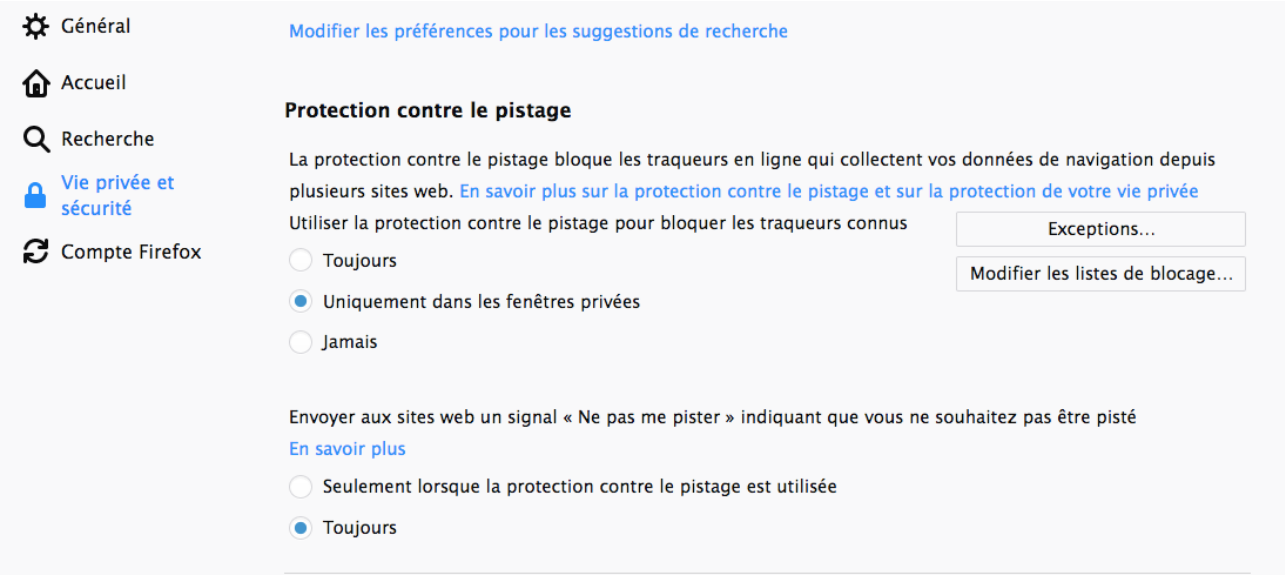


Figure 34 : *Extrait d'une capture d'écran de Firefox version 61 montrant l'activation du signal DNT:1*

Le 8 février 2011, David Vladeck, directeur du bureau de la protection des consommateurs de la FTC publia un communiqué de presse (FTC, 2011) appelant expressément les différents acteurs de l'industrie, et notamment de l'industrie du marketing en ligne, à se mettre autour de la table pour adopter un standard interopérable permettant à un internaute d'exprimer sa volonté de ne pas être tracé. Dans celui-ci, il rappela que « la publicité comportementale soulève de sérieuses inquiétudes relatives à la vie privée[67] » (FTC, 2011, p. 1). Puis, il formula la proposition suivante à l'attention de l'industrie de la publicité en ligne : soit elle acceptait de négocier un accord autour du projet de standard *Do Not Track* et elle le respectait, soit la FTC se prononcerait en faveur de l'adoption d'une loi contraignante par le Congrès, à l'instar d'une proposition de loi qui avait été déposée par le député démocrate Jackie Speier le 11 février 2011[68] (Vladeck 2011, p. 2-4).

67 Traduction de l'auteur. Texte original : « behavioral advertising raises serious privacy concerns ».
68 Il s'agit du Do Not Track Me Online Bill.

Le 24 février 2011, Microsoft déposa formellement un projet de « *Web Tracking Protection* » auprès du W3C, signé par trois employés : Andy Zeigler, Adrian Bateman et Eliot Graff. L'abstract de cette proposition la résume :

> « La spécification Web Tracking Protection (NDT : *Protection contre le pistage Web*) est conçue pour permettre aux utilisateurs de refuser le pistage [*tracking*] en ligne. Cette plate-forme est conçue en deux parties :
>
> - Des listes de filtrage, qui permettent d'exécuter les préférences de vie privée de l'utilisateur en empêchant l'agent utilisateur [*user agent*] d'effectuer des requêtes indésirables aux serveurs Web qui pistent les utilisateurs.
> - Une préférence utilisateur, sous forme d'en-tête HTTP et de propriété DOM, à utiliser par les serveurs Web pour respecter la vie privée de l'utilisateur.
>
> Ensemble, ces technologies peuvent être utilisées pour faire respecter la vie privée des utilisateurs et donner accès à du contenu et à des services qui respectent les préférences des utilisateurs en matière de vie privée[69]. » (Zeigler, Bateman et Graff, 2011)

Le même jour, Thomas Roessler annonça sur *public-privacy* la proposition de Microsoft.

Cette séquence, sur fond de forte implication de la FTC, converge avec le témoignage d'un des enquêtés lors de notre campagne d'entretiens avec des participants au PING :

> « À la base, c'était tout simplement politique. Il n'y avait aucune, genre, action de réglementation ou d'application de la Loi formelle qu'ils auraient prise. Mais la FTC publiait d'une certaine façon des rapports sur des domaines d'intérêt, et a particulièrement insisté sur des recommandations en rapport avec le Do Not Track. Je crois que c'était dans un rapport de 2010. Je pense que c'est un changement assez important pour le secteur aux États-Unis. Cela ne garantit rien, mais lorsque la FTC dit vraiment : 'il faut faire quelque chose'… alors ça suffit à regrouper des gens et réfléchir ensemble à quelque chose. Et la FTC a également envoyé des participants, donc elle s'est activement impliquée dans les discussions. Donc… enfin je pense que c'est quelque chose de peu commun pour la FTC.

69 Traduit de l'anglais. Texte original : « The Web Tracking Protection specification is designed to enable users to opt-out of online tracking. The platform has two parts:
- Filter lists, which can enforce user privacy preferences by preventing the user agent from making unwanted requests to webservers that track users.
- A user preference, which is an HTTP header and a DOM property, to be used by webservers to respect the user's privacy.

Together these technologies can be used to enforce privacy protection for users, and provide access to content and services that respect user privacy preferences. »

> Mais ils ont envoyé des participants très impliqués dans les discussions du Tracking Protection Working Group. Quant aux commissaires… je ne sais pas à quel point vous connaissez la structure de la FTC. Mais il y a jusqu'à cinq commissaires. Les commissaires faisaient des discours à ce sujet. Un commissaire a participé à l'une de ces réunions d'élaboration de standards. Cela envoyait un signal fort, montrant que la question était une priorité[70]. » (Entretien W3C5)

Parallèlement à la création du groupe au W3C, Jonathan Mayer, Arvind Narayanan et Sid Stamm proposent à l'IETF un brouillon intitulé « *Do Not Track: A Universal Third-Party Web Tracking Opt Out* », daté du 7 mars 2011 (IETF draft-mayer-do-not-track-00). Mais c'est finalement le W3C qui hébergea les discussions sur le Do Not Track, et non l'IETF. Selon Sid Stamm, interrogé à ce sujet :

> « C'était après que l'IETF eut dit que ce n'était pas pour eux, car ce n'est pas une question de protocole mais plutôt une question de société. Je n'avais pas de préférence concernant l'organisme de standardisation qui traiterait de la question tant que l'on pouvait réunir toutes les parties prenantes et qu'elles s'accordaient sur la manière de communiquer cette préférence[71]. » (Entretien avec Sid Stamm)

La fondation Mozilla annonça ensuite l'implémentation du *Do Not Track* dans son navigateur Firefox le 30 mars 2011. Le site web *AP Press*, et celui de la *Digital Advertising Alliance* furent parmi les premiers à le mettre en œuvre côté serveur (Fowler, 2011). Puis une conférence intitulée « *Workshop on Web Tracking and User Privacy* » fut organisée à l'Université de Princeton les 28 et 29 avril 2011, et le groupe de travail *Tracking Protection Working Group* débuta officiellement ses activités par une téléconférence inaugurale le 14 septembre 2011[72]. La Charte de ce groupe énonce l'objectif suivant :

---

70 Traduit de l'anglais. Texte original : « Basically it was political. There wasn't any, like, formal regulatory or law enforcement action that they took. But the FTC sort of published reports on areas of interest. And they specifically highlighted Do Not Track as a center of recommendation. It was a 2010 report I think. And I think that makes a fairly significant difference for the industry in the US. This does not guarantee anything, but when FTC really says: we should do this… it's enough to take people on board or consider something. And the FTC also sent participants, like was actively involved in the conversations. So that's … I think that's something of an uncommon practice for FTC. But they sent participants who were very actively involved in the discussions of the Tracking Protection Working Group. And commissioners… I dunno how well you know the FTC structure. But there is up to five commissioners. Commissioners would make speeches about it. A commissioner attended one of those standard setting meetings. So I think it was sort of sending a strong signal that this is a priority. »

71 Traduit de l'anglais. Texte original : « It was after the IETF said this is not for them, because it's not a protocol issue, it's more a social issue. And I had no preference for which standard organization took it on, as long as you could get all the stakeholders together to agree on how to communicate the preference. »

72 Voir le compte-rendu de cette réunion disponible sur : https://www.w3.org/2011/09/14-dnt-minutes.html (page consultée le 30 mai 2018).

> « Le groupe de travail produira des spécifications incluses dans le processus de recommandation [*Recommendation-track specifications*] pour un mécanisme simple d'expression de préférence lisible par une machine (« Do Not Track ») et des technologies pour permettre ou bloquer des éléments de pistage de manière sélective[73]. » (W3C TPWG Charter)

Malgré l'enthousiasme initial qu'illustrent la relative rapidité de l'enchaînement d'événements début 2011, et le soutien apporté non seulement par deux fabricants de navigateurs (Microsoft et Mozilla) mais aussi par la FTC à cette initiative, le projet s'enlisa rapidement, notamment autour d'une controverse longue sur la question de la définition du terme « *tracking* ». Roy Fielding et ses collègues travaillant pour la société Adobe s'opposaient formellement à toute avancée tant qu'une décision consensuelle sur ce terme n'était pas adoptée formellement par le TPWG. Cette querelle ne fut résolue qu'en 2013.

En 2012, Microsoft annonça de façon unilatérale que désormais, le signal DNT:1 serait activé par défaut sur son navigateur Internet Explorer (Lynch, 2012). Cette décision provoqua l'ire des représentants de l'industrie de la publicité en ligne, qui refusa de respecter un signal aussi généralisé, qui lui interdirait pratiquement toute publicité comportementale en ligne, au motif que cela brouillait le signal. Pour ces derniers, en effet, le signal DNT:1 devait émaner d'une préférence de l'utilisateur, et donc d'une logique d'*opt-out*, et non d'une configuration standard décidée par le fabricant du navigateur web (Angwin, 2012).

Le projet a reçu entre temps un deuxième soutien politique, en plus de celui de la FTC : celui de la Commission européenne. Dans son analyse d'impact annexée à la proposition pour un règlement e-Privacy[74] de 2017, il est écrit que :

> « Le fait de centraliser le consentement dans des logiciels comme les navigateurs Internet, d'inviter les utilisateurs à choisir leurs paramètres de confidentialité et d'étendre les exceptions à la règle du consentement pour les cookies donnerait à une grande partie des entreprises la possibilité de se débarrasser des bandeaux et avis en la matière et conduirait donc à des économies de coûts et une simplification potentiellement importantes. » (Commission européenne, 2017, p. 9)

73 Traduit de l'anglais. Texte original : « The Working Group will produce Recommendation-track specifications for a simple machine-readable preference expression mechanism ("Do Not Track") and technologies for selectively allowing or blocking tracking elements. »

74 Projet de Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques») (COM(2017) 10 FINAL, 2017/0003(COD)).

Plus loin, dans le considérant 22 du projet de règlement :

> « Le présent règlement devrait prévoir la possibilité d'exprimer un consentement en utilisant les paramètres appropriés d'un navigateur ou d'une autre application. Les choix effectués par l'utilisateur final lorsqu'il définit les paramètres généraux de confidentialité d'un navigateur ou d'une autre application devraient être contraignants pour les tiers et leur être opposables. »

Et l'article 9 du projet de règlement précise encore :

> « […] si cela est techniquement possible et réalisable […] le consentement peut être exprimé à l'aide des paramètres techniques appropriés d'une application logicielle permettant d'accéder à Internet. »

Ceci, combiné à l'entrée imminente en application du RGPD, explique la décision prise en avril 2018 par Tim Berners-Lee d'étendre la charte du TPWG jusqu'au 30 septembre pour prendre en compte l'impact de la réglementation européenne sur le projet *Do Not Track* (*public-tracking*, e-mail de Xueyuan du 10 avril 2018). Mais en août 2018, soit plus de sept ans après la création du groupe, les documents produits par le TPWG n'en étaient qu'au stade de *Candidate Recommandations*. La charte ne fut plus prolongée et, le 17 janvier 2019, le TPWG fut officiellement fermé (*public-tracking*, e-mail de Xueyuan du 17 janvier 2019).

Le Tracking Protection Working Group (TPWG) du W3C travaillait à la production de deux recommandations formant ensemble le standard Do Not Track (DNT) :

- Le document *Tracking Preference Expression* (TPE) qui permet d'indiquer comment le navigateur communique le choix de l'internaute, et la façon dont le serveur peut répondre ou solliciter une demande d'exception (W3C TPE) ;
- Le document *Tracking Compliance and Scope* (TCS) qui détermine la façon dont un serveur qui reçoit un signal formulé de façon conforme au document TPE doit se comporter pour agir de façon conforme aux spécifications du standard Do Not Track (W3C TCS).

Ces documents sont désormais considérés comme de simples « notes », rétrogradées de leur statut de « *Candidate Recommendation* ». Comme indiqué dans cet extrait du second document :

> « Depuis sa dernière publication en tant que Recommandation Candidate en avril 2016, il n'y a pas eu suffisamment d'adoption […] pour justifier une poursuite des travaux, ni d'indications répandues ou de support prévu par des *first parties*[75], *third parties* et fournisseurs de service. Le *Tracking Protection Working Group* a décidé de conclure ses travaux et de republier ce […] document comme une note, tout futur ajout devant être publié séparément[76]. » (W3C TCS, version du 22 janvier 2019)

Le projet DNT, a l'heure de rédiger ces lignes, semble donc avoir échoué de la même façon que le projet P3P. Pendant l'essentiel de notre enquête sur le PING et, de fait, le TPWG, conduite entre 2016 et fin 2018, son sort n'était toutefois pas encore scellé. Cela explique que les documents et extraits d'entretien cités présentent le DNT comme un projet en cours, et non un échec.

Maintenant que nous avons présenté le PING, le TPWG auquel notre enquête a été élargie, et l'historique des discussions au W3C sur la « vie privée » qui ont précédé leur création, et avant de nous attaquer à l'analyse de notre corpus de documents et d'entretiens pour étudier les discours et les controverses sur la « vie privée » dans ces arènes, nous devons encore nous attarder sur l'étude des dispositifs de communication qui en constituent la matérialité et ont fortement conditionné la production du corpus.

5.4.6. Présentation des outils de communication utilisés par le PING et le TPWG

Les groupes du W3C utilisent des outils pour permettre à leurs membres, qui vivent à de grandes distances d'écart répartis sur plusieurs continents, de communiquer. Ces outils fondent la matérialité technique des arènes dans lesquelles se sont déployées les controverses sur la « vie privée » que nous allons analyser dans ce chapitre. Ils ont eu des effets sur la production des documents du corpus sur lequel nous avons fondé notre enquête de terrain. Il est donc utile de revenir avant d'entamer la présentation de l'analyse de son contenu.

Nous allons présenter ici dans le détail les moyens de communication utilisés par le PING, le TPWG utilisant exactement les mêmes outils.

75 NDT : Ces termes techniques ne sont généralement pas traduits en français.

76 Traduction de l'auteur. Texte original : « Since its last publication as a Candidate Recommendation in April 2016, there has not been sufficient adoption […] to justify further advancement, nor have there been widespread indications of planned support among first parties, third parties and service providers. The Tracking Protection Working Group has decided to conclude its work and republish the Compliance document as this Note, with any future addendums to be published separately. »

Les participants du PING – mais cela est vrai aussi pour le TPWG – se réunissent rarement *de visu*. La seule exception est la réunion « *Face to Face* » (F2F) annuelle lors du *Technical Plenary and Advisory Committee* (TPAC), la grande réunion annuelle du W3C. Le groupe ne dispose pas de locaux. Leurs échanges, comme ceux, d'ailleurs, des autres groupes, ont essentiellement lieu par courrier électronique et par téléconférences.

Le groupe dispose d'une liste de discussion publique : *public-privacy*, dont les archives sont accessibles en ligne :

Figure 35 : *Extrait de capture d'écran de la page d'accueil des archives publiques de la liste de discussion* public-privacy *sur le site du W3C, à l'adresse web : https://lists.w3.org/Archives/Public/public-privacy/ (page consultée le 18 juillet 2018)*

Quant aux téléconférences, celles-ci ont lieu avec le logiciel WebEx, développé par le MIT. A chaque réunion, y compris lors de la réunion F2F du TPAC, quelqu'un se désigne pour être le « scribe » de la réunion pendant la discussion sur IRC. Lorsque le « scribe » prend la parole, il doit attendre qu'un autre volontaire se désigne pour prendre le relais. Cela permet de toujours garder une trace écrite des discussions qui ont lieu à l'oral pendant les réunions.

La discussion sur IRC sert également à organiser les tours de parole, gérés par un robot dénommé « Zakim » avec lequel il est possible d'interagir (avec les commandes « q+ » pour s'inscrire sur le tour de parole, « q- » pour s'en désinscrire et « q ? » pour demander qui est inscrit). « ack » permet d'accorder la parole. L'utilisation des commandes est illustrée dans la

capture d’écran ci-dessous, réalisée pendant la réunion F2F de PING pendant un TPAC, le 26 octobre 2018, à Lyon :

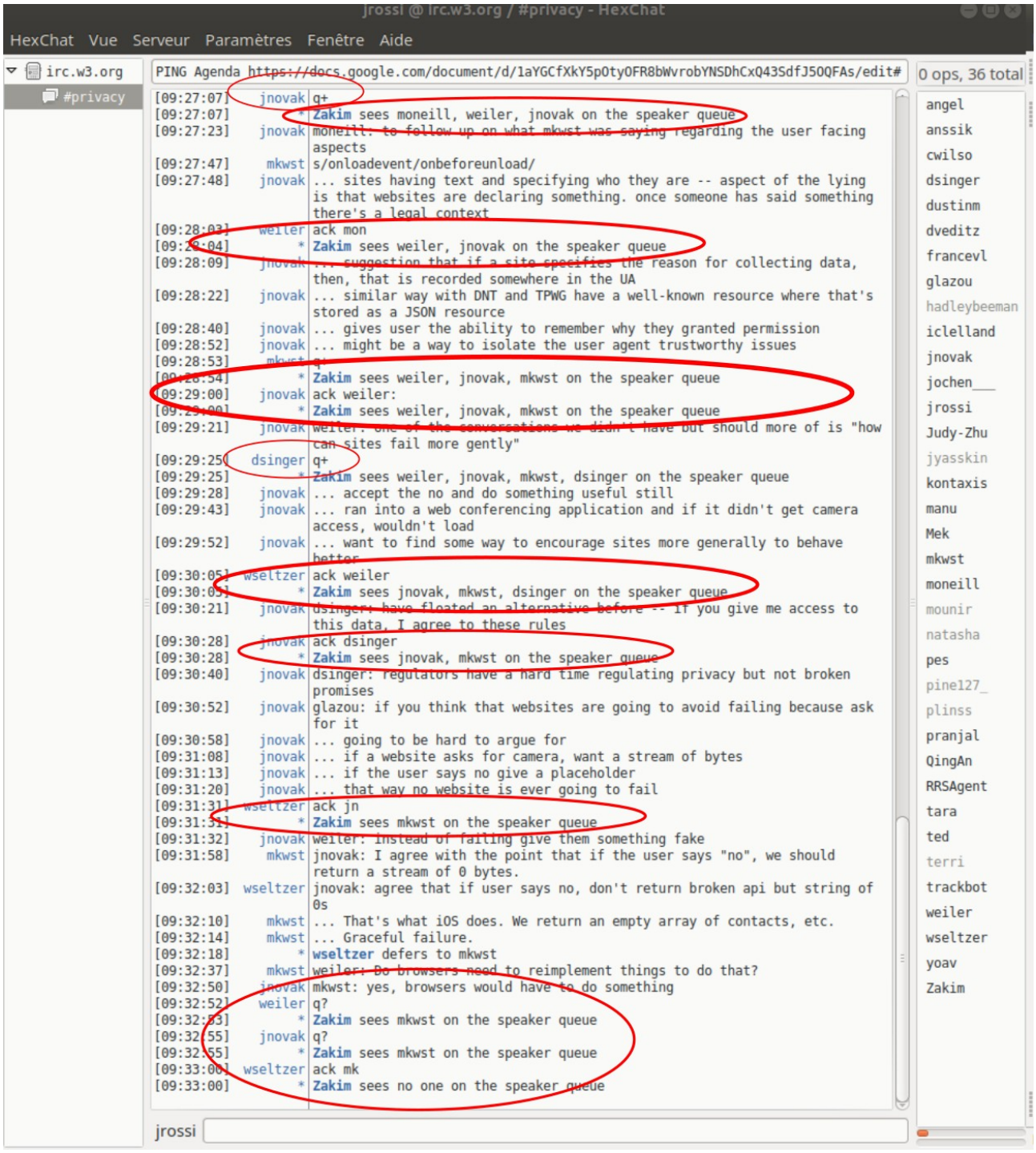
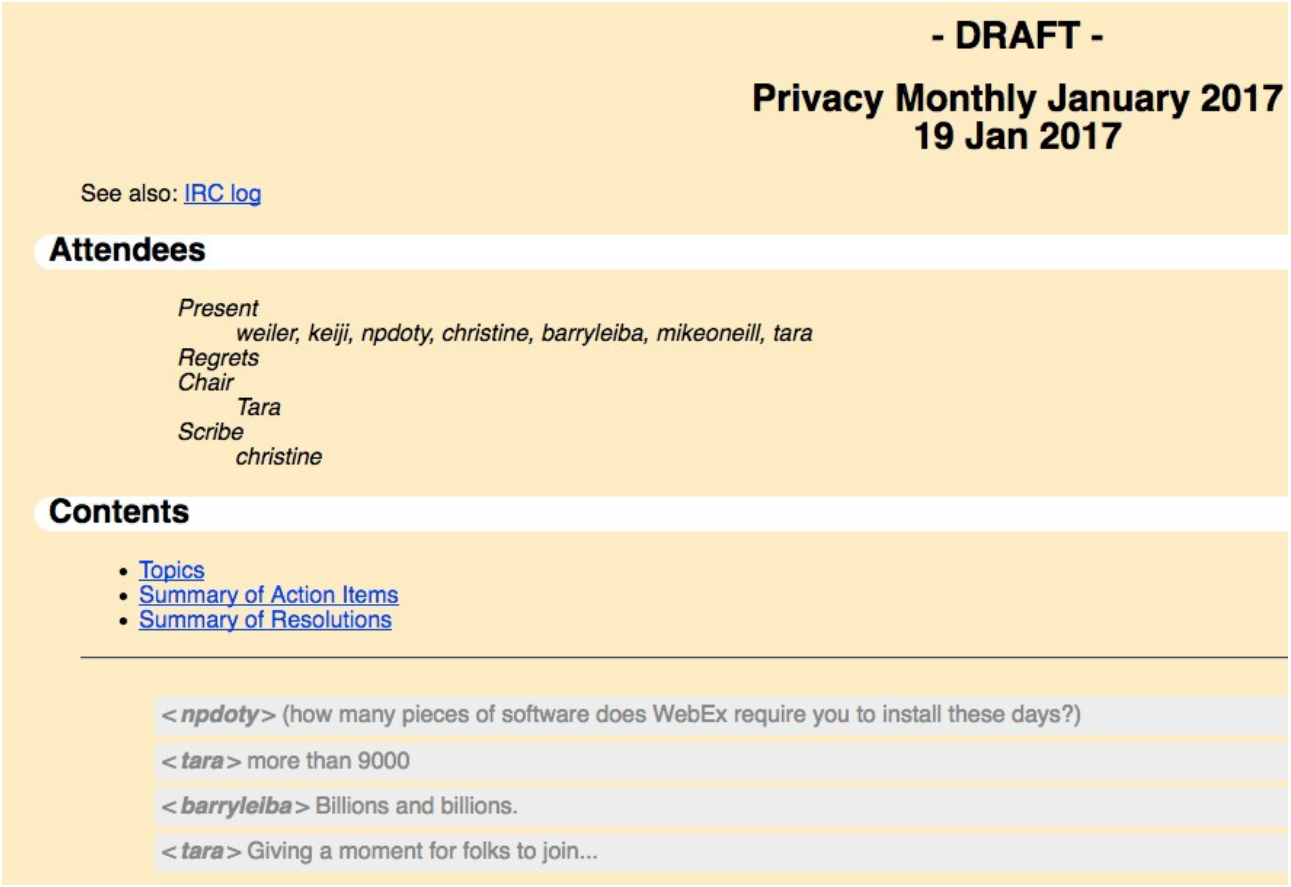


Figure 36 : *Capture d’écran d’une discussion sur le canal IRC #privacy du W3C pendant la réunion F2F du PING le 26 octobre 2018 lors du TPAC de Lyon, les interactions avec le robot Zakim étant entourées en rouge*

Ces prises de notes peuvent être complétées par des interactions écrites via cet outil de messagerie instantanée, soit via des messages privés entre membres, soit directement sur le fil de discussion, où se superposent alors deux conversations : la conversation orale prise en note par le « scribe » et la conversation écrite, auxquelles se superposent les interventions de Zakim.

Ces conversations IRC sont archivées pour servir d'archives au groupe, à partir desquelles des comptes-rendus sont générés de façon automatique, comme dans la capture d'écran ci-dessous :



- DRAFT -

Privacy Monthly January 2017
19 Jan 2017

See also: IRC log

Attendees

Present
weiler, keiji, npdoty, christine, barryleiba, mikeoneill, tara
Regrets
Chair
Tara
Scribe
christine

Contents

- Topics
- Summary of Action Items
- Summary of Resolutions

<*npdoty*> (how many pieces of software does WebEx require you to install these days?)
<*tara*> more than 9000
<*barryleiba*> Billions and billions.
<*tara*> Giving a moment for folks to join...

Figure 37 : *Capture d'écran du début du compte-rendu détaillé de la réunion du 19 janvier 2017, disponible à l'adresse web : https://www.w3.org/2017/01/19-privacy-minutes.html (page consultée le 18 juillet 2018)*

Ces comptes-rendus IRC sont parfois complétés par des comptes-rendus rédigés par les coprésidentes (*co-chairs*) du groupe, mais cela n'est pas systématique.

Les journaux des discussions IRC sont difficiles à exploiter. Comme nous avons pu le voir en allant à la réunion F2F de PING au TPAC le 26 octobre 2018, les contraintes de la lenteur de l'écriture sur clavier, le fait que les scribes ne sont pas formés à la prise de note, et la rapidité des échanges font que la retranscription est souvent lacunaire. Des déformations ont également lieu, puisque ce n'est pas la personne qui parle qui écrit ce qu'elle dit dans la discussion sur IRC. Par exemple, dans l'extrait de discussion figure 36, nous voyons sur la troisième ligne l'utilisateur « jnovak » (Jason Novak, d'Apple) qui prend en note ce que dit l'utilisateur « moneill » (Mike O'Neill, de Baycloud). Plus loin, à 9h 30 minutes et 40 secondes, il indique qu'il prend désormais en note ce que dit « dsinger » (David Singer, d'Apple). Puis, lorsqu'il prend la parole à son tour à 9h 31 minutes et 58 secondes, c'est « mkwst » (Mike West, de Google) qui prend en note ce qu'il dit.

Dans de telles conditions d'écriture, ces journaux ne sont donc pas véritablement exploitables comme corpus pour une vraie exploitation qualitative à moins d'avoir assisté effectivement à la réunion et de se servir des comptes-rendus comme aide-mémoire.

À noter qu'il arrive de surcroît, au cours de la réunion, qu'un participant demande à ce ce qu'il doit soit « *off the record* », donc non-retranscrit. Or, ces moments particulièrement pertinents pour l'analyse sont perdus à la lecture des journaux IRC et des compte-rendus de réunion.

C'est pour toutes ces raisons que nous avons privilégié, pour notre enquête sur le W3C PING, l'enquête par entretien, l'exploitation d'un corpus d'e-mails qu'une recherche par mots-clefs à l'aide de scripts Python nous a aidé à sélectionner, et la journée d'observation participante au TPAC de 2018. Cela est valable aussi pour le TPWG, qui dispose des mêmes outils de communication, avec les mêmes contraintes.

5.5. La contrainte discursive du consensus dans la controverse sur le « *tracking* » et la « *privacy* »

5.5.1. Présentation de la controverse sur la définition du mot « *tracking* »

Notre premier réflexe au moment d'entamer l'étude de terrain sur le W3C PING, puis le TPWG, a été de repérer une ou des controverses autour de la notion de « *privacy* », pour pouvoir étudier les conceptions sur celle-ci qu'auraient défendues les uns et les autres, et observer les conséquences de ces controverses sur le contenu des documents rédigés. Or, et nous y reviendrons[77], nous n'avons pas trouvé la trace d'une telle controverse. Au mieux, nous avons

77 Cf. section 5.5.3.

repéré quelques (rares et courtes) discussions philosophiques sur *public-privacy* sur ce qu'est la « vie privée », mais sans que cela ne provoque la moindre controverse, ou soit connecté directement à un enjeu de rédaction d'un document à valeur normative. En entretien, les enquêtés ont accepté de répondre à notre question sur ce que, pour eux, le droit *à la* vie privée désignait, mais ils ont souligné qu'ils jugeaient inutile et contre-productif d'en discuter entre eux sur *public-privacy*.

Tous les enquêtés, y compris ceux qui ont répondu sous le sceau de l'anonymat, et y compris celui qui a refusé que l'entretien soit enregistré, ont affirmé qu'il y avait un consensus sur la question : la notion de vie privée est essentiellement contestée, et il est inutile de la définir pour analyser de façon productive des caractéristiques techniques de projets de recommandations du W3C. Par contre, selon Vincent Toubiana[78] :

> « Le gros débat c'était qu'est-ce qu'on entend pas tracking en fait. C'est ça le gros débat. » (Entretien avec Vincent Toubiana)

Cet extrait d'entretien, et d'autres allant dans le même sens, nous ont ainsi quand même mis sur la piste d'une vraie controverse, s'étalant sur plusieurs années, et qui s'est déroulée sur *public-tracking*, la liste de discussion du TPWG. Cette controverse ne portait pas directement sur la « vie privée », mais sur la notion de « *tracking* » (« pistage » ou « traçage » en français). Comme le « *tracking* » était l'infraction au droit à la « *privacy* » que le projet *Do Not Track* devait aider à protéger, cela nous a quand même permis d'observer indirectement ce qui, implicitement, était aussi une controverse sur la définition et la valeur de la « vie privée ».

La controverse sur la « *tracking* » soulevait des enjeux rédactionnels directs sur les documents produits par le groupe de travail.

Le standard Do Not Track est décrit dans deux documents : le document *Tracking Preference Expression* (TPE), et *Tracking Compliance and Scope* (TCS). Le premier décrit la façon dont le *user agent* transmet au serveur web le signal que l'internaute ne souhaite pas être tracé, le signal que le serveur doit renvoyer au *user agent* lorsqu'il reçoit ce signal, et la façon dont il doit être possible de stocker sur le terminal de l'internaute des exceptions spécifiques à un nom de domaine en particulier. Le second décrit ce qu'un serveur web, pour être conforme au standard DNT, doit faire lorsqu'il reçoit d'un *user agent* le signal DNT:1.

Les éditeurs de TPE sont David Singer, d'Apple, et Roy Fielding, d'Adobe. Les éditeurs successifs de TCS ont été Erica Newland, de CDT, puis Sean Harvey, de Google, Justin

78 Au moment de l'entretien, Vincent Toubiana, expert invité du TPWG et contributeur à la liste de discussion du PING travaillait à la CNIL. Avant cela, il avait fait de la recherche en informatique, en collaboration avec Helen Nissembaum, sur la protection contre le traçage des comportements en ligne.

Brookman, de CDT, Heather West, de Google (et aujourd'hui Mozilla), et enfin Nick Doty, un universitaire états-unien invité à prendre part aux travaux du TPWG en qualité d'expert invité.

La question (« *issue* ») de la définition de la notion de « *tracking* » a été soulevée par Roy Fielding dès 2011. Il en a fait un préalable à toute avancée possible sur le document TPE. Voici le contenu de son e-mail, le deuxième dans le fil de discussion dédié à la question sur le tracker du TPWG après le message automatique annonçant la création du fil, envoyé le 12 octobre 2011 :

> « S'il vous plaît, concentrons-nous d'abord sur ce problème. J'ai ajouté une description :
>
> Le mot "tracking" est au cœur de toutes les définitions et de tous les mécanismes définis par ce groupe de travail.
>
> Certaines personnes pensent que le "tracking" revient à suivre toutes les actions de l'utilisateur, ce qui impliquerait un enregistrement des données du flux de clics par une first-party.
>
> D'autres pensent que le "tracking" revient à suivre un utilisateur d'un site à un autre, d'une marque différente, ce qui exclurait un enregistrement par une first-party de données non partagées avec des tiers.
>
> Quelle est la bonne définition ?
>
> Chaque fois que je regarde les compte-rendus de réunions ou l'IRC, je vois que tout le monde se contredit et cela complique considérablement la compréhension des opinions de chacun.
>
> ....Roy[79] » (*public-tracking*, e-mail de Roy Fielding du 12 octobre 2011)

Pour bien analyser et comprendre cette controverse, notamment la façon dont elle a pour partie été une controverse par procuration sur le contenu et la valeur du droit *à la* « vie privée », il est important de comprendre les contraintes communicationnelles spécifiques que l'obligation ultime d'arriver à un consensus pour qu'un document se transforme en standard effectif produit sur les acteurs, et qui expliquent la volonté de certains de ne surtout pas essayer de se mettre d'accord sur une définition de la « vie privée ».

79 Traduit de l'anglais. Texte original : « Please address this issue first. I have added a description:
The word "tracking" is central to all of the definitions and mechanisms being defined by this working group.
Some people think "tracking" means following all of the user's actions, which would include first-party click-stream data collection.
Other people think that "tracking" means following a user from one site to another (differently branded) site, which would exclude first-party data collection that isn't shared with third-parties. Which is it?
Every time I look back at the IRC or meeting minutes, I see half the people assuming one or the other, and it is making it very hard to understand each other's opinions.
....Roy »

En effet cette caractéristique fondamentale de recherche de consensus qui pèse sur les acteurs du W3C complique la tâche de quiconque souhaiterait y cartographier des coalitions rivales, puisque les dissensus deviennent souvent implicites dans leur expression. Appliquer notre méthodologie générale inspirée des approches cognitives des politiques publiques et de l'ACF sans l'adapter n'était pas approprié. Un détour par l'analyse de cette caractéristique s'imposait avant de poursuivre l'analyse du corpus de discours collectés.

5.5.2. Un agir communicationnel qui s'impose

L'absence de trace de dissensus – qui n'est pas la même chose que l'absence de dissensus – s'explique en partie par la transparence des échanges sur *public-privacy* et *public-tracking*. Comme le rappellent Deirdre Mulligan et Nick Doty dans leurs travaux sur le W3C :

> « Les procédures fondées sur le consensus peuvent réduire la transparence en raison du désir d'éviter d'enregistrer des votes, ceux-ci étant perçus comme polarisants. […] La volonté de conserver une trace de dissensus dans un processus ostensiblement orienté vers le consensus fait ressortir le conflit entre d'une part une procédure fondée sur le consensus, mettant l'accent sur l'accord et la collégialité, et d'autre part le niveau de clarté et de transparence des positions, et les contours effectifs de ce consensus tels que délimités par les votes publics[80]. » (Doty et Mulligan, 2013, p. 172)

Mais ce n'est pas la seule raison.

Deirdre Mulligan et Nick Doty nous rappellent aussi un élément essentiel à prendre en compte pour être capable de détecter des controverses politiques qui, au W3C, sont souvent très feutrées ou prennent l'allure de « simples » discussions « techniques ». Cet élément, c'est que le caractère non-coercitif des standards du web est perçu par les acteurs du W3C comme une contrainte au consensus :

> « Puisque le W3C ne peut imposer l'adoption, il y a une grande préférence pour le consensus, qui est considéré comme permettant d'augmenter les chances d'une adoption large. (Au W3C, l'on parle de consensus lorsqu'il n'existe pas d'objection formelle)[81] »

80 Traduit de l'anglais. Texte original : « Consensus processes can reduce transparency due to the desire to avoid recorded votes, which are viewed as polarizing. […] The desire to have a record of dissent in an ostensibly consensus process points to the tension between consensus processes that emphasize agreement and collegiality, and the level of clarity and transparency about positions and the actual contours of that consensus recorded by public votes. »

81 Traduit de l'anglais. Texte original : « Given that W3C cannot compel adoption there is a strong preference for consensus as it is thought to increase the odds of widespread adoption. (Consensus is defined at W3C as lacking formal objection) ».

(Doty et Mulligan, 2013, p. 171)

Produire et maintenir un consensus dans un groupe de travail est tellement important par le W3C qu'il existe un document collectif intitulé l'*Art du consensus*[82] avec de très nombreuses ressources, se voulant un guide à destination de ses membres (W3C, non daté (c)).

Lorsque les documents produits au W3C contiennent des éléments qu'un ou plusieurs participants considère comme n'étant pas consensuel, il ne peut pas faire appel à un vote. Ainsi, lorsque Alan Chapell, un consultant en droit de l'industrie publicitaire qui n'a participé qu'au TPWG et n'était pas familier des us et coutumes des organismes de standardisation d'Internet, a demandé la tenue d'un vote pour clore le débat sur le « *tracking* », il lui a tout de suite été répondu que cela n'est pas la façon dont le W3C fonctionne :

> « Pourquoi le document intitulé "What Base Text to Use for the Do Not Track Compliance Specification" ("Decision Document") (NDT :*« Quel texte de base doit être utilisé pour la spécification de conformité Do Not Track ?, « Document de décision »*) était-il défini comme relevant d'une décision de groupe plutôt que d'une décision de la présidence ? Le Document de décision utilise de manière répétée le terme de « décision de groupe ». Toutefois, une décision de groupe tendrait à impliquer que les votes des membres du groupe de travail concordent, alors que je ne trouve nulle part de récapitulatif des votes[83]. » (*public-tracking*, e-mail d'Alan Chapell du 18 juillet 2013)

> « Ce document est à juste titre caractérisé comme une décision de groupe : au vu de la discussion et des objections reçues, les présidents [*chairs*] ont identifié la démarche suscitant les objections les plus faibles [*weakest objections*] et l'ont enregistré [*recorded*] comme décision de groupe (comme leur tâche l'exige).
>
> Pour mémoire, dans le document de procédure du W3C : « Les groupes devraient privilégier les propositions suscitant les objections les plus faibles. Ces propositions sont préférées à celles soutenues par une large majorité mais qui suscitent des objections fortes de la part d'un petit nombre de personnes[84]. » (*public-tracking*, e-mail de Thomas Roessler

82 Traduction de l'auteur. Texte original : « The Art of Consensus ».

83 Traduit de l'anglais. Texte original : « Why was the document entitled "What Base Text to Use for the Do Not Track Compliance Specification" ("Decision Document") characterized as a group decision rather than a chair's decision ? The Decision Document repeatedly uses the term "group decision." However, a group decision would seem to suggest that WG members votes were tallied, but I don't see votes tabulated anywhere. »

84 Traduit de l'anglais. Texte original : « The document is correctly characterized as a group decision: Based on the discussion and the objections received, the chairs identified the path forward that drew the weakest objections, and recorded it as a group decision (as is their task).
Of note, in the W3C process document : "Groups should favor proposals that create the weakest objections. This is prereferred over proposals that are supported by a large majority but that cause strong objections from a few people". »

du 18 juillet 2013

Le vote n'est pas la procédure habituelle de règlement des dissensus. Illustrant la citation en début de section de Nick Doty et Deirdre Mulligan, Matthias Schunter, président (*chair*) du TPWG, a fait appel à une procédure d'appel à objections, en 2013, pour clore le débat autour de la définition de la notion de « *tracking*[85] ». Dans cette procédure, plusieurs options sont proposées, et les membres sont invités à dire pourquoi ils s'opposent à telle ou option. L'option qui recueille le moins d'objections est alors adoptée. Ce n'est donc pas un vote, mais néanmoins, comme le vote formel, une façon de parvenir à délégitimer à l'avenir toute future expression de désaccord sur le point ayant été soumis à cette procédure formelle. Cette technique permet un retour au consensus, objectif primordial de tout *chair* souhaitant mener à bien le projet de standardisation de son groupe de travail.

Notons que l'impératif de consensus facilite des comportements stratégiques de flibuste, qui visent à faire s'éterniser les discussions en créant du dissensus pour ralentir et à terme empêcher l'adoption d'un standard :

> « Même si le pouvoir de prise de décision qu'un processus fondé sur le consensus accorde aux parties-prenantes peut contribuer à une meilleure perception de la légitimité matérielle [*substantive legitimacy*], il offre aussi des opportunités de comportement stratégique susceptibles de nuire au succès du résultat [*undermine successful outcomes*][86]. » (Doty et Mulligan, 2013, p. 172)

Selon les enquêtés interrogés, le débat lancé par des employés d'Adobe au sein du TPWG pour adopter une définition du terme « tracking » serait une parfaite illustration de ce type de comportement.

Or, un tel agir stratégique est stigmatisé par les participants du W3C, à tel point qu'il arrive que certains participants sacrifient une part de leurs objectifs pour ne pas sacrifier le consensus, quitte à produire une recommandation qui leur semble de moins bonne qualité. Aleecia McDonald, dans une contribution au débat sur la définition du terme « *tracking* », revenait sur cette tension. Elle y expliquait que pour aller vite et être efficace dans la production d'un document consensuel, il était possible d'adopter un standard DNT qui n'interdise que les transferts de données personnelles du site visité par un internaute vers des « *third parties* » comme des serveurs publicitaires. Mais pour elle, une telle solution de facilité irait à l'encontre

85 Cf. section 5.5.4.

86 Traduit de l'anglais. Texte original : « While the decision-making power consensus processes afford stakeholders may contribute to greater perception of substantive legitimacy it provides opportunities for strategic behavior that can undermine successful outcomes. »

de ce qu'elle pense que le DNT doit être, puisque pour elle un internaute exprimant la volonté de ne pas être pisté l'exprime aussi à l'égard du site web qu'il visite :

> « Pour en revenir à nos critères de réussite initiaux établis à Boston, d'un côté, il y avait la facilité d'implémentation. Clairement, si nous limitons le DNT au transfert de données entre sites, le coût d'implémentation est substantiellement abaissé. C'est vraiment important. Nous avions également un autre critère selon lequel le DNT devait fonctionner pour les utilisateurs. C'est un argument pour que le DNT concerne davantage de processus que les simples transferts de site à site.[87] » (*public-tracking*, e-mail d'Aleecia McDonald du 12 octobre 2011)

En raison de cette tension, les participants peuvent facilement être prêts à abandonner des revendications qu'ils jugent secondaires, et même à le signaler d'emblée, comme Justin Brookman donnant son avis sur la proposition de changer le nom du standard « *Do Not Track* » :

> « Je suis ouvert aux propositions concrètes sur un autre nom à donner au signal (« Respectez ma vie privée » : REFUSÉ!), mais étant donné que ce navigateur est chargé de l'expérience utilisateur [*UX*] et qu'il a la responsabilité d'informer l'utilisateur de ce que va permettre la configuration, je questionne l'utilité. Si vous souhaitez renommer l'en-tête « Ne-Pas-Pister-À-Travers-Des-Domaines-Ne-Partageant-Pas-La-Même-Marque-Sauf-Pour-Quelques-Relations-Etroitement-Définies-Pour-la-Prévention-De-La-Fraude-Et-Des-Fournisseurs-De-Services-En-Silos », nous pouvons toujours essayer, mais au final, cela n'aura pas d'importance[88]. » (*public-tracking*, e-mail de Justin Brookman du 13 octobre 2011)

Un autre exemple est qu'il arrive que lors d'appels formels à objection, certaines personnes préfèrent s'abstenir de formuler des objections sur un point qui ne leur paraît pas essentiel, pour éviter de faire dérailler le consensus[89].

---

87 Traduit de l'anglais. Texte original : « To come back to our initial success criteria in Boston, on the one hand we had ease of implementation. Clearly, if we limited DNT to just being about data transfer between sites, this is substantially lower cost to implement. That is really important. We also had another criteria that DNT has to work for users. That argues for DNT covering more than just site-to-site transfers. »

88 Traduit de l'anglais. Texte original : « I am open to concrete suggestions about what else we would want to call the signal ("Respect My Privacy": REJECTED!) but given that that browser's in charge of the UX and has the responsibility to tell the end user what the setting will do, I question the utility. It you want to rebrand the header as "Do-Not-Track-Across-Non-Commonly-Branded-Domains-Except-For-Narrowly-Defined-Excepted-Fraud-Prevention-And-Siloed-Service-Provider-Relationships," we can give it a shot, but it's not going to matter at the end of the day. »

89 Cf. section 5.5.4.

Au-delà de la controverse sur le « *tracking* », plusieurs autres affaires, au sein du TPWG mais aussi plus largement au W3C, ont illustré le coût du dissensus pour l'implémentation d'un standard.

En 2012, Microsoft voulut forcer la main aux publicitaires participant au TPWG en utilisant sa position de producteur de navigateur web. L'entreprise décida alors que, par défaut, le signal DNT serait activé, avec une valeur égale à 1 (Whitney, 2012). Pour que DNT soit égal à 0, dans Internet Explorer, il fallait alors que l'internaute fasse un choix délibéré. Or, cette décision, qui n'était pas consensuelle, eut pour effet de ralentir l'adoption du standard DNT par les publicitaires, rendant le signal inopérant puisqu'il n'était pas respecté par les sites visités :

> « Microsoft a essayé à un moment de forcer un peu en mettant Do Not Track par défaut, ce qui a eu un effet contre-productif […] » (Entretien avec Vincent Toubiana)

> « Alors notre intention était que le signal Do Not Track soit un indicateur, qui dise : ‘ne me pistez pas’. Microsoft l'a considéré comme un interrupteur on/off du pistage. Ce qu'il n'était pas. Et le secteur publicitaire a considéré que c'était un élément juridique auquel on pouvait se raccrocher pour engager des poursuites en cas de pistage. Microsoft a ensuite dit : « Voilà ce que nous allons faire. Nous allons tous investir à fond dans Do Not Track et l'activer par défaut ». […] Nous avons donc tourné en rond un certain temps avec Microsoft avant qu'ils ne se rendent compte que : ah, okay, oups, on l’a activé par défaut alors il n’a pas de valeur[90]. » (Entretien avec Sid Stamm)

> « Dans un certain sens, peut-être que c'est une des raisons pour lesquelles le Do Not Track n'a pas progressé aussi vite qu'il aurait peut-être pu. Parce qu'il n'existait pas de stratégie cohérente parmi les développeurs de navigateurs, qui ne l’implémentaient pas de façon uniforme au même moment[91]. » (Entretien avec Simon Rice)

Au-delà du TPWG, l'affaire du WHATWG, étudiée par Guillaume Sire (Sire, 2017), où une série de membres du W3C créèrent une arène alternative pour la standardisation du W3C

90 Traduit de l’anglais. Texte original : « So we intended the Do Not Track signal to be an indicator, to say: hey please don't track me. Microsoft took it as an on/off switch for tracking. Which it wasn't. And the ad indusry took it as a legal hook to sue them if they track. And what happened was that Microsoft said: well, here is what we're gonna do. We're gonna go all in, we're going to invest fully in Do Not Track and we're going to turn it on by default. […] So we went back and forth with Microsoft for a long time before they figured out: oh, okay, well, oops, we turned it on by default, so now it's not valuable. »

91 Traduit de l’anglais. Texte original : « And in some ways maybe that's a reason why Do Not Track has not progressed as fast as perhaps it could have. Because there was no coherent strategy amongst the browser developers that did not implement it in the same way at the same time. »

suite à un désaccord de fond avec Tim Berners-Lee et d'autres membres du W3C, montre aussi la fragilité d'une organisation qui repose sur la recherche permanente de consensus pour encourager l'implémentation uniforme de ses standards. Cela est vrai pour le W3C, mais aussi le WHATWG ou encore l'IETF. Sans uniformité dans l'implémentation, c'est en effet l'interopérabilité et l'unité du Web et d'Internet qui est remise en cause, différents appareils et logiciels ne pouvant alors plus communiquer entre eux.

Face à cet impératif toujours présent à l'esprit des participants, ceux qui ne jouent pas le jeu sont rappelés à l'ordre.

Par exemple, en 2011, Jonathan Mayer, dans le fil de discussion sur la définition du terme « *tracking* », dans le TPWG, s'opposa aux positions de l'*Interactive Advertising Board* (IAB) de façon directe et explicite à deux reprises le même jour :

> « Je suis particulièrement surpris d'entendre ces arguments hypocrites venir de la part de l'IAB et d'autres acteurs de l'espace de l'autorégulation, étant donné que les systèmes d'opt-out que vous proposez actuellement sont bien plus trompeur, et de beaucoup, qu'un standard Do Not Track transparent ne le sera jamais[92]. » (*public-tracking*, permier e-mail de Jonathan Mayer du 13 octobre 2011)

> « Si l'IAB pense que nous devons enfreindre les attentes des consommateurs en matière de vie privée, alors il faut le dire[93]. » (*public-tracking*, second e-mail de Jonathan Mayer du 13 octobre 2011)

Le jour même, il s'est fait rappeler à l'ordre en des termes très vifs par quelqu'un qui partageait pourtant ses positions dans la controverse :

> « Les attaques personnelles ne sont pas les bienvenues dans ce groupe. Comme nous l'avons dit lors de la réunion de lancement à Boston, c'est le meilleur moyen d'obtenir que les présidents [*chairs*] ne vous donnent pas la parole, comme première sanction. […] Je n'ai ni le temps, ni la patience, de jouer à l'institutrice de maternelle. Il y a un niveau basique de professionnalisme et de respect mutuel qui sont nécessaires à la réussite de ce

92 Traduit de l'anglais. Texte original : « I'm particularly surprised to hear these hypocritical arguments coming from IAB and others in the self-regulatory space, since the opt outs y'all currently offer are orders of magnitude more misleading than a transparent Do Not Track standard ever will be. »

93 Traduit de l'anglais. Texte original : « If IAB thinks we should be violating consumer privacy expectations, do tell. »

processus[94]. » (*public-tracking*, e-mail d'Aleecia McDonald du 13 octobre 2011)

Encore plus que dans les sous-systèmes de politiques publiques de l'UE[95], le capital de crédibilité requis pour avoir une parole efficace dans une controverse au sein d'un groupe de travail par le W3C passe par un discours se présentant sous la forme d'une expertise technique rationnelle, qui peut aboutir à une dépolitisation de la forme, même lorsque le fond reste très politique. Comme nous le verrons dans l'analyse du contenu des discussions tant dans le débat au sein du TPWG sur la définition du « *tracking* » que dans les discussions au sein du PING, cette technicisation des débats est une façon d'inciter les participants à la délibération rationnelle, évitant des « sentiments » parasites laissés volontiers au personnel politique, dans le but de maintenir l'indispensable consensus :

> « Heureusement, nous ne sommes pas là pour obtenir la paix dans le monde. Je pense que nous pouvons atteindre un bon consensus sur la manière d'établir des recommandations avec lesquelles tout le monde peut vivre, même si nos raisons de trouver ces accords sont différentes. […] Il y a plein de régulateurs et de législateurs. Nous disposons d'une position unique pour établir des standards qui soutiennent ces différents systèmes de valeurs, pas pour essayer de standardiser des valeurs.[96] » (*public-tracking*, e-mail d'Aleecia McDonald du 12 décembre 2011)

Luca Belli, en étudiant le fonctionnement de l'IETF, avait conclu que le processus de délibération dans cette arène « vis[ait] à aboutir à la solution régulatoire la plus efficace sur la base d'un « discours rationnel » enrichi par la participation directe d'experts » (Belli, 2016, p. 369). Pour lui, les conditions fixées par Jürgen Habermas dans sa *Théorie de l'agir communicationnel* (Habermas, 1987) pour permettre l'émergence d'un processus discursif participatif sont rempliées par l'IETF (Belli, 2016, p. 369-371), à savoir :

- L'absence de limites concernant la possibilité de prendre part aux discussions en proposant de nouveaux arguments ;

94 Traduit de l'anglais. Texte original : « Personal attacks are not welcome in this group. As stated during the kickoff Boston, that's a great way to make sure the chairs will not recognize you to speak, as a first measure. […] I do not have the time or patience to be put in the rôle of kindergarten teacher. There is a basic level of professionalism and mutual respect necessary to make this process work. »

95 Cf. chapitre 4 et en particulier section 4.1.5.

96 Traduit de l'anglais. Texte original : « Fortunately, we are not here to solve world peace. I believe we can make good consensus decisions on how to create recommendations everyone can live with, even when we have different reasons for reaching those agreements. […] There are regulators and lawmakers aplenty. What we are uniquely positioned to do is to work out standards that support those different value systems, not try to standardize values. »

- L'absence de contraintes qui peuvent biaiser la discussion et empêcher l'examen rationnel des arguments présentés par les participants dans le but de faire émerger la meilleure décision possible ;
- La proposition d'arguments sous forme d'hypothèses pour permettre l'émergence d'arguments alternatifs (Belli, 2016, p. 369).

Ce constat est à nuancer. Il existe des barrières à l'entrée pour participer, même à l'IETF : un coût matériel en temps et en formation, ou en déplacement pour se rendre aux conférences. Le registre de l'expertise nécessaire à la construction d'une crédibilité permettant une participation efficace peut exclure des prises de parole dans un registre d'engagement politique d'acteurs moins expérimentés. Enfin, la participation d'entreprises à l'IETF peut être guidée par des logiques d'intérêt. Au W3C, les travaux de Nick Doty et Deirdre Mulligan (Doty et Mulligan, 2013), mais aussi les éléments de terrain observés dans notre étude, montrent bien qu'il existe des barrières à l'entrée et que certains acteurs peuvent tout à fait développer un agir stratégique dans cette arène.

Cependant, déployer un agir stratégique visible est une pratique stigmatisée, qui n'est revendiquée par aucun des participants. La parole, si elle doit être experte et technique, doit néanmoins impérativement s'inscrire dans la recherche d'un consensus technique dans l'intérêt commun de tous les membres du W3C et des internautes. L'ethos de l'agir communicationnel est donc bel et bien présent au point où – et cela peut paraître paradoxal – il peut devenir stratégique de jouer le jeu de l'agir communicationnel.

5.5.3. À la non-recherche d'une définition commune de la vie privée, un concept « essentiellement contesté »

Avec notre cadre méthodologique générale, et avec la pratique de l'enquête sur des sous-systèmes de politiques publiques, l'un des premiers réflexes pour essayer d'identifier des coalitions au sein du W3C PING a été de chercher à voir s'il y avait ou non un consensus autour de la valeur de la vie privée. Faut-il protéger la vie privée ? À quel prix ? Pourquoi ? Et qu'entend-on par vie privée ?

Or, dès le début du W3C PING, et en raison de la contrainte discursive du consensus que nous venons d'exposer, il y a eu une volonté ferme de ne surtout pas essayer de définir ce que signifie le terme « *privacy* ». Voici par exemple un extrait du journal d'une discussion sur le tchat IRC du W3C PING du 14 septembre 2011 :

« 15:11:46 [npdoty]

… 3) Définitions et Conformité

15:12:00 [npdoty]

… ne pas chercher à définir la « vie privée » ou des concepts si profonds

15:12:15 [npdoty]

… [je] préférerais que nous définissions des conditions plus spécifiques comme par exemple ce qui comptera comme “first-party”

15:12:30 [npdoty]

… travailler sur des définitions est susceptible d'être itératif[97]. » (Aleecia Cooper, propos retranscrits par Nick Doty, dans le log IRC de la première téléconférence du TPWG, le 14 septembre 2011)

Cette préoccupation de ne pas entrer dans un débat de fond sur la définition de la vie privée pour ne pas entraver le « travail productif » et cet omniprésent impératif de recherche de consensus ont été exprimés et évoqués par plusieurs des enquêtés en entretien :

« Alors c'est une question qui a été discutée au sein de l’équipe [*staff*] du W3C et dans le cadre du Privacy Interest Group : celle de savoir s'il fallait une définition formelle et motivante de la vie privée. Je pense que nous n'en avons pas vraiment besoin à ce stade. Je ne suis pas sûr que ce soit actuellement dans notre culture de chercher une définition. […] Ce concept signifie différentes choses pour différentes personnes, et suffisamment de ces concepts ont un lien de parenté pour nous permettre de travailler de manière productive sans disposer de la même définition. […] Il faut être capable de travailler de manière productive[98]. » (Entretien W3C5)

« Certainement cette idée de consensus, de processus multi-parties, et tout ça, des choses

97 Traduit de l’anglais. Texte original : « 15:11:46 [npdoty]
… 3) Definitions and Compliance
15:12:00 [npdoty]
… not looking to define "privacy" or such deep concepts
15:12:15 [npdoty]
… would rather have us define more specific terms, like what will count as a first party
15:12:30 [npdoty]
… work on definitions is likely to be iterative. »

98 Traduit de l’anglais. Texte original : « So it's something that's been discussed in W3C staff and within the Privacy Interest Group, about whether we should have a formal motivating definition of privacy. And I don't think we really do at this point. And I'm not sure there is a strong culture to do so at the moment. […] The concept means different things to different people, and enough of those concepts are related that we can still do productive work in that we don't have exactly the same definition. […] You need to be able to do productive work. »

faites différemment selon les groupes avec différentes forces dominantes, sont tout à fait des questions actuelles, et ce sont des questions suffisamment difficiles lorsque les questions sont assez claires pour que les gens s'accordent sur ce qui doit être fait. Alors si on ajoute à cela que nous ne sommes pas sûrs du tout de la bonne démarche à adopter pour des problèmes aussi nébuleux que la vie privée, alors je dirais que de façon générale cela n'aide pas pour trouver un consensus[99]. » (Entretien W3C10)

Il arrive à de rares occasions que soient mentionnées des questions de définition de la notion de vie privée, ou des éléments de doctrine philosophique ou juridique sur la liste de discussion *public-tracking*. Par exemple, dans un e-mail du 19 avril 2011, Rigo Wenning a évoqué l'article de Samuel Warren et Louis Brandeis (Warren et Brandeis, 1890) dans un fil de discussion sur la notion de droit à l'oubli, tout en faisant mention – comme Cornelius Gallagher l'avait fait avant lui dans les années 1960[100] – à la notion judéo-chrétienne de « pardon » comme sous-bassement spirituel à l'idée d'un droit à l'oubli :

« Le droit à l'oubli n'est qu'un énoncé fonctionnel pour une chose qui mène à un but : Être pardonné. Les humains font des erreurs. Imaginez à quel point ce serait cruel pour une société d'évaluer tout un chacun comme des hommes et femmes politiques de haut niveau. Dès qu'une personne acquiert une certaine notoriété, des éléments d'un passé douteux remontent toujours à la surface (pour traîner dans la boue).

C'est Brandeis, à Boston (ancien juge à la Cour suprême des États-Unis) qui s'est exprimé contre les nouveaux appareils photos portables permettant aux photographes du Boston Inquirer (le journal, je crois) de prendre une photo de son partenaire, Warren, et d'une femme qui n'était pas la sienne, marchant main dans la main dans un parc.

Après quelques années la tension était retombée et Warren a pu reprendre ses activités.[101] » (*public-privacy*, e-mail de Wenning du 19 avril 2011)

99 Traduit de l'anglais. Texte original : « Certainly this idea of consensus and the multi-stakeholder process, and all that, which are done differently in different groups, where there are different dominating forces, is definitely an ongoing issue, and is something where it's difficult enough when the questions are fairly crisp for people to agree on what they think ought to be done. So then add to that that we're not really sure, even close, what the right to thing may be to do for asking various questions on things as nebulous as privacy, and it doesn't help the consensus process any, in general, I would say. »

100 Cf. section 3.2.

101 Traduit de l'anglais. Texte original : « The right to be forgotten is just a functional statement for a thing that leads to a goal: To be forgiven. Humans make mistakes. Imagine how cruel a society would be that would measure everyone of us like high profile politicians. As soon as a persons gets some profile, we are guaranteed to see some nasty things from the past appear (mud throwing).
It was Brandeis in Boston (late judge at the US Supreme court) who wrote against those new portable cameras that allowed photographers from the Boston Inquirer (I think was the newspaper) to take a picture of his partner Warren and a woman who wasn't his wife walking and in hand in a park.
After some years, the dust had settled and Warren could restart to practice. »

Mais, par exemple, ce courriel contient la seule occurrence du terme « brandeis » dans tous les mails échangés sur *public-privacy*. « westin », en référence à Alan Westin, donne seulement deux résultats. La recherche de mots-clefs de quelques autres auteurs (« prosser », « packard », « foucault », « simitis », « mckinnon », « raab », « flaherty ») dans le moteur de recherche de l'archive de public-privacy n'ont donné aucun résultat[102].

Cela ne veut pas dire pour autant que les participants au PING ou au TPWG n'ont pas leur propre définition de la « vie privée ». Łukasz Olejnik, un des membres les plus actifs au sein du PING, désormais élu au TAG du W3C, a été le seul à indiquer en entretien que la vie privée n'avait pas de définition. Simplement, le fait que les membres du PING aient été en mesure de donner leur propre définition du mot « *privacy* » (ou « vie privée » pour les personnes interrogées en français) ne veut pas dire pour autant qu'ils cherchent à la faire adopter par les autres.

La volonté de ne pas chercher à trouver de définition collective au terme a trouvé une expression théorique partagée par plusieurs enquêtés dans la notion de « concept essentiellement contesté » :

> « Nous avons eu en quelque sorte de la chance de ne pas tomber dans certains des sables mouvants, mais peut-être que c'est parce que nous évitons de nous attaquer à certaines des choses fondamentales. C'est peut-être un échec, c'est difficile de savoir de quelle façon le cadrer. Mais je pense que nous avons [travaillé] en ayant conscience que […] certains de ces problèmes ne sont pas bien définis. Deirdre Mulligan parlerait de « concept essentiellement contesté ». Vous savez, c'est un peu le genre de chose sur laquelle il n'y aura jamais de consensus[103] […] ? » (Entretien W3C10)

Nicholas Doty, qui participe au TPWG et à PING, et Deirdre Mulligan, qui a participé longtemps au projet P3P, sont les co-auteurs avec Colin Koopman de l'article scientifique théorisant cette notion qui semble désormais être une référence partagée par les membres du PING (Mulligan, Koopman et Doty, 2016).

L'absence de définition communément partagée de la vie privée ou du droit à la vie privée n'est perçue par aucune des personnes interrogées comme un frein. Cela permettrait au contraire

102 La recherche de ces mots-clefs a été effectuée le 18 juillet 2018.

103 Traduit de l'anglais. Texte original : « So maybe we're kind of fortunate up to this point to not have fallen too deeply into some of the quicksands, and then maybe that we're not tackling some of those fundamental things. It can be failing, it's hard to say which way to frame it. But I think we've [worked] under the knowledge that […] some of these are not well defined, in what Deirdre Mulligan is gonna call an "essentially contested concept". You know, there's this thing where there is never going to be a consensus on […] ? »

de s’assurer que la discussion porte sur des éléments considérés comme plus techniques, un accord consensuel découlant d’implications concrètes de conceptions théoriques sur la « vie privée » étant dégagé au cas par cas seulement dans de rares cas où cela est perçu comme incontournable. Par exemple, sur le mode « incognito » des navigateurs web :

> « Si vous vouliez par exemple, je sais pas, un ensemble d'éléments de base que vous considérez comme disponibles en mode incognito, vous pourriez le faire, parce que c'est bien plus délimité. Cela peut susciter un peu de débat, mais vous pouvez dire que : « pour les besoins de cette discussion ou de ces documents, nous allons utiliser cette définition, vous pouvez en utiliser une autre mais alors signalez-le ». Cela vous permet en quelque sorte de contourner certaines de ces questions.[104] » (Entretien W3C10)

La discussion peut également porter sur l'élaboration de critères d'évaluation objectifs d'un projet de recommandation à évaluer. Par exemple, quelle est sa « surface de *fingerprinting* », c'est-à-dire combien de nouvelles informations la nouvelle fonctionnalité transmet-elle au serveur ? Ces informations sont-elles des données à caractère personnel ? C’est à cela que servent des documents comme le *Fingerprinting Guidance* (W3C Fingerprinting Guidance) et les *Privacy Considerations* (W3C Privacy Considerations) produits par le TPWG :

> « Il existe un document « Mitigating Browser Fingerprinting ». Il existe un questionnaire qui aide, lorsque vous travaillez sur une spécification, à réfléchir aux enjeux de vie privée[105]. » (Entretien W3C10)

En pratique, cela signifie que dans le cas où le PING repère qu'un projet de recommandation prévoit par exemple de nouveaux transferts de données personnelles du client au serveur, l'argument soulevé pour s’y opposer n'est pas un argument de fond sur la nécessité de protéger la vie privée. À la place, la question est posée de savoir si ce transfert de données est nécessaire à la nouvelle fonctionnalité envisagée et si, le cas échéant, il peut être retiré du document discuté, ou s'il pourrait porter sur des données moins précises. La question politique est transformée en question d’apparence technique, susceptible de générer du consensus. Selon Joseph Hall, une telle argumentation peut avoir son efficacité :

---

104 Traduit de l’anglais. Texte original : « If you wanted to have for example, I dunno, a base set of things that you'd consider are available in incognito mode, you might do that, because it's much more constrained. Even then you can get a little bit of debate about that but if you can sort of say: “for the pruposes of this discussion, or these documents, we're going to use this definition, and you can deviate, but you just have to say it then”. And so it kind of allows you to sidestep a few of those questions. »

105 Traduit de l’anglais. Texte original : « There's a Mitigating Browser Fingerprinting document. There is a questionaire, which helps people think through some of the privacy implications of their designs while they're working on a specification. »

> « Dans certains cas, ils disaient : « bon sang [*oh geez*], nous ne souhaitons pas avoir un jeu de valeurs aussi riche pour cette fonctionnalité en particulier, il nous faut vraiment aller vers un signal très simple pour que cela n'aboutisse pas à davantage d'informations identifiantes qui pourraient être utilisées pour violer la vie privée de quelqu'un[106]. » (Entretien avec Joseph Hall)

Le cas où Mozilla est revenu sur son implémentation de la recommandation *Battery Status API* suite à la publication d'une étude montrant que le navigateur Firefox, au moins dans sa version pour GNU/Linux, transmettait des informations trop précises sur l'état de charge des batteries de l'appareil de l'internaute, montre qu'il existe des cas où cet argument fonctionne (Hern, 2016).

Suivant cette logique, les auteurs du document *Privacy Considerations for Web Protocols* du PING ne définissent pas et ne cherchent donc pas à définir la notion de « vie privée » autrement qu'à travers une série de conseils conçus comme de nature technique et opérationnels, et faisant consensus au sein du groupe :

> « Ce document n'essaie pas de définir la vie privée (dans un contexte Web). À la place, la vie privée est une synthèse de ce que contient ce document. Bien que cela puisse ne pas être ce à quoi la plupart des lecteurs s'attendent typiquement, la vie privée est un concept compliqué, avec une longue histoire, traversant plusieurs disciplines, et il demeure toujours une certaine confusion sur le sens de ce concept[107]. » (W3C Privacy Considerations)

Si le PING est parvenu à « éviter le piège », du point de vue de ses membres, d'un débat sur la définition de la « vie privée » comme préalable à la rédaction de documents prodiguant des conseils aux groupes de travail du W3C pour mieux la prendre en compte dans la rédaction de leurs recommandations, le TPWG a été le théâtre d'une longue controverse sur la notion de « *tracking* ».

106 Traduit de l'anglais. Texte original : « In some cases, they said : "oh geez, we don't want this rich of a set of values for this particular feature, it really needs down to a very simple signal, so that it doesn't lead to further identification information that might be used to violate someone's privacy". »

107 Traduit de l'anglais. Texte original : « This document does not attempt to define what privacy is (in a Web context). Instead privacy is the sum of what is contained in this document. While this may not be exactly what most readers would typically assume but privacy is a complicated concept with a rich history that spans many disciplines and there remains confusion over the meaning. »

5.5.4. La controverse sur la définition du « *tracking* »

Pour étudier la controverse qui s'est déroulée au sein du TPWG au sujet de l'adoption d'une définition pour le terme « *tracking* », nous nous sommes fondé sur les trois corpus suivants :

- Les entretiens réalisés avec des membres du W3C PING et TPWG,
- Les 471 courriers électroniques structurés dans la page « *ISSUE-5: What is the definition of tracking?* » du groupe TPWG, échangés entre le 21 septembre 2011 et le 8 avril 2015, accessibles à l'adresse web : https://www.w3.org/2011/tracking-protection/track/issues/5 ;
- Les réactions à plusieurs propositions de définitions d'un appel à objections (Call for Objections) destiné à résoudre le dissensus, ouvert du 8 au 20 novembre 2013, et disponibles à l'adresse web : https://www.w3.org/2002/09/wbs/49311/twpg-tracking-5/results ;
- Les versions successives des documents de travail (Working Drafts) du TPWG archivées sur le site web du W3C, et la proposition initiale qui avait été faite à l'IETF par Jonathan Mayer, Arvind Narayanan et Sid Stamm en 2011 (document IETF draft-mayer-do-not-track-00).

La controverse a été lancée sur la liste *public-tracking* par Roy Fielding, salarié la compagnie Adobe, qui propose des logiciels dans le domaine de la publicité en ligne[108]. Il était éditeur de la spécification TPE du TPWG[109], et avait été co-éditeur des standards de l'IETF sur le HTTP (RFC 1945 et 2616), ce qui lui conférait d'emblée un important capital de crédibilité fondée sur son expertise technique. Cela était particulièrement vrai pour DNT. En effet, son mécanisme de base repose essentiellement sur l'ajout d'un champ « DNT » aux requêtes HTTP du navigateur. Or, dans le domaine du HTTP, même ses plus virulents détracteurs s'accordèrent pour souligner sa compétence[110].

La demande de Roy Fielding de débattre de la définition du mot « *tracking* » n'a pas fait l'unanimité. Aleecia McDonald a réagi le jour même au courriel de Roy Fielding qui lançait le débat en soulevant la même objection que celle par laquelle les participants à PING interrogés dans notre campagne d'entretiens refusaient de débattre de la définition de la vie privée :

108 Voir notamment des produits comme Adobe Marketing Suite et Adobe Web Experience Management.
109 David Singer, de la société Apple, est devenu co-éditeur à partir de la version du 13 mars 2012 du projet de recommandation TPE
110 Entretien avec Rigo Wenning.

> « Une des raisons pour lesquelles nous n'avons pas ouvert le sujet "qu'est-ce que le pistage [*tracking*]" est que nous aurions pu passer facilement jusqu'au mois de juillet à ça. Je comprends la volonté de rédiger des définitions (tracking, first-party, etc.) et c'est effectivement important, mais il serait également utile d'avancer sur des exemples concrets pour produire les premiers documents martyrs [*strawman document*]. Je ne veux rendre aucun débat dépendant de celui-ci[111]. » (*public-tracking*, e-mail d'Aleecia McDonald du 12 octobre 2011)

D'autres ont insisté sur le fait que, quelle que soit la définition adoptée dans les recommandations produites par le TPWG, les conditions particulières de réussite des énoncés performatifs qu'elles renferment font que ce sont les développeurs de navigateurs web qui, de toutes façons, auront en définitive la main sur la façon dont cette option sera présentée aux internautes :

> « C'est aussi important de souligner que le nom que notre groupe attribue ne sera pas forcément communiqué à l'utilisateur. Le paramétrage actuel de Mozilla indique "Dire aux sites web de ne pas me pister". Celui de Microsoft dit : "Protection contre le tracking"[112]. » (*public-tracking*, e-mail de Justin Brookman du 13 octobre 2011)

Brett Error, qui travaillait comme Roy Fielding pour Adobe, une compagnie qui propose des solutions de publicité ciblée fondée sur des analyses comportementales, vint soutenir la proposition de débattre de la définition du « *tracking* » le jour même où ce dernier l'avait ouvert sur *public-tracking* :

> « La volonté [*the urge*] de définir le terme "tracking" vient du fait que l'expression "do not track" signifie que tout pistage est interdit. Ce n'est bien sûr pas notre intention et il nous a donc paru nécessaire de redéfinir et de délimiter [*curtail*] la notion de "tracking"[113]. » (*public-tracking*, e-mail de Brett Error du 12 octobre 2011)

111 Traduit de l'anglais. Texte original : « One of the reasons we did not open with "what is tracking" is we could easily spend until July just on that. I understand the desire to get definitions done (tracking, first party, etc.) and they are certainly important, but we can usefully move forward with concrete examples as we work towards the strawman documents. I do not want to make other discussions dependent on this one »

112 Traduit de l'anglais. Texte original : « It's also important to point out that whatever we call it as a group is not necessarily going to be conveyed to the user: Mozilla's current setting says "Tell websites I do not want to be tracked." Microsoft's setting is "Tracking Protection". »

113 Traduit de l'anglais. Texte original : « The urge to define "tracking" stems from the concern that "do not track" sounds like it will forbid all tracking. That, of course, also is not our intention so we fell compelled to redefine the "tracking" to curtail its scope. »

À mesure que la discussion s'enlisait entre plusieurs propositions de définitions, de plus en plus de voix se firent entendre dans le fil de discussion pour dire que ce débat serait inutile :

> « Le groupe de travail tourne en rond sur les questions de la définition du tracking et du Do Not Track. […] Cette approche n'est pas productive. […] Je propose que nous indiquions que l'ISSUE-5 est REPORTÉE puisque l'obtention d'un consensus à ce sujet n'est pas nécessaire aux tâches du groupe de travail[114]. » (*public-tracking*, e-mail de Jonathan Mayer du 10 décembre 2011)

Ce débat était jugé d'autant plus inutile pour avancer sur le document TPE, dont Roy Fielding était l'éditeur, que celui-ci ne sert qu'à définir la façon dont est codée l'information sur les préférences de l'utilisateur par le navigateur, puis est transmise au serveur web. C'est un autre document, TCS, qui devait permettre de discuter ensuite de ce que devait faire le serveur pour se conformer au signal DNT:1 envoyé par le *user agent* au serveur web. Selon Rigo Wenning, il était donc parfaitement inutile de discuter de la définition du terme « *tracking* » pour rédiger le document TPE :

> « Roy essaie d'importer les discussions difficiles sur le sens de la Spécification sur la Compliance dans la Spécification DNT[115] […] » (*public-tracking*, e-mail de Rigo Wenning du 12 janvier 2012)

Avec le soutien de ses collègues de chez Adobe, Brett Error et Kevin Smith, Roy Fielding imposa la poursuite du débat :

> « Je ne m'intéresse pas au mythe d'un "progrès" continu dans lequel chaque participant comprend différemment ce que nous avons décidé de mettre en place, et prétendons même standardiser[116]. » (*public-tracking*, e-mail de Roy Fielding du 16 janvier 2012)

Dans les e-mails échangés sur le fil de discussion du *tracker* « ISSUE-5 » comme dans les entretiens réalisés dans le cadre de notre enquête, cette demande de la part de Roy Fielding a été

114 Traduit de l'anglais. Texte original : « The working group has now swirled around the "How do we define tracking?" and "How do we define Do Not Track?" drains several times. […] This approach is not productive. […] I would propose that we mark ISSUE-5 as POSTPONED since achieving consensus on it is not necessary to the working group's tasks. »

115 Traduit de l'anglais. Texte original : « Roy is trying to import the difficult meaning discussions of the Compliance Specification into the DNT Specification […] ».

116 Traduit de l'anglais. Texte original : « I am not interest in the fantasy of continued "progress" in which every participant has a different notion of what we have agreed to implement, let alone standardize. »

perçue comme une manœuvre de flibuste : faire durer la discussion en créant des débats (et des clivages) inutiles, pourtant impératifs à résoudre, et faire en sorte de retarder l'adoption du standard ou de le vider de sa substance :

> « Une échappatoire de l'industrie était de discuter sur la définition même du tracking. À un moment, c'était tellement apparent que les autres dans le groupe de travail se disaient: "ah encore cette discussion inutile". Parce que le reste du groupe il était grosso modo conscient du fait que c'était une diversion. » (Entretien avec Rigo Wenning)

Malgré la présence de nombreux opposants à la tenue même d'un débat, de nombreuses propositions de définitions furent soumises à la discussion, y compris par de tels acteurs. Encore une fois, l'impératif de consensus a pris le pas sur les clivages, car il était (ou était perçu comme, ce qui revient au même du point de vue de la contrainte exercée sur les acteurs) impératif d'y parvenir pour que les documents discutés soient implémentés et deviennent véritablement un standard.

L'un des enjeux principaux tournait autour de la distinction entre « *first party* » et « *third parties* ». Le « *first party* » est le site web auquel se connecte un utilisateur, par exemple www.lemonde.fr. Et les « *third parties* » sont tous les autres sites web qui sont appelés pendant le chargement de la page sur www.lemonde.fr, comme dt.adsafeprotected.com, ping.chartbeat.net, static.kameleoon.com, s1.lmde.fr, et bien d'autres encore que nous n'avons pas la place d'énumérer :

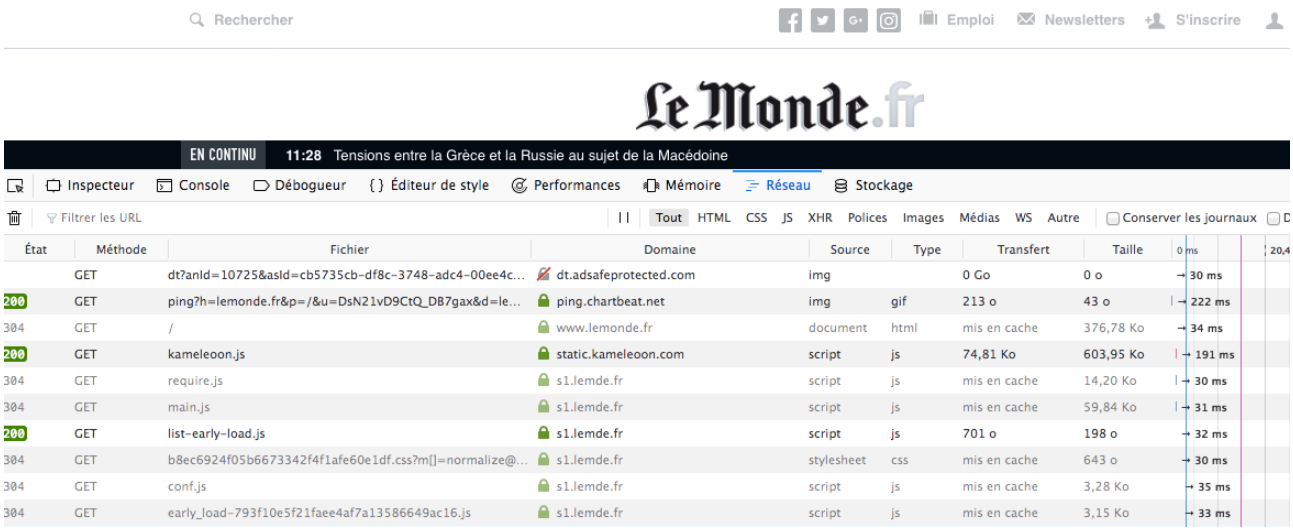


Figure 38 : *Capture d'écran de la console d'analyse des flux réseaux depuis le navigateur web Firefox en allant visiter le site web www.lemonde.fr (page consultée le 19 juillet 2018)*

Si une requête HTTP contenant le signal DNT:1 est transmise au serveur web, par exemple de www.lemonde.fr, ce serveur-ci doit-il lui aussi respecter ce signal ? Ou bien est-ce que le signal ne s'adresse qu'aux sites tiers appelés à partir du serveur de la page web demandée par l'internaute (« *first party* ») ?

Selon Chris Pedigo, de l'*Online Publishers Association* (OPA), qui regroupait alors des éditeurs de journaux en ligne comme Aol news, Fox News, le Financial Times, Reuters ou encore Tech Media Networks[117], imposer des obligations aux « *first parties* » signifierait la mort économique des journaux en ligne, qui ont pourtant, selon lui, la confiance des internautes qui les visitent, et surtout, auraient besoin de la publicité en ligne pour survivre :

> « L'an dernier, les membres de l'OPA ont investi environ 750 millions de dollars dans la création de contenus numériques de grande qualité, qu'ils distribuent en grande partie gratuitement. […]
>
> L'OPA partage la conviction de la FTC que la collecte et l'utilisation d'informations de mesure d'audience à des fins de marketing par des entreprises qui sont en relation directe, de *first party*, avec les consommateurs, sont des pratiques avec des implications en termes de vie privée qui sont très différentes de la collecte et de l'utilisation du même type de données par des tiers [*third parties*] […]. Dans une relation directe de *first party*, les consommateurs sont plus susceptibles de comprendre pourquoi ils reçoivent des informations personnalisées, et sont en meilleure position pour soulever des inquiétudes sur l'utilisation d'information à leur sujet, ou d'exercer leur liberté de choix dans la relation d'affaire [*to exercise choice by taking their business elsewhere*]. […]
>
> Les éditeurs en ligne ont une relation directe et de confiance avec les personnes qui visitent leur site. Dans le cadre de cette relation, les membres de l'OPA recueillent et utilisent parfois des informations pour cibler et proposer de la publicité en ligne qui permet de financer la production de contenus numériques de qualité. […]
>
> Sans une solide exonération des *first-parties* (et une exonération similaire pour des questions opérationnelles et de partage avec les fournisseurs de services), le DNT pourrait devenir un « bouton de mort » [*kill switch*] pour les annonceurs en ligne[118] […]. »

117 Selon la page web archivée par WayBackMachine sur web.archive.org d'une page du site http://www.online-publishers.org, disponible à l'URL : https://web.archive.org/web/20120330163422/http://www.online-publishers.org:80/index.php/join_opa/current_members (page consultée le 10 mai 2018).

118 Traduit de l'anglais. Texte original : « Last year, OPA members invested approximately $750 million in the creation of high quality digital content, most of which they distribute free of charge. […]
OPA shares the FTC's belief that collection and use of audience information for marketing purposes by compagnies that stand in a direct, first-party relationship with consumers have very different privacy implications than similar data collection and use by third-parties […]. In a direct first-party relationship,

(*public-tracking*, e-mail de Chris Pedigo du 30 novembre 2011)

Cette alliance entre plusieurs acteurs de l'industrie de la publicité en ligne, comme Adobe, l'OPA, ou encore l'*Interactive Advertising Bureau* (IAB) pour tenter de redéfinir le « *tracking* » était alors perçue par une coalition de gens par ailleurs pour la plupart actifs au sein de PING comme une tentative de vider le projet DNT de sa substance :

> « Et donc là c'était grosso modo de redéfinir le *tracking*, pour sortir tout ce qui fait obstacle au commerce des données, et de rester avec une carcasse vide où qui rassemble […] les abus les plus grands, mais en même temps, par exemple, les gens de Facebook ont dit : pour nous c'est pas dans le champ d'application parce que de toutes façons on a l'accord de l'utilisateur par la souscription à notre service […] et donc on fait à peu près ce qu'on veut. » (Entretien avec Rigo Wenning)

Effectivement, les discussions ont assez rapidement dérivé sur un éventuel changement de nom du standard reflétant le fait qu'il ne s'applique pas aux « *first parties* ». Le 9 décembre, Kevin Smith, d'Adobe, écrivait :

> « Une suggestion alternative qui, je crois, est alignée sur les opinions de la majorité des membres du TPWG :
>
> Do Not Cross Track (DNXT ci-après) = Ne pas partager ou pister des données entre sites non-affiliés et de marques différentes, avec des exceptions. Dans ce cas, les exceptions seraient bien plus simples, car elles concerneraient à la fois les *first-parties* et les *third-parties* qui n'auraient ni l'un ni l'autre le droit de pister de façon croisée [*cross track*] […].
>
> La confusion que je retrouve dans presque toutes les discussions est que nous parlons *tous* de DNT alors que *la plupart* d'entre nous voulons dire DNXT[119]. » (*public-*

consumers are more likely to understand why they received tailored recommendations and are in a better position to raise concerns about use of information about them, or to exercise choice by taking their business elsewhere. […]
Online publishers share a direct and trusted relationship with visitors to their website. In the context of this relationship, OPA members sometimes collect and use information to target and deliver the online advertising that subsidizes production of quality digital content. […]
Without a robust first-party exemption (and related exemptions for operational purposes and sharing with service providers), DNT could operate as a "kill switch" for online advertisers […]. »

119 Traduit de l'anglais. Texte original : « An alternative suggestion that I believe is in alignment with the majority of the TPWG member's opinions could be :
Do Not Cross Track (DNXT henceforth) = Do not share or track data across unaffiliated non-commonly branded sites – again with possible exceptions. In this case, exceptions would be much simpler as this would apply equally to both 1st and 3rd parties as neither are allow [sic] to cross track […].

tracking, e-mail de Kevin Smith du 9 décembre 2011)

Cette nouvelle définition devait alors permettre des cas d'usage qui, toujours selon Kevin Smith, ne causeraient aucun préjudice à l'internaute :

> « Peu importe à quelle partie appartient le widget. Sous DNXT, aucun pistage croisé n'est possible. Je ne crois pas qu'il y aurait d'inquiétude particulière si google ou un widget météo, dans les exemples cités, ne vous pistaient que dans le contexte du site dans lequel ils sont intégrés. Par exemple, google pourrait se souvenir du niveau auquel vous zoomez, ou de vos coordonnées, et le site météo pourrait configurer le code postal que vous avez saisi comme code postal par défaut[120]. » (*public-tracking*, e-mail de Kevin Smith du 9 décembre 2011)

Cette proposition reçut dès le lendemain l'appui de Chris Pedigo, de l'OPA :

> « Merci, Kevin. Nous sommes d'accord sur le fait que cette approche a les plus grandes chances de succès. Avec ces limites claires, davantage d'entreprises pourront l'implémenter rapidement. Cette approche serait également plus facilement comprise pour le grand public[121]. » (*public-tracking*, e-mail de Chris Pedigo du 10 décembre 2011)

Nous voyons dès ici apparaître un argument fondé sur les attentes (réelles ou supposées par les membres du TPWG) de l'internaute qui active par l'interface de son navigateur web le signal DNT:1. Chaque camp a mobilisé cette figure de l'utilisateur et de ses attentes pour justifier sa position. D'autres participants ont ainsi soulevé une série d'objections au changement de nom en raison de la notoriété que le projet aurait acquis, via la presse, auprès des internautes :

> « Pour ce qui est de changer le nom Do Not Track, je m'y oppose fortement. D'abord, c'est le nom sous lequel cette proposition est connue par le monde entier. […] Tenter de la renommer "Tracking Preference Expression" (NDT : *Expression des préférences de*

The confusion I see in almost every thread is that we *all* say DNT when *most* of us mean DNXT. »

120 Traduit de l'anglais. Texte original : « It does not matter what party the widget is. Under DNXT it cannot cross track. I don't think there would be a ton of concern if google or the weather widget in the examples discussed only tracked you in the context of the site on which they are embedded. For instance, google could remember your zoom level or the coordinates to which you panned, and the weather site may default to the zip code you entered. »

121 Traduit de l'anglais. Texte original : « Thanks Kevin. We agree and think this approach would have the greatest chance at success. With these clean lines of distinction, more companies could quickly implement it. Also, it would be more easily understood by the general public. »

pistage) a entraîné beaucoup de confusion inutile parmi les parties prenantes. Ensuite, Do Not Track est un nom dont la force est de porter un vrai message[122]. » (*public-tracking*, e-mail de Jonathan Mayer du 13 octobre 2011 (a))

D'autres, comme John Simpson, de l'association *Consumer Watch*, ont aussi mobilisé cette image de l'internaute, au début de la discussion, pour exiger que des obligations soient imposées par un signal DNT:1 même à des « *first parties* » :

> « Bien que plusieurs, voire beaucoup de personnes de ce groupe, définissent le DNT comme "ne pas me pister sur des sites de marques différentes", nous ne pensons pas que l'utilisateur l'entendra ainsi. Les utilisateurs s'attendent à ce que le DNT signifie "ne pas pister mes actions sans distinguer entre les actions sur un seul site ou les actions sur plusieurs sites". […] Il me semble que le groupe doive définir la DNT de manière aussi proche que possible des attentes des utilisateurs, ce qui ne se résume pas à le limiter à des sites de même marque[123]. » (*public-tracking*, e-mail de John Simpson du 29 novembre 2011)

Néanmoins, d'autres représentants d'ONG étaient d'accord pour limiter, aux fins des recommandations en cours de discussion, le sens du signal DNT:1 aux situations d'échanges de données vers des « *third parties* », comme l'illustre cet extrait d'un e-mail de Justin Brookman, de CDT :

> « Le groupe s'est accordé assez rapidement sur un cadre selon lequel la DNT doit empêcher le pistage entre plusieurs parties[124]. » (*public-tracking*, e-mail de Justin Brookman du 13 octobre 2011)

Brett Error, quant à lui, mobilisa cette image des internautes « ordinaires » (« *peeps* ») et de leur définition du terme « *tracking* » pour continuer à plaider pour un changement de nom au

122 Traduit de l'anglais. Texte original : « As for changing the name from Do Not Track, I would strongly oppose the move. First, it's the name the world knows this proposal by. […] Attempting to retitle to "Tracking Preference Expression" caused a lot of unnecessary confusion among stakeholders. Second, Do Not Track has real messaging force. »

123 Traduit de l'anglais. Texte original : « Though some – perhaps many – in this group define DNT to mean do not track me across non-same-branded sites, that is not how we believe a user will understand it. Users expect DNT to mean do not track what I'm doing, and don't necessarily make the distinction between activity on one site or across sites. […] It seems to me that that this group should define DNT to conform as closely as possible to consumers' expectations, and that is much broader than merely limiting DNT to non-same-branded sites. »

124 Traduit de l'anglais. Texte original : « The group pretty quickly settled on a framework that says DNT is meant to stop cross-party tracking. »

profit d'un terme qui ne leur fasse pas croire qu'en activant la nouvelle fonctionnalité dans son navigateur, il interdit aux *first-parties* de tracer ses comportements :

> « Si nous choisissons de poursuivre sur notre chemin actuel en imaginant que les gens ordinaires [*peeps*] viendraient à croire que le tracking se résume à une pratique qui concerne uniquement plusieurs sites, soit. Je vais juste attendre dans un coin en vous détestant en silence, et j'essaierai d'utiliser poliment ma petite voix intérieure quand je jubilerai en vous disant dans quelques mois que j'avais raison ;)[125] » (*public-tracking*, e-mail de Brett Error du 13 octobre 2011)

La discussion se prolongea de mois en mois. À partir de mars 2012, de plus en plus de propositions de définitions circulèrent dans le fil de discussion « ISSUE-5 ». Roy Fielding proposa une définition de compromis (assez longue) qui servit un certain temps de base de discussion :

> « "Le tracking correspond au fait de suivre ou d'identifier un utilisateur, agent utilisateur ou appareil sur plusieurs visites vers un site (temps) ou plusieurs sites (espace).
>
> Les mécanismes permettant d'effectuer du tracking comprennent, sans s'y limiter :
>
> - attribuer un identifiant unique à l'utilisateur, l'agent utilisateur [*user agent*] ou appareil afin de le renvoyer au serveur lors de visites futures ;
> - personnaliser les références ou les informations de renvoi [*referral information*] afin de renvoyer l'utilisateur, l'agent utilisateur [*user agent*], ou l'identité de l'appareil vers d'autres sites ;
> - corréler les données fournies dans la requête avec des données identifiantes recueillies lors de requêtes précédentes ou obtenues auprès d'un tiers ; ou,
> - combiner des données fournies dans la requête avec des données désidentifiées recueillies ou obtenues dans des requêtes précédentes, afin de réidentifier ces données ou de les associer à l'utilisateur, l'agent utilisateur [*user agent*] ou l'appareil.
>
> Une préférence de "Do Not Track" signifie que l'utilisateur ne souhaite aucun tracking pour sa requête : ni mécanisme de pistage, ni utilisation de données d'un pistage précédent, ni rétention ou partage de données de sa requête pour un pistage futur, au-delà de ce qui doit nécessairement être mis en œuvre pour permettre :

125 Traduit de l'anglais. Texte original : « If we choose to continue on the current path pretending that the peeps could ever come to think of track as meaning something only involving multiple websites, so be it. I'll just sit here (somewhat) quietly hating you all and I'll try to use my polite inside voice when I dance around saying "I told you so" in a few months ;) ».

1. Les exemptions limitées définies à la section XX ;
2. Au *first-party* (et les tiers agissant en tant que *first-party*) de fournir le service demandé de manière intentionnelle par l'utilisateur ; et
3. D'autres services pour lesquels l'utilisateur a fourni un consentement préalable, précis et informé[126]. » (*public-tracking*, e-mail de Roy Fielding du 4 mars 2012)

Même Rigo Wenning, dont les positions tranchent avec celles de Roy Fielding, accueillit favorablement cette proposition :

« Roy,

considère-moi heureux [*color me happy*] car à première vue, ta définition intelligente me plaît[127]. » (*public-tracking*, e-mail de Rigo Wenning du 7 mars 2012)

Par la suite, Roy Fielding, s'inspirant d'une proposition rédigée par David Singer, rédigea une définition plus succincte :

« Le tracking est la rétention ou le partage de données recueillies lors d'une interaction, afin d'associer cette interaction à un utilisateur spécifique (ou à son agent utilisateur [*user agent*] ou appareil [*device*]), et l'utilisation de cette association pour obtenir, recueillir ou corréler le comportement de cet utilisateur au-delà d'une seule session[128]. » (*public-*

126 Traduit de l'anglais. Texte original : « "Tracking is defined as following or identifying a user, user agent, or device across multiple visits to a site (time) or across multiple sites (space).
Mechanisms for performing tracking include but are not limited to:
• assigning a unique identifier to the user, user agent, or device such that it will be conveyed back to the server on future visits;
• personalizing references or referral information such that they will convey the user, user agent, or device identity to other sites;
• correlating data provided in the request with identifying data collected from past requests or obtained from a third party; or,
• combining data provided in the request with de-identified data collected or obtained from past requests in order to re-identify that data or otherwise associate it with the user, user agent, or device.
A preference of "Do Not Track" means that the user does not want tracking to be engaged for this request, including any mechanism for performing tracking, any use of data retained from prior tracking, and any retention or sharing of data from this request for the purpose of future tracking, beyond what is necessary to enable:
1. The limited exemptions defined in section XX;
2. The first-party (and third-parties acting as the first-party) to provide the service intentionally requested by the user; and
3. Other services for which the user has provided prior, specific, and informed consent. »

127 Traduit de l'anglais. Texte original : « Roy,
color me happy as on a first glance, I like your smart definition. »

128 Traduit de l'anglais. Texte original : « Tracking is the retention or sharing of data collected from an interaction to associate that interaction with a specific user (or their personal user agent or device) and use that association to

tracking, e-mail de Roy Fielding du 4 septembre 2012)

En 2013, plus de deux ans après l'ouverture du fil de discussion « ISSUE-5 » sur le tracker du groupe, Matthias Schunter, employé chez Intel et président (« *chair* ») du TPWG, écrivit que le groupe semblait converger vers une nouvelle évolution de la définition proposée par Roy Fielding :

> « Salut l'équipe,
>
> Pendant notre appel [*call*], il semble que le groupe ait atteint un consensus autour de cette définition du tracking (option 5, de Roy) :
>
> Le tracking est la collecte de données auprès de domaines ou de services de plusieurs parties, et la rétention de ces données sous une forme qui demeure attribuable à un utilisateur, agent utilisateur [*user agent*] ou appareil [*device*][129]. » (*public-tracking*, e-mail de Matthias Schunter du 9 octobre 2013)

Tout l'enjeu devint alors, sur la base de cette proposition vers laquelle convergeait un consensus, de trouver une formulation courte, élégante, et compatible avec ce consensus. La notion de « contexte[130] » fut alors proposée par Roy Fielding pour remplacer des expressions comme « après qu'une transaction réseau ait été complétée[131] » ou encore « à travers les domaines ou services de plusieurs parties[132] ».

Matthias Schunter annonça le 25 octobre 2013 l'ouverture d'un appel à objections. Du 8 au 20 novembre 2013, les participants furent invités à se prononcer sur les trois propositions suivantes :

Option A	Le tracking est la collecte de données sur l'activité d'un utilisateur donné à travers différents contextes distincts, et la rétention, l'utilisation ou le partage de données issues de cette activité en dehors de son contexte.[133]

obtain, collect, or correlate that user's behavior beyond the scope of a single session. »

129 Traduit de l'anglais. Texte original : « Hi Team,
During our call, it seemed that the group was converging on a consensus for this definition of tracking (option 5 by Roy):
Tracking is the collection of data across multiple parties' domains or services and retention of that data in a form that remains attributable to a specific user, user agent or device. »

130 Cf. sections 2.3.5. et 5.6.2.

131 Traduction de l'auteur. Texte original : « after a network transaction is completed ».

132 Traduction de l'auteur. Texte original : « across multiple parties' domains or services ».

133 Traduit de l'anglais. Texte original : « Tracking is the collection of data regarding a particular user's activity across multiple distinct contexts and the retention, use, or sharing of data derived from that activity outside the context in which it occurred. »

Option B	En général, le tracking correspond à la rétention, à l'utilisation ou au partage, après qu'une transaction réseau a été effectuée, de données qui sont ou peuvent être associées à un utilisateur, un agent utilisateur ou un appareil[134].
Option C	Pas de définition

Tableau 14 : *Récapitulatif des trois propositions de définitions soumises au TPWG dans le cadre d'un appel à objections du 8 au 20 novembre 2013. Source : https://www.w3.org/2002/09/wbs/49311/twpg-tracking-5/results (page consultée le 19 juillet 2018).*

Seule une partie des participants au TPWG ont donné leur avis. Rigo Wenning, Vincent Toubiana, Aleecia McDonald, Nick Doty ou encore Joseph Hall, pourtant parmi les plus actifs, ne répondirent pas. Les avis sur la page web qui regroupe toutes les réponses à l'appel à objections ne sont donc pas suffisamment représentatifs pour en tirer des conclusions d'ensemble sur l'état du consensus à cette étape de la discussion. Ce qui est cependant certain, c'est que comme nous l'avons vu, ce mécanisme fut utilisé par le président du TPWG pour résoudre le dissensus sans figer des lignes de clivage, mais en légitimant une position comme étant consensuelle car ayant recueilli moins d'objections que les autres.

L'option A, qui reprenait la version la plus récente des propositions de Roy Fielding, fut adoptée suite à cette procédure, et intégrée dans le document TPE, avec l'adjonction d'une définition du terme « context » :

> « Le tracking est le recueil de données sur l'activité d'un utilisateur donné à travers différents contextes distincts, et la rétention, l'utilisation et le partage de données issues de ces activités hors de leur contexte. Un contexte est un ensemble de ressources contrôlé par une seule partie, ou conjointement par plusieurs parties[135]. » (W3C TPE, version du 19 octobre 2017)

Notons qu'indépendamment de cette définition rédigée dans le document TPE, le document TCS inclut, à côté d'obligations pour les « *third-parties* », quelques obligations que

134 Traduit de l'anglais. Texte original : « In general terms, tracking is the retention or use after a network transaction is complete, or sharing, of data that is, or can be, associated with a specific user, user agent, or device. »

135 Traduit de l'anglais. Texte original : « Tracking is the collection of data regarding a particular user's activity across multiple distinct contexts and the retention, use, or sharing of data derived from that activity outside the context in which it occurred. A context is a set of resources that are controlled by the same party or jointly controlled by a set of parties. »

même les « *first-parties* » doivent respecter lorsque ces sites reçoivent le signal DNT:1 (W3C TCS).

Maintenant que nous avons repéré une controverse qui porte, même indirectement, sur ce qui doit être protégé au nom du « droit à la vie privée », nous pouvons essayer, à partir de celle-ci, d'identifier d'éventuelles coalitions.

5.5.5. La structuration d'une *privacy community* des standards du Web

Est-il possible de distinguer, au sein du PING ou du TPWG, des coalitions d'acteurs, voire même des coalitions de cause au sens de Paul Sabatier ? La tâche n'est pas évidente. L'impératif de consensus, l'évitement des controverses jugées improductives et le non-recours au vote compliquent l'observation de ces coalitions.

Pour ne rien simplifier, il n'est pas toujours possible de savoir si les gens s'expriment en leurs noms propres, ou au nom de leur employeur. Lorsque Simon Rice, de l'ICO britannique, Rob van Eijk, de l'ancien *College Bescherming Persoonsgegevens* néerlandais, ou Vincent Toubiana, qui a travaillé à la CNIL, s'expriment sur *public-tracking* ou *public-privacy*, parlent-ils en leur nom propre, en tant qu'experts invités travaillant pour des organismes qui ne sont pas membres du W3C ? Enfin, les participants passent souvent d'un employeur à l'autre tout en maintenant leur participation au PING ou au TPWG.

Nous venons aussi de voir qu'il existe une marge de manœuvre pour se convaincre mutuellement, pour passer des compromis, ce qui peut parfois déstabiliser la frontière entre coalitions.

Enfin, au W3C comme dans d'autres organisations de standardisation technique, les personnes qui sont en désaccord avec une décision peuvent partir et développer un projet concurrent. Ce fut le cas des participants en désaccord avec le XHTML 2.0, qui partirent créer le WHATWG (Sire, 2017), et ce fut le cas lorsque des anciens du projet P3P souhaitèrent poursuivre leurs efforts en dehors du W3C dans un projet financé par la Commission européenne intitulé « *Scalable policy aware data architecture for privacy, transparency and compliance* » et abrévié SPECIAL[136]. Mais nous n'avons pas observé de scission dans le projet DNT entre un projet qui aurait été porté, par exemple, par une coalition industrielle et un autre porté par une coalition de défenseurs de la vie privée.

136 Entretien avec Rigo Wenning.

Les entretiens n'ont pas non plus permis d'identifier de façon claire des coalitions stables et structurées d'acteurs. À part pour quelques dénonciations du débat sur la définition du terme « *tracking* », perçu comme une manœuvre dilatoire de la part des représentants de la compagnie Adobe, aucun enquêté n'a pu ou souhaité répondre aux questions portant sur l'existence d'alliés ou de rivaux au sein du W3C, en matière de protection de la vie privée et/ou des données à caractère personnel.

L'analyse des controverses à travers les traces qu'elles ont laissées dans les listes de diffusion publiques a été plus productive pour cerner des divergences de point de vue entre acteurs. Il est alors possible, en croisant les renseignements tirés d'e-mails analysés et du corpus d'entretiens, de reconstituer certaines lignes de clivage, qui demeurent néanmoins bien moins nettes que, par exemple, celles qui s'observent dans le champ de l'action publique européenne relative à la protection des données à caractère personnel.

Il existe une préférence forte des participants aux discussions pour éviter les questions de fond potentiellement clivantes et perçues comme plus « politiques » que « techniques ». C'est donc en réalité autour de ce que Paul Sabatier appelle les *aspects secondaires*, c'est-à-dire des éléments textuels concrets qui sont des mesures concrètes n'ayant en fait rien de secondaire, que se sont concentrées les oppositions. Savoir ce que veut dire le « *tracking* », ou se mettre d'accord sur ce que veut dire « *privacy* » et les raisons pour lesquelles il faut protéger la vie privée sont des sujets écartés, au profit de discussions portant, par exemple, sur le degré de précision décimale au-delà de laquelle la possibilité d'accéder à des données sur la charge de la batterie de l'appareil d'un internaute peut contribuer à accroître son exposition à des techniques de *fingerprinting (Hern, 2016* ; Olejnik, Englehardt et Narayanan, 2017).

Dans la même veine, lors de la réunion du PING du 26 octobre 2018 au TPAC de Lyon, une discussion opposait Michael O'Neill de Baycloud à Michael West de l'équipe de développement du navigateur Chrome de Google sur le point de savoir si cela constituait un risque pour la vie privée que des informations permettant de faire du *fingerprinting*, déjà disponibles par des requêtes en Javascript, soient désormais également disponibles dans des en-têtes HTTP en application d'un nouveau standard en cours de discussion : les *Client Hints* (document IETF draft-ietf-httpbis-client-hints-06). Les deux protagonistes du débat étaient d'accord sur l'objectif commun de réduction de la surface de *fingerprinting*, c'est-à-dire de la quantité et de la précision des informations disponibles sur un client pour un serveur, permettant d'identifier les internautes, mais pas sur les modalités d'atteindre cet objectif.

Les logiques d'intérêt, si elles sont souvent passées sous silence, existent malgré tout. La présence de l'industrie publicitaire dans les négociations sur le *Do Not Track* en atteste, tout comme – nous avons pu l'observer lors de la réunion au TPAC de 2018 – la consigne passée aux

ingénieurs d'Apple de ne donner aucune information sur le fonctionnement de l'entreprise. La présence dans le PING d'entreprises comme Brave ou Baycloud qui produisent des logiciels de protection de la vie privée et qui ont intérêt à ce que les standards techniques du Web favorisent l'usage de leurs produits contribuent encore à la démonstration.

Le caractère volontaire et bien souvent bénévole de la participation au PING, et l'impératif de consensus qui pèse sur les discussions au sein des groupes du W3C aboutissent toutefois au sein du PING, et bien plus qu'au sein du TPWG, à une certaine homogénéité.

Ce groupe est ainsi parvenu à structurer un groupe relativement informel de personnes qui sont principalement des ingénieurs qui, pour diverses raisons, se connaissent, et œuvrent de façon volontaire voire bénévole pour une mise à l'agenda de la thématique de la « *privacy* » dans les arènes de gouvernance du Web. Sans définition forcément commune de la vie privée, tous insistent néanmoins comme nous le verrons sur l'importance du « *user control* ». Parmi les membres du TPWG, ceux qui sont aussi membres du PING sont ceux qui auront le plus tendance à exprimer un engagement en faveur d'une plus forte protection de la « vie privée » des internautes. Par exemple, Chris Pedigo, de l'industrie de la presse en ligne, a participé aux échanges sur *public-tracking*, mais pas à ceux sur *public-privacy*. À l'inverse, des personnes comme Mike O'Neill ou Rigo Wenning ont contribué aux deux.

Nous ne pouvons donc pas identifier un système de coalitions de cause rivales comme dans le chapitre précédent. Néanmoins, nous pouvons observer que le W3C PING offre un cadre permettant d'accueillir une discussion entre ces personnes et de fournir une forme de cadre institutionnel, aux contours certes flous, mais qui permet tout de même d'identifier un « lieu » d'expertise sur la protection de la vie privée. Cela a permis de structurer une forme de proto-coalition de défenseurs de la vie privée au sein du W3C, comme nous avions déjà commencé à le voir lors de la présentation de la structure et du rôle de ce groupe[137]. Enfin, c'est sur la poursuite de cet objectif au moment où le groupe devait renouveler sa charte auprès du W3C que les différents participants à la réunion du PING au TPAC de 2018 le 26 octobre 2018 se sont mis d'accord.

En conclusion, rappelons que le projet de standard DNT, combinaison des recommandations TPE et TCS, visait uniquement à permettre à un internaute d'exprimer, via l'interface de son navigateur, sa volonté de ne pas être suivi. Ce n'est pas le seul mécanisme de protection de sa vie privée : il peut utiliser le mode incognito de son navigateur, des protocoles de communication chiffrés comme HTTPS, le réseau TOR, et bien d'autres techniques encore à sa disposition. De ce fait, ce standard DNT n'a pas été perçu par les participants à la discussion comme devant résoudre tout le problème de la protection de la vie privée sur Internet.

137 Cf. section 5.4.4.

L'étude de cette controverse permet néanmoins de tirer de nombreux renseignements sur les conceptions de la « vie privée » exprimées par ses différents acteurs.

Le débat n'a pas directement porté sur une définition de la « vie privée », ni sur l'établissement d'une liste d'effets néfastes de l'absence de vie privée. Mais régulièrement, des arguments ou des termes qui font référence à des conceptions particulières de la vie privée ou reposent sur ces dernières ont été mobilisés par certains acteurs. Le terme de « contexte » renvoie par exemple à la notion de « vie privée contextuelle » d'Helen Nissenbaum (Nissenbaum, 2010), et la figure de l'usager est revenue tout autant que dans les entretiens avec les membres du PING. La question du préjudice est elle aussi abordée : la simple collecte est-elle préjudiciable pour l'internaute ? Ou bien faut-il que cette collecte ait une conséquence néfaste pour qu'il y ait préjudice ?

Chacun de ces arguments et contre-arguments vont maintenant être analysés de façon plus détaillée, en lien avec les autres débats au sein du W3C et avec les résultats de la campagne d'entretiens avec des membres du W3C PING.

5.6. Analyse des arguments sur la « vie privée » en circulation dans les arènes du W3C étudiées

5.6.1. L'image de l'utilisateur et de son contrôle sur ses données

Les personnes qui ont participé à la campagne d'entretiens ont rarement cité des auteurs précis à l'appui de la définition qu'ils donnaient de la notion de vie privée, ou d'une argumentation visant à justifier l'importance du droit à la vie privée. Quatre auteurs font exception : Deirdre Mulligan[138], Helen Nissenbaum[139], Alan Westin[140], et Daniel Solove[141].

Deirdre Mulligan, Nick Doty et Colin Koopman ont défini la vie privée comme étant un concept essentiellement contesté (Mulligan, Koopman et Doty, 2016). Ils rejoignent également Helen Nissenbaum sur sa théorie de la vie privée contextuelle[142], qui a eu une influence certaine sur les discussion au sein du TPWG, comme en témoigne la définition du terme « *tracking* » qui a finalement été adoptée (W3C TPE). Mais, comme nous le verrons, les acteurs du W3C PING ont interprété les théories d'Helen Nissenbaum d'une manière qui les a rendues compatibles avec le paradigme libéral de la vie privée.

138 Evoquée dans les entretiens avec Vincent Toubiana et Joe Hall.
139 Evoquée dans les entretiens : W3C10 et celui avec Nick Doty.
140 Evoqué dans l'entretien W3C1.
141 Evoqué dans l'entretien avec Frank Dawson, cité dans le document *Specification Privacy Assessment*, et cité dans un e-mail de Rob van Eijk du 5 septembre 2012 sur *public-tracking.*
142 Cf. section 2.3.5.

Alan Westin et Daniel Solove sont quant à eux des juristes des États-Unis d'Amérique qui s'inscrivent parfaitement dans le paradigme libéral de la vie privée[143]. Selon ce paradigme, le droit *à la* vie privée est une expression ou une dimension de l'autonomie individuelle exerçant un *contrôle* de l'accès à un espace physique et informationnel dont il fixe les limites selon la poursuite de son utilité.

L'individu, dans le contexte du PING et du TPWG, c'est l'internaute. Son image est omniprésente dans les discussions et les arguments que s'échangent les membres de ces deux groupes. Par exemple, Brett Error et Roy Fielding ont tenté de légitimer le débat sur la définition du terme « *tracking* » par l'importance de coller aux attentes des utilisateurs lorsqu'ils entendent « *Do Not Track* »[144]. S'en est suivie une longue discussion pour savoir quelle était la définition la plus intuitive du terme « *tracking* » pour l'internaute. Voici quelques extraits pertinents de la discussion illustrant ce point :

> « Si un site, strictement *first-party*, peut afficher une publicité grâce à des informations fournies à l'inscription et à la géolocalisation de l'IP, disant : "Bienvenue à nouveau [*Welcome back*], Julia du New York Times ! Vous avez visité ce site pour la dernière fois il y a 2 heures. Je vais vous raconter la vente de gâteaux dans l'école primaire de votre quartier", alors je suis convaincue que les attentes des utilisateurs quant au DNT seront enfreintes de manière significative[145]. » (*public-tracking*, e-mail d'Aleecia McDonald du 12 octobre 2011)
>
> « Je suis d'accord avec Brett et toutes les personnes qui se sont inquiétées du nom "Do Not Track." Il peut engendrer beaucoup de confusion pour les utilisateurs, voire les tromper[146]. » (*public-tracking*, e-mail de David Wainberg du 13 octobre 2011)
>
> « Je pense que la compréhension intuitive est très importante ici. Et je pense que dans l'intuition des gens, le "tracking" signifie "me suivre, noter tout ce que je fais, partout où je vais, tout ce que je regarde, et tout ce que j'achète". C'est louche [*creepy*] dans la vie réelle, et c'est louche [*creepy*] sur Internet.
>
> L'une des choses que j'ai apprises au sujet des humains, des risques, et ainsi de suite, c'est

143 Cf. section 2.2.

144 Voir : E-mails de Brett Error du 12 octobre 2011 et de Roy Fielding du 13 octobre 2011, par exemple, sur le fil de discussion « ERROR-5 ».

145 Traduit de l'anglais. Texte original : « If a strictly-first-party can display an ad based on registration information and geoIP saying, "Welcome back, Julia from the New York Times! It's been 2 hours since you last visited this site. Let me tell you about the bake sale at the elementary school in your neighbourhood,", then I strongly believe user expectations for DNT are going to be violated in a non-trivial way. »

146 Traduit de l'anglais. Texte original : « I agree with Brett and all the others who have expressed concern about the name "Do Not Track." It has great potential to be confusing or even misleading to users. »

que l'on est effrayé par ce qui est involontaire, invisible et intangible, et avec des conséquences inconnues. L'exposition aux radiations est un exemple classique de ce qui peut allumer tous ces voyants [*the classic one that pushes all those buttons*]. Je pense que le tracking sur Internet s'y apparente grandement aussi, malheureusement[147]. » (*public-tracking*, e-mail de David Singer du 22 octobre 2011)

« Si le signal a pour effet que le pistage se poursuive mais que l'on ne voit pas de publicités utilisant ces données, alors il doit être nommé "do not target" (*ne pas cibler*). […] Et de manière similaire, le nom de "do not track" a un sens intuitif : celui de dire que je ne suis pas "suivi" sur le Web, et que personne n'observe ni ne note tous mes faits et gestes[148]. » (*public-tracking*, e-mail de Sean Harvey du 24 octobre 2011)

Quelques rares participants ont refusé de chercher à comprendre comment un internaute définirait le terme « *tracking* », comme Jonathan Mayer[149] et Justin Brookman[150], non pas parce que l'avis de l'internaute ne comptait pas pour eux, mais parce qu'il n'y aurait pas d'accord entre internautes sur ce sujet, et qu'il faudrait aussi tenir compte de différences linguistiques et enfin du fait que de toutes façons, ce sont les navigateurs web qui vont définir les interfaces utilisateur permettant l'activation du signal DNT:1 et l'explication textuelle qui l'accompagne.

Quoi qu'il en soit, l'outil développé dans le cadre du projet de *Do Not Track* devait permettre à l'internaute de mieux contrôler la circulation de ses données. Le terme de « contrôle » est d'ailleurs utilisé à plusieurs reprises, comme par exemple dans l'extrait ci-dessous d'un courriel d'un ingénieur employé par la société Microsoft :

« Consacrons-nous à fournir aux consommateurs davantage de transparence et de **contrôle[151]** sur la collecte et l'utilisation de données en ligne[152] » (public-tracking, e-mail

147 Traduit de l'anglais. Texte original : « I think intuitive understanding is very important here. And I think that people's intuitive sense of "tracking" is "following me around, taking notes of everywhere I go, everything I do, everything I look at, and everything I buy". That's creepy in real life, and is creepy on the internet.
One of the things that I have learned about humans and risks etc., is that people get freaked when something is involuntary, and invisible/intangible, and with unknown consequences. Radiation exposure is the classic one that pushes all those buttons. I think internet tracking comes quite close as well, unfortunately. »

148 Traduit de l'anglais. Texte original : « If the effect of the signal is that tracking carries on, but you don't see ads that are targeted based on that data, then it should be called "do not target". […] Similarly, called "do not track" has an intuitive meaning that I am not being "followed" around the web, no-one is "tracking my every move and writing it down". »

149 E-mail du 13 octobre 2011.

150 Email du 13 octobre 2011.

151 Mis en gras par l'auteur.

152 Traduit de l'anglais. Texte original : « Let's focus on providing consumers with greater transparency and **control** over online data collection and usage. »

de J.C. Cannon du 23 octobre 2011)

C'est cet objectif de contrôle par l'internaute qui est opposé par Jeffrey Chester de CDT, le 1er décembre 2011, à l'argument exposé dans un e-mail du 30 novembre 2011 par Chris Pedigo de l'OPA, selon lequel interdire aux *first-parties* de faire de la publicité comportementale auprès des internautes ayant activé le signal DNT:1 reviendrait à tuer économiquement l'industrie des médias numériques :

> « Plutôt que de voir le DNT comme un « disjoncteur » [*"kill switch"*], offrir du **contrôle utilisateur**[153] [*user control*] sur un processus puissant conçu pour influencer son comportement et sa prise de décision devrait être vu comme une pratique commerciale qui bénéficie à tous[154]. » (*public-tracking*, Jeffrey Chester, e-mail du 1er décembre 2011)

Cette formule désignant le contrôle par l'internaute (« *user control* ») se retrouve dans des documents produits par le TPWG, mais aussi par le PING :

> « Les utilisateurs ont besoin d'un mécanisme pour indiquer leurs préférences en termes de pistage [*tracking*] qui soit à la fois simple à configurer, et efficace lors de sa mise en œuvre[155]. » (W3C TPE, version du 19 octobre 2017)
>
> « Do Not Track est conçu pour proposer aux utilisateurs un mécanisme simple d'expression d'une préférence, pour autoriser ou limiter le pistage [*tracking*][156]. » (W3C TCS, version du 26 avril 2016)
>
> « Il est important pour les utilisateurs de pouvoir contrôler l'accès à leurs données[157]. » (W3C Privacy Considerations)

Au cours des entretiens réalisés avec les membres de PING, nous avons demandé quelle définition chacun donnait à la « vie privée », quelle justification il donnait au droit *à la* vie privée, et, lorsque la durée de l'entretien le permettait, quels arguments il utilisait pour convaincre des gens qui n'accorderaient à leurs yeux pas assez d'importance ou de ressources à la protection

153 Mise en gras par l'auteur.

154 Traduit de l'anglais. Texte original : « Rather than seeing DNT as a "kill switch", providing **user control** over a powerful process designed to influence their behavior and decision-making is a business practice that should benefit everyone. »

155 Traduit de l'anglais. Texte original : « Users need a mechanism to express their own preferences regarding tracking that is both simple to configure and efficient when implemented. »

156 Traduit de l'anglais. Texte original : « Do Not Track is designed to provide users with a simple mechanism to express a preference to allow or limit online tracking. »

157 Traduit de l'anglais. Texte original : « It is important for users to be able to control access to their data. »

de la vie privée. Le thème du contrôle par l'internaute sur ses données est systématiquement revenu dans les réponses. Cette sélection d'extraits d'entretiens illustre la façon dont l'image du contrôle par l'internaute (ce « *user control* »), proche, finalement, de l'idée d'auto-détermination informationnelle, est évoquée au sein du groupe :

> « Voici comment je vois les choses : la vie privée et la sécurité sont toutes deux des attributs du système. Et la sécurité est la tendance d'un système à faire ce qu'il est conçu pour faire. […] La vie privée est légèrement différente car elle est **centrée sur l'utilisateur**. Ainsi, peu importe qui a créé le système, la question est la suivante : **le système fait-il de leurs données ce que les utilisateurs en attendent**[158] ? » (Entretien avec Sid Stamm)

> « Il y avait cette mouvance en recherche, qui disait : tiens, on va faire quelque chose d'intelligent, et on va donner, on va créer de la transparence, […] guidés par la philosophie américaine qui est : notice and choice […]. **Ça veut dire que c'est assez proche de l'auto-détermination**[159]. » (Entretien avec Rigo Wenning)

> « Il s'agit juste de montrer du point de vue de l'utilisateur, de l'individu, à quoi va ressembler l'utilisation de ces protocoles sur leur appareil et où qu'ils soient déployés […]. Nous sommes là pour protéger les individus et leurs droits informationnels[160]. » (Entretien avec Simon Rice)

> « Alors il y a une forme de définition, […] je pense : **le contrôle utilisateur**. Il a beaucoup été question de choses comme : les permissions, le consentement, dans le modèle Web, avoir un agent utilisateur … L'idée est censée être que **tu disposes d'un élément logiciel qui travaille en ton nom et que tu contrôles**[161]. » (Entretien W3C5)

---

158 Traduit de l'anglais. Texte original : « The way I see it is: privacy and security are both attributes of the system. And security is a tendency for a system to do what it's designed to do. […] Privacy is a little different because this one is **user-centric**. So regardless of whoever created the system, the question is: **does the system do what its users expect with the data**? »
Texte mis en gras par l'auteur.

159 Texte mis en gras par l'auteur.

160 Traduit de l'anglais. Texte original : « Just showing, from the perspective of the user, of the individual, what it's gonna be using these protocols in their device or wherever it ends up being deployed […]. We're here to protect people and their information rights. »

161 Traduit de l'anglais. Texte original : « So there is a form of definition, […] I think: **user control**. And so there has been a lot of focus on things like: talking about permissions, consent, in the web model, having a user agent... The idea is supposed to be that **you have this piece of software that is working on your behalf, that you have this control over**. »
Texte mis en gras par l'auteur.

Cette idée du contrôle exercé par l'internaute s'articule assez bien avec la façon dont les navigateurs web sont définis comme des *user agents* au W3C. Sid Stamm a ainsi mobilisé cet argument pour convaincre ses collègues de Mozilla d'accorder plus d'importance à la protection de la vie privée et de s'impliquer dans le projet *Do Not Track* :

> « I thought it would be really nice if that web browser that Mozilla was producing, which claimed to be a user agent, was actually asserting some sort of agency for its users[162]. » (Entretien avec Sid Stamm)

Cet argument de l'intérêt de l'utilisateur semble être, selon les enquêtés, utilisé avec succès dans le cadre d'une institution comme le W3C qui s'affiche comme menant une mission d'intérêt public, et où cet intérêt public correspond à l'intérêt du plus grand nombre d'utilisateurs du Web :

> « Je pense que lorsque la vie privée est considérée comme une sorte de contrôle utilisateur ou comme un bénéfice pour l'utilisateur… ce qui je crois est assez courant, je pense qu'alors on n'entend pas trop dire que : oh, c'est une mauvaise chose[163]. » (Entretien W3C5)

Dans la version de 2015 du questionnaire sur la sécurité et la protection des données produit par le TAG pour aider les groupes à rédiger leurs « *Security and Privacy Considerations* », l'argument d'un besoin de contrôle par l'utilisateur a également été mobilisé pour justifier l'importance d'accorder du temps et des ressources à ces questions :

> « L'ajout de fonctionnalités au Web est un piège. D'un côté, nous voulons donner aux développeurs accès à tout ce dont ils ont besoin pour créer des expériences fortes. D'un autre côté, nous devons nous assurer que nous ne donnons pas trop de pouvoir à des personnes mal intentionnées, qui pourraient en abuser ou involontairement exposer les données privées des personnes **sans contrôles appropriés**. Il serait idéal de minutieusement examiner chaque spécification que nous publions afin de trouver le bon équilibre[164]. » (W3C TAG Security and Privacy 2015)

---

162 Traduction : « Je pensais que ce serait une bonne chose que le navigateur Web que Mozilla produisait, et qui était soi-disant un agent utilisateur, avance une sorte d'agencéité pour ses utilisateurs. »
Les concepts anglais utilisés dans cet extrait se traduisent mal en français. Le texte original en anglais a donc été conservé dans le corps du texte.

163 Traduit de l'anglais. Texte original : « So I think when privacy is branded as that sort of user control, or user benefit perspective, which … I think is fairly common, I don't think we'll hear too much: oh, that's a bad thing. »

En définitive, l'invention de mécanismes de contrôle est une tâche qui peut être réalisée par de l'ingénierie, comme à travers des projets comme P3P ou DNT. Il devient alors possible, comme l'a fait Łukasz Olejnik en entretien, de définir la vie privée comme étant une propriété d'un système technique ; ou bien, comme nous l'avons vu plus haut avec une citation de l'entretien avec Sid Stamm, comme étant un système qui tend à exécuter les commandes de son utilisateur au lieu de celles de son concepteur.

La thématique du « *user control* » côtoie l'idée selon laquelle, conformément à la théorie d'Helen Nissenbaum, la vie privée est une affaire de « contextes ». Un projet comme le *Do Not Track* devait permettre, selon les discours de notre corpus, d'offrir à l'*individu* un *contrôle* sur les *contextes* dans lesquels des informations qui le concernent circulent. Ce faisant, les acteurs de notre terrain sur le W3C ont rendu compatible la théorie de la vie privée contextuelle[165] avec un paradigme libéral de la vie privée[166] auquel Helen Nissenbaum s'oppose pourtant.

5.6.2. La vie privée contextuelle

La discussion sur la définition du « *tracking* » a débouché sur à la rédaction d'une définition du pistage comme étant la circulation de données recueillies sur une personne dans un contexte vers d'autres contextes, par exemple : la réutilisation de données collectées par un site web de comparatif de prix de billets d'avions pour afficher une publicité avant une vidéo sur un site de partage de vidéos comme Youtube ou Dailymotion.

Certains acteurs de la controverse, comme Chris Pedigo de l'OPA, ont essayé de s'appuyer sur un argumentaire inspiré de la notion de « contexte » développée par Helen Nissenbaum[167] pour fonder l'argument selon lequel il était socialement acceptable, dans le contexte de la visite d'un internaute sur un site web, que ce dernier apprenne des choses sur lui (*public-tracking*, e-mail de Chris Pedigo du 30 novembre 2011). Ils y sont parvenus, puisque cette position est reflétée, outre dans la définition du mot « *tracking* », dans le document TCS :

164 Traduit de l'anglais. Texte original : « Adding features to the web is a tricky thing; on the one hand, we want to provide developers with access to all the things they need in order to build amazing experiences. On the other, we need to ensure that we don't accidentally hand over too much power to malicious folks who could abuse it, or unintentionally expose people's private data **without adequate controls**. Ideally, careful review of every specification we publish will allow us to strike the right balance. »
Texte mis en gras par l'auteur.

165 Cf. section 2.3.5.

166 Cf. section 2.2.

167 Cf. section 2.3.5.

> « Concernant une action donnée de l'utilisateur, une première partie en rapport avec cette action qui reçoit un signal DNT:1 PEUT collecter, conserver et utiliser des données reçues par ces interactions réseaux[168]. » (W3C TCS)

Ce succès des acteurs ne souhaitant pas interdire aux « *first parties* » de conserver et utiliser des données sur les utilisateurs visitant leur propre site web ne signifie pas pour autant qu'ils sont parvenus à convaincre les défenseurs de la vie privée du PING. Mais comme nous l'avons vu, la contrainte de consensus pèse très lourdement[169] et, pour ces acteurs militants, un standard DNT interdisant *a minima* aux parties tierces (« *third parties* ») de pister les internautes valait mieux qu'une absence de standard.

La théorie contextuelle de la vie privée définit également des contextes où l'utilisation de données est légitime, voire attendue. Pour Joseph Hall, de CDT, une association militante qui défend le droit *à la* vie privée et avait été à l'initiative du projet P3P au début des années 1990, cela peut définir des cas d'utilisation légitime de données personnelles malgré l'opposition de la personne concernée :

> « Aux États-Unis, Helen Nissenbaum a défini la notion d'intégrité contextuelle, et elle utilise la surveillance de la santé publique comme un grand exemple de violation de la vie privée. Quelque chose est utilisé contre votre volonté, nécessairement, peut-être que vous n'avez pas eu le choix. Mais dans le même temps, c'est pour un intérêt public supérieur[170]. » (Entretien avec Joseph Hall)

Nous avons d'ailleurs vu qu'Helen Nissenbaum a développé une critique de la notion de consentement présente dans le droit *de la* protection des données personnelle. Il pourrait donc y avoir contradiction entre d'une part l'image d'un utilisateur en contrôle de ses données et le droit à l'auto-détermination informationnelle, et, d'autre part, l'application d'une théorie contextuelle de la vie privée.

168 Traduit par l'auteur. Texte original : « With respect to a given user action, a first party to that action which receives a DNT:1 signal MAY collect, retain and use data received from those network interactions. »

169 Cf. section 5.5.

170 Traduit de l'anglais. Texte original : « In the US, Helen Nissenbaum has this notion of contextual integrity, and she uses the public health monitoring as a great example of something that is of: yes, it's a privacy violation, something is being used against your choice, necessarily, you may not have a choice. But at the same time, it's for a greater public good. »

Mais l'usage que des défenseurs de la vie privée font de la théorie contextuelle se fond finalement assez bien avec le paradigme libéral de la vie privée et l'idée du « *user control* ». Ainsi, selon Vincent Toubiana, l'un des membres actifs du projet *Do Not Track*, salarié de la CNIL au moment de l'entretien, et qui avait d'ailleurs travaillé avec elle sur des travaux de recherche :

> « J'avais développé un outil qui permettait de générer des fausses requêtes sur Google. Et ensuite donc, c'est comme ça que j'avais commencé à m'intéresser à cette thématique-là. Y avait des gens à l'université de New York, Helen Nissenbaum, qui travaillaient sur un outil similaire. J'ai rejoint l'université de New York pour mon post-doc. […] Et j'avais aussi développé une extension, à l'époque, […] qui s'appelait **Context Aware Do Not Track**. […] Helen Nissenbaum travaille beaucoup sur tout ce qui est **contextual integrity**, donc l'idée est de dire que ce qui compte c'est le contexte dans lequel les informations sont collectées et utilisées. Donc **si les informations sont utilisées dans le même contexte que dans lequel elles sont collectées, pour lesquelles on a consenti, y a, a priori, dans l'esprit des internautes, pas de violation de la vie privée**[171]. » (Entretien avec Vincent Toubiana)

Dans cet extrait, nous pouvons voir qu'un contexte où une information sur un individu peut légitimement circuler est donc un contexte pour lequel la personne concernée a consenti.

Quant à Deirdre Mulligan, Nick Doty et Colin Koopman (Mulligan, Koopman et Doty, 2016), la théorie de la vie privée contextuelle permet de régler des situations qu'un contrôle individuel sur ses données ne pourrait pas résoudre, par exemple quand des algorithmes sont capables de faire des inférences inattendues sur des données librement partagées par une personne (Mulligan, Koopman et Doty, 2016, p. 2). La théorie contextuelle vient là répondre aux situations dans lesquelles le mécanisme du consentement n'est pas suffisant, sans pour autant remettre en cause, loin s'en faut, le principe de « *user control* » assimilable au droit à l'auto-détermination informationnelle du paradigme libéral de la vie privée.

Ainsi, dans le discours des acteurs du PING, il ne semble pas exister de contradiction forte entre le rôle central de l'image de l'internaute en contrôle (individuel) de ses données et l'adhésion à la théorie de la vie privée contextuelle. Traduite en les termes utilisés par le droit de l'Union européenne de la protection des données à caractère personnel, inspiré par le paradigme libéral de la vie privée, le consensus au sein du PING serait de dire que, dans le cas général, un site web peut collecter des données avec le consentement libre et éclairé de l'utilisateur (c'est le

171 Mise en forme en caractères gras et surlignage ajoutés par l'auteur.

« *user control* ») ou bien, dans certains cas, se fonder sur un intérêt légitime (ce qui n'est possible que dans un contexte socialement accepté dans le langage de la théorie contextuelle[172]).

Le mécanisme DNT était justement conçu pour collecter ce consentement à ce que des tiers à la relation entre l'internaute et le site qu'il visite collecte des données à d'autres fins que la fourniture du service pour lequel l'internaute a visité ce site.

Pour revenir à l'exemple donné par Joseph Hall d'utilisation de données médicales contre l'avis de la personne concernée pour faire une étude épidémiologique, il s'agit d'un argument qui est également utilisé par Amitai Etzioni pour montrer que le droit à la vie privée doit pouvoir être limité par des considérations d'intérêt légitime (Etzioni, 1999). Mais Amitai Etzioni a tort de prétendre que les membres de la coalition de cause de la « *privacy community* » n'admettent aucun cas d'utilisation de données personnelles contre le gré de la personne concernée dans des cas d'intérêt général. Ainsi, l'association EDRi, l'une des plus actives dans les arènes européennes pour défendre le droit *à la* vie privée et à la protection des données à caractère personnel, reconnaissait implicitement un droit à la recherche médicale à accéder à des données même sans consentement :

> « Le traitement de données sensibles à des fins historiques, statistiques et scientifiques **n'est pas aussi urgent ou pressant que la santé publique** ou la protection sociale. En conséquence, il n'y a pas lieu d'introduire d'exception fondée sur le droit national, qui mettrait ces traitements au même niveau que les autres justifications recensées, en risquant de nuire aux droits fondamentaux à la sécurité juridique et au marché unique[173]. » (Corpus Lobbyplag, EDRI2)

La mobilisation combinée d'arguments en faveur d'un « *user control* » proche de la théorie libérale de la vie privée et de la théorie contextuelle d'Helen Nissenbaum soulève donc quelques contradictions, puisque les deux théories sont en désaccord sur le point de savoir ce qui peut légitimer la collecte de données sur un individu. Dans le premier cas, c'est le consentement, et dans le second, cela dépend du respect de barrières contextuelles socialement situées. De plus,

172 Dans le droit de l'Union européenne, le consentement de la personne concernée n'est qu'une des bases légales, prévues à l'article 7 de la directive 95/46/CE puis à l'article 6 paragraphe 1 du RGPD, pour qu'une collecte de données à caractère personnel soit licite. L'article 6, paragraphe 1, sous e) du RGPD prévoit ainsi la possibilité qu'une autorité publique se passe du consentement de la personne concernée dans le cadre de la réalisation d'un service public prévu par la loi. Et la CEDH a déjà eu l'occasion de dire que certaines ingérences dans la vie privée d'une personne pouvaient être autorisées sur le fondement de la poursuite d'un autre intérêt général, tant que cela reste dans les limites de ce qui est « nécessaire dans une société démocratique ».

173 Traduit de l'anglais. Texte original : « Processing of sensitive data for historical, statistical and scientific research purposes is **not as urgent or compelling as public health** or social protection. Consequently, there is no need to introduce an exception, based on national law, which would put them on the same level as the other listed justifications, which risks undermining fundamental rights, legal certainty and the single market. »
Texte mis en gras par l'auteur.

des acteurs du débat sur le « *tracking* » ont utilisé la notion de « contexte » pour épargner aux « *first parties* » de se voir imposer des obligations en cas de réception d'un signal DNT:1.

Pour les défenseurs de la vie privée du W3C, dont nous avons vu dans l'étude de la controverse sur le « *tracking*[174] » qu'ils étaient opposés à cette demande de représentants de l'industrie de la publicité en ligne même s'ils l'ont acceptée pour permettre au projet DNT d'avancer, la référence à la théorie contextuelle n'a pas tout à fait le même sens. Elle est plutôt assimilable à une référence théorique sur la valeur sociale du droit *à la* vie privée tout en rejoignant, dans les modalités pratiques du contrôle du respect de ce droit, le paradigme libéral : c'est dans leurs discours l'individu qui doit être équipé d'outils techniques (comme P3P ou le DNT) qui lui permettent d'exprimer ses préférences personnelles en matière de vie privée. En d'autres termes, c'est lui qui doit être en mesure de dire les contextes acceptables de collecte, circulation et utilisation de données qui le concernent.

5.6.3. Le thème de la confiance

Comment faire en sorte, pour les défenseurs de la vie privée du W3C, inspirés par le paradigme libéral et des emprunts à la théorie contextuelle rendus compatibles avec le paradigme libéral, de convaincre d'autres acteurs d'investir des efforts dans l'adaptation des standards techniques du Web pour les rendre plus protecteurs de leur vision du droit *à la* vie privée ?

Sur les terrains de l'OCDE, du Conseil de l'Europe[175] puis dans les « discussions » sur le RGPD[176], l'argument de la confiance avait joué un rôle déterminant dans la stratégie argumentative des défenseurs de la vie privée.

Nous retrouvons aussi sur le terrain du W3C PING et du TPWG l'argument selon lequel, sans l'adoption de certaines mesures protectrices de la vie privée, le public – constitué ici par les internautes – risque de perdre confiance, ce qui pourrait avoir des conséquences économiques négatives pour les entreprises qui génèrent leur revenu sur le Web.

Le schéma ci-dessous montre l'évolution du terme « trust » dans les arènes étudiées. Il présente pour chaque liste de discussion représentée (*public-tracking* pour le TPWG et *public-privacy* pour le PING) :

174 Cf. sections 5.5.4. et 5.5.5.
175 Cf. section 3.8.
176 Cf. section 4.5.

- Une ligne continue qui représente le nombre d'occurrences du mot « *trust* », par mois, dans les e-mails échangés sur la liste de discussion ;
- Une ligne pointillée qui représente le nombre d'occurrences de ce mot, divisé par le nombre total de mots dans tous les e-mails sur le mois, multiplié par 10 000 par souci de lisibilité.

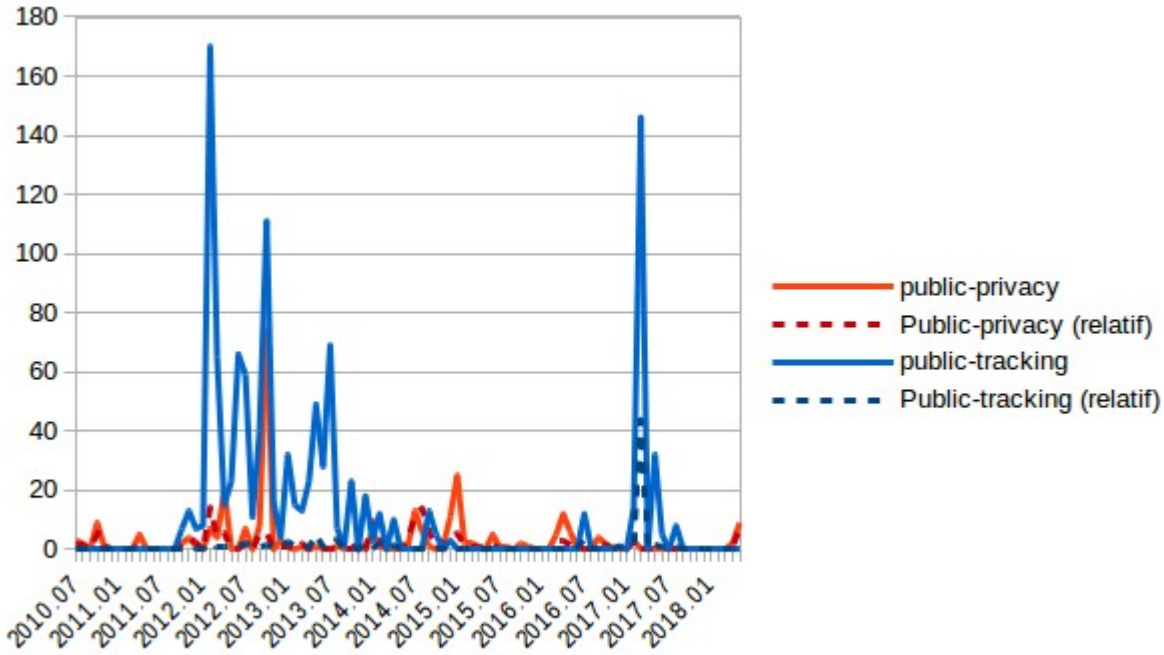


Figure 39 : *Evolution de l'utilisation du mot « trust » sur* public-tracking *et* public-privacy

Le premier constat est que le terme « *trust* » n'est pas présent de manière continue dans les discussions, ni en termes absolus, ni en proportion de l'intensité des discussions sur un mois donné. Le terme semble rarement prendre une place importante dans les discussions. En même temps, ce même schéma montre également le mot « *trust* » n'est pas totalement absent. De plus, ce n'est pas parce que l'argument est rarement formulé et répété, que lorsqu'il l'est, il n'a pas d'importance. L'organisation, à l'époque du PLING, d'un atelier sur « l'établissement de la confiance et de la vie privée sur le web social[177] » (W3C, 2008) montre que, pour ses organisateurs, le lien entre les notions de « vie privée » et de « confiance » n'était pas anecdotique.

Sur *public-tracking*, les premières discussions sur la confiance ont porté sur la confiance entre *first-party* et *third-parties* : un *first-party* peut-il faire confiance aux *third-parties* pour que

177 Traduction de l'auteur. Texte original : « Enabling Trust and Privacy on the Social Web »

ces derniers respectent le signal DNT:1 que l'internaute lui a transmis[178] ? Mais nous trouvons aussi des exemples dans la liste d'e-mails que le graphique ci-dessus nous aide à identifier où il est fait mention de l'argument selon lequel la confiance en un responsable de traitement (en l'occurrence, un site web) est utile pour permettre à un marché économique, comme celui de la publicité, d'exister et de se développer :

> « Lorsque des consommateurs constatent que leurs droits sont dûment reconnus ils deviennent plus enclins à faire confiance au commerce en ligne, ce qui aura pour résultat d'élargir le marché dans son ensemble[179]. » (*public-tracking*, e-mail de Mike O'Neill du 11 octobre 2012)
>
> « Il s'agit de créer de la confiance pour les marchés[180]… » (*public-tracking*, e-mail de Rigo Wenning du 16 octobre 2012)

Cet argument a été concédé par Chris Pedigo, de l'OPA, qui regroupe des entreprises du secteur de la presse en ligne, dans le fil de discussion sur la définition du « *tracking* » :

> « Les éditeurs savent que leurs capacités futures à attirer d'importantes audiences de consommateurs vers leurs propriétés numériques dépendront de la confiance des consommateurs[181]. » (*public-tracking*, Chris Pedigo, e-mail du 30 novembre 2011)

Dans l'analyse de ces exemples, nous devons garder à l'esprit le rôle joué par l'obligation de parvenir à un consensus dans les groupes de travail du W3C, qui contraignent à des discours prenant au moins l'apparence de l'agir communicationnel. Les discours ouvertement stratégiques, comme les discours fondés sur l'idée qu'il « faut » adopter le DNT pour garder la « confiance des utilisateurs » sont donc relativement rares quoi qu'il arrive, ce qui rend chacune de leurs occurrences d'autant plus significatives.

Les discussions sur *public-privacy* sont encore moins conflictuelles que sur *public-tracking*, puisque contrairement à ce dernier, les personnes qui y consacrent du temps sont globalement d'accord entre elles sur les objectifs à poursuivre. Cela n'a pas empêché des emplois du terme « *trust* » en relation étroite avec des réflexions sur la vie privée.

---

178 Voir : *public-tracking*, e-mail de David Wainberg du 30 novembre 2011

179 Traduit de l'anglais. Texte original : « When consumers see their rights are being properly recognised they will be more prepared to trust online commerce which will result in a larger total market. »

180 Traduit de l'anglais. Texte original : « It is all about making trust for the market place... »

181 Traduit de l'anglais. Texte original : « Publishers know that their future ability to attract large consumer audiences to their digital properties will depend on consumers' trust. »

Par exemple, le 18 avril 2012, Dan Brickley, qui travaillait pour le projet Schema.org, un projet en rapport avec le web sémantique, et qui a rejoint Google depuis, se demandait comment les autres membres du PING définiraient la « vie privée », dans une discussion informelle qu'il souhaitait sans enjeux, de simple curiosité, et ne transgressant pas le tabou sur les débats théoriques sur les définitions[182], d'où l'emphase qu'il a mise sur « in _your own_ definition » dans la citation ci-dessous. Dans le même e-mail, il évoquait la difficulté de faire confiance à des grandes entreprises ou à des États pour respecter sa vie privée :

> « Et… ce n'est pas vrai. Encore une fois, qu'est-ce que la vie privée (selon _votre propre_ définition ?) ?
>
> J'ai ma propre idée, mais je suis curieux de voir votre raisonnement. […]
> […] J'accorde en particulier de la valeur à **la possibilité pour les personnes de dire et de faire** des choses en ligne avec des preuves techniques, sociales ou juridiques que des personnes indésirables ne suivent et ne journalisent pas leurs activités, par exemple pour autoriser les activités anonymes ou sous pseudonyme.
> En pratique, il faut avoir des connaissances très techniques et avoir du temps pour réussir cela sans **faire confiance** aux grandes entreprises pour (a) qu'elles se comportent bien (b) être facilement infiltré et (c) être contraint par les gouvernements à se comporter de manière inappropriée.
> J'aime « le droit d'être laissé tranquille » [*"right to be let alone"*]. C'est clair, simple, et cela définit la vie privée comme un droit (qui devrait être protégé par la Loi)[183]. » (*public-privacy*, e-mail de Dan Brickley du 19 avril 2012)

Dans un autre e-mail, Charles McCathie Neville, de Yandex, évoquait le fait que les navigateurs ont un rôle dans la réputation des sites web et la confiance que peut leur accorder ou non les internautes :

> « 29.01.2015, 18:41, "Wendy Seltzer" <wseltzer@w3.org>:
> > Je me demande quel genre de commentaires pourrait conforter les utilisateurs finaux
> > dans l'idée que leur consentement a été mérité.
>
> Celui qui est évident, c'est la gestion de la réputation, qui peut être gérée par des navigateurs, des tierces parties [*third parties*], […]

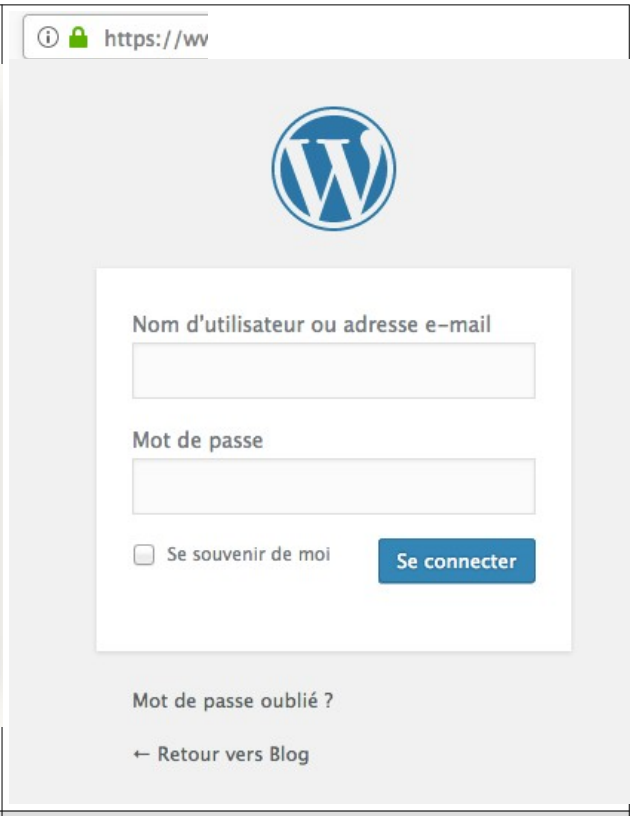
182 Cf. section 5.5.3.

183 Traduit de l'anglais. Texte original : « And... it is not true. Once again, what is privacy (in _your own_ definition)?
I have my own idea, but I'm curious about this line of thought. […]
[…] I value in particular **the ability for people to say and do** things online with some technically and social/legally grounded evidence that unexpected others aren't monitoring and logging one's activities, e.g. to allow anonymous or pseudonymous activities.
In practice, you have to be very technical and have time on your hands to achieve that without placing some **trust** in big companies to (a) behave well (b) be easily infiltrated (c) be forced into misbehaviour by govts.
I like "the right to be let alone". It's clear and simple, and defines privacy as a right (which should be protected by law). »
Texte mis en gras par l'auteur.

D'un autre côté, utiliser une telle modalité en conjonction avec un environnement réglementaire respectueux de la vie privée et avec les types de systèmes d'alertes qui nous protègent actuellement contre les logiciels malveillants, le phishing et les spams, pourrait suffire à de nombreuses personnes et constituer une motivation pour les concurrents de trouver des moyens de prouver qu'eux aussi méritent tout autant **la confiance des gens**[184]… » (*public-privacy*, e-mail de Charles McCathie Neville du 30 janvier 2015)

Il faisait référence dans son e-mail à la possibilité pour les navigateurs de sémiotiser la confiance ou l'absence de la confiance par ce que Armen Khatchatourov, Patrick Waelbroeck, Claire Levallois-Barth et Antoine Dubus appellent des « marques de confiance » ou des « signes de confiance » (Khatchatourov, 2018 ; Levallois-Barth, 2018 ; Waelbroeck et Dubus, 2018), comme c'est déjà actuellement le cas sous Firefox lorsqu'un site web nous invite à entrer un mot de passe alors qu'il n'utilise pas le protocole HTTPS :

Exemple de tentative de connexion à un compte sur un site web sans support HTTPS



Exemple de tentative de connexion à un compte sur un site web avec support HTTPS

184 Traduit de l'anglais. Texte original : « 29.01.2015, 18:41, "Wendy Seltzer" <wseltzer@w3.org>:
> I wonder what sorts of feedback could help to reinforce to end-users
> that their trust was in fact merited.
The obvious one is reputation management, which can be done by browsers, third parties, […]
On the other hand, using such a mode, in conjunction with a privacy-friendly regulatory environment and the sort of warning systems that currently protect us against malware, phishing and spam might be enough for a lot of people - and a motivator for competing services to find ways of demonstrating that they too are equally deserving of **people's trust**… »
Texte mis en gras par l'auteur.

Figure 40 : *Exemple de sémiotisation par les navigateurs web de signes de danger ou de confiance en fonction du support ou non du protocole HTTPS par les sites visités*

La lecture des *mailing-lists public-tracking* et *public-privacy* nous apprend donc que le terme « confiance » n'est pas si souvent utilisé, et pas de manière constante. Mais elle permet de trouver quelques exemples significatifs où la « confiance » a été utilisée comme argument pour justifier la mise en place de mesures de protection de la vie privée, d'une façon similaire à celle que nous avons observée dans les arènes européennes. Par ailleurs, nous voyons bien qu'il existe bien un lien entre les deux thématiques, y compris dans les discussions au sein du W3C, et il arrive que la confiance soit évoquée sans pour autant qu'elle soit mobilisée au service d'une stratégie argumentative, mais simplement pour constater un lien entre « vie privée » et « confiance ».

Là où les cas d'emploi de la stratégie argumentative fondée sur la « confiance » sont significatifs mais rares dans les listes de discussion étudiées, ce discours a eu une place importante dans les réponses des enquêtés aux questions en entretien.

Pour Frank Dawson, la confiance est même au cœur de la définition de la notion de protection de la vie privée, en tout cas dans un contexte de communications électroniques. Il a raconté en entretien comment, lorsqu'il s'est documenté sur la notion de vie privée, il est tombé sur cette notion de confiance qui peut revêtir de nombreux sens différents et dont il regrette qu'elle ne fasse pas l'objet d'une discussion plus explicite :

> « En 2009, lorsqu'on m'a demandé de faire de la vie privée [*to do privacy*], j'ai dit […] eh bien, je sais pas, je verrai bien que c'est que la vie privée. […] Je suis allé à quelques réunions des professionnels de l'*International Association of Privacy Professionals*, et j'ai commencé à consulter tous les articles sur le sujet dans le *New York Times*, le *Guardian*, et le *Wall Street Journal*. Et un mot était sans cesse répété, qui faisait hocher la tête à tout le monde : oui, oui. Et c'était le mot « confiance ». Et quand je regardais qui était autour de la table, il y avait des Américains, des Britanniques, et la confiance pour les Britanniques était une sorte de confiance conditionnelle, née de la révolution industrielle. Mais si l'on s'intéressait aux pays du nord de l'Europe, comme la Finlande, et aux entreprises des pays nordiques, on s'aperçoit que leur conception de la confiance y est fondée sur la philosophie d'Emmanuel Kant. Cela ressemble à la confiance d'une mère en ses enfants, cela s'appelle souvent la confiance perpétuelle[185]. » (Entretien avec Frank

185 Traduit de l'anglais. Texte original : « In 2009, when I was told to do privacy, I said […] well, I don't know, I'll figure out what privacy is. […] I went to some of these privacy profesionals meetings, the International Association of Privacy Professionals, and I started following on the New York Times, and the Guardian, and Wall Street Journal, all the articles on privacy. And one word was always repeated, and everybody would nod their head: yes, yes. And it was the word trust. And, you know, ironically, when I looked around the table, we

Dawson)

Sid Stamm et Vincent Toubiana ont aussi évoqué l'importance de se préoccuper de la protection de la vie privée de ses utilisateurs pour garantir et mériter sa confiance. Pour Joseph Hall, de CDT, l'objectif du PING est de créer des outils dans lesquels, parce qu'ils en ont le contrôle, les internautes peuvent avoir confiance :

> « Nous faisons de notre mieux pour nous assurer que les utilisateurs puissent avoir **confiance** dans toutes les choses formidables que nous construisons sur Internet, mais également pour qu'ils puissent avoir du **contrôle**[186]. » (Entretien avec Joseph Hall)

Dans ce discours, « confiance » et « contrôle par l'utilisateur » sont liés. Selon encore un autre des enquêtés, le contrôle des données qui le concernent par l'utilisateur est la condition pour que ceux-ci acceptent d'utiliser les services qui lui sont proposés. Cet argument est une ligne de défense lorsque l'argument selon lequel les données collectées sont nécessaires pour proposer des services innovants aux utilisateurs est avancé, par exemple dans le cadre d'applications de *Quantified Self* :

> « Je pense que nous entendons souvent que certaines pratiques de collecte de données sont bonnes pour l'utilisateur. Et je pense que c'est comparable au concept de *Quantified Self* : **si** les utilisateurs ont le contrôle alors ils pourraient réellement recueillir des données […] sur eux-mêmes et utiliser des services en ligne pour les gérer[187]. » (Entretien W3C5)

Il semble même que « *trust* », « *user control* » et « *privacy* » soient encore davantage liés dans le discours des défenseurs de la vie privée du PING que dans ceux de la « *privacy community* » du Conseil de l'Europe, de l'OCDE ou de l'Union européenne. En effet, pour ces derniers, l'argumentaire fondé sur la « confiance » était surtout un discours stratégique d'articulation de leur référentiel au référentiel global. Leur engagement en faveur des droits *à la* vie privée et *à la* protection des données à caractère personnel découlait plutôt, dans leur grande majorité, de convictions fondées sur le paradigme libéral de la vie privée.

---

had Americans, we had British, and their version of trust was sort of a conditional trust. How, like you would, trust grew up out of the industrial revolution. If you looked though at Nothern Europe, and Finnish and Nordic and Northern European companies, their view of trust is based around Emmanuel Kant. It is a similar kind of trust that a mother has for their children, it's often called perpetual trust. »

186 Traduit de l'anglais. Texte original : « We're trying our best to make sure that users can **trust** these wonderful things we're building in the Internet, but also that they have **control**. »
Texte mis en gras par l'auteur.

187 Traduit de l'anglais. Texte original : « I think we often hear the perspective of some sorts of data collection practices are good for the user. And I think that is actually a bit similar with the Quantified Self, right, that **if** users are in control then they might really collecting data […] about themselves and use online services to deal with that. »
Texte mis en gras par l'auteur.

Mais même si les acteurs du PING intègrent plus facilement – mais pas toujours – la notion de « confiance » dès le moment où ils donnent leur définition de la « vie privée », comme dans certains des exemples que nous venons de voir, nous avons aussi vu des exemples d'emploi stratégique de cet argument pour légitimer le « besoin » d'adopter des mesures (comme le DNT) pour éviter de perde une confiance du public qui serait une condition indispensable au bon fonctionnement de marchés économiques en ligne.

N'oublions d'ailleurs pas que la FTC avait joué un rôle important pour contraindre les acteurs de l'industrie publicitaire à participer aux discussions sur le DNT[188]. Or, c'est justement cet emploi stratégique de l'argument de la confiance que David Vladeck, de la FTC, mobilisa dans son discours :

> « Comme l'industrie l'a elle-même reconnu, donner aux consommateurs des choix quant à la publicité en ligne est **capital pour construire la confiance nécessaire à la croissance du marché**. Sur le long terme, la méfiance détériore la confiance dans le marché, ce qui n'est bénéfique pour personne[189]. » (Vladeck, 2011, p. 10)

À ce sujet, tant la littérature (Doty et Mulligan, 2013) que plusieurs des entretiens réalisés[190] insistent sur le rôle du FTC dans la création du projet DNT. Et si, finalement, la crainte de la sanction juridique n'était pas l'argument moteur derrière les efforts entrepris au W3C en matière de vie privée, dans lesquels de grandes entreprises comme Google, Apple et Microsoft, ont également investi ?

5.6.4. La réglementation en embuscade

Comme nous l'avons vu dans la section présentant les arènes de la gouvernance d'Internet[191], l'IETF et le W3C plongent leurs racines dans un projet de rejet du rôle des États dans la gouvernance d'Internet, exprimé entre autres dans la fameuse « Déclaration d'indépendance du Cyberespace » (Barlow, 1996) et reflétée par le *Tao* de l'IETF (Hoffman, 2012). En entretien, certains enquêtés ont minimisé l'importance du rôle des réglementations de nature étatique dans les raisons qui ont motivé les membres du TPWG à participer au projet DNT, ou qui motivent les autres groupes de travail du W3C à solliciter les conseils du PING. Le rôle

188 Cf. section 5.4.5.

189 Traduit de l'anglais. Texte original : « As industry itself has recognised, providing consumers with choices about online advertising **is essential to building the trust necessary for the marketplace to grow**. In the long run, mistrust erodes market confidence, and that benefits no one. »

190 Entretiens avec Rigo Wenning, Sid Stamm et Vincent Toubiana.

191 Cf. section 5.2.3.

qu'avait joué la FTC dans les années 1990 dans le soutien au projet P3P, puis à partir de 2009 dans le soutien au projet DNT, nous a toutefois conduit à interroger de près les rapports réels entretenus par le PING et le TPWG à la puissance étatique, et en particulier à la Loi. Nous verrons ici qu'en réalité, l'argument d'un nécessaire respect de lois – et au moins des lois européennes de protection des données – a joué un rôle au moins aussi important que l'argument de la « confiance » dans la stratégie argumentative des défenseurs de la vie privée du W3C.

Ce rôle n'est pas nécessairement perçu par les acteurs eux-mêmes, ou tout du moins, il est souvent minimisé en entretien. Certains jugent de tels arguments inefficaces dans le contexte du W3C[192]. Simon Rice, un ingénieur employé par une autorité européenne de protection des données au moment de l'entretien, a ainsi rappelé que les personnes physiques et morales qui s'occupent de standardisation ne sont pas nécessairement celles qui la mettent en œuvre et qui, donc, en sont responsables au sens des diverses lois de protection des données qui existent de par le monde :

> « C'est compliqué. Cela nous ramène au fait que les designers de protocoles ne sont pas spécifiquement les responsables du traitement. Donc c'est difficile à dire : est-ce que ce protocole est conforme à la législation européenne ? Dans beaucoup de cas il n'a pas besoin de l'être. C'est juste un protocole. Ce n'est pas vraiment du traitement de données, il n'y a pas de responsable du traitement[193]. » (Entretien avec Simon Rice)

Cela signifie qu'en soi, l'adoption d'un standard technique permettant de commettre de nouvelles infractions, ou facilitant la commission de nouvelles infractions au droit *de la* protection des données à caractère personnel, n'est pas juridiquement répréhensible. De toutes façons, et cela est régulièrement évoqué et discuté dans les nombreux échanges d'e-mails que nous avons lus, tant sur *public-geolocation*, *public-tracking* que *public-privacy*, les éditeurs de standards ne peuvent pas toujours prédire les usages qui seront faits des systèmes techniques qu'ils normalisent. Ils ne peuvent donc pas, de leur point de vue, en assumer la responsabilité.

De surcroît, il existe sur la planète de nombreuses lois différentes, parfois contradictoires. Plusieurs enquêtés ont donné cette explication pour expliquer pourquoi ils préféraient se tenir à distance des lois :

> « La législation est très différente d'une juridiction à l'autre […]. Les objectifs de W3C

192 Entretien W3C10.

193 Traduction de l'auteur. Texte original : « It's tricky. It goes back to the protocol designers not being the data controllers specifically. So it's difficult to say: does this protocol comply with European legislation? In a lot of cases it doesn't need to. Because it's just a protocol. It's not actual processing, there is no data controller. »

sont de développer des choses qui vont se compléter et être utilisés à une échelle mondiale[194]. » (Entretien W3C5)

Le monde de la standardisation technique et le W3C en particulier seraient donc peu perméables aux lois et règlements des États :

« Je pense qu'au moins dans mon expérience avec les standards, tout d'abord, il y a une tendance à rester raisonnable à distance de la Loi… par super loin. Mais il n'y a pas vraiment de grande attention portée à la réglementation dans la façon dont les standards sont faits. Donc ça veut dire qu'ils ne seront pas convaincus par des questions d'accès à certains pays, par des perspectives juridiques ou ce genre de choses. Il arrive qu'il en soit question, mais cela n'a pas tendance à dominer les discussions[195]. » (Entretien W3C10)

Il semblerait alors, au moins dans un premier temps, que la déclaration d'indépendance du cyberespace de John Perry Barlow soit effectivement suivie d'effet. Le web se serait affranchit de ses « las géants de chair et d'acier[196] » (Barlow, 1996). La *Lex Informatica* régirait les interactions sociales sur Internet sans obéir nullement à un hiérarchie des normes juridiques (Kelsen, 1962 [1934]) qui la placerait en dessous des lois et règlements d'origine étatique.

Pourtant, à y regarder de plus près, nous avons pu observer :

1. Le droit est très régulièrement mobilisé comme argument en faveur de telle ou telle modification d'un projet de recommandation du W3C ;
2. Les participants perçoivent une forme de pression d'origine étatique qui les incite à investir dans des projets comme P3P, DNT ou PING, et à relâcher leurs efforts lorsque cette pression se fait moins sentir.

L'État, même s'il est tenu à distance, demeure en fait fortement présent dans les discours et les préoccupations des acteurs de notre terrain. D'ailleurs, le terme « law » est évoqué, avec des hauts et des bas, mais de façon stable, avec régularité, depuis la fin des années 1990, et pas seulement dans les arènes du W3C spécialisées dans des thématiques de protection de la vie privée :

194 Traduit de l'anglais. Texte original : « Regulations differ so much between jurisdictions […]. The goals of W3C are to develop these things that are going to be complemented and used worldwide »

195 Traduction de l'auteur. Texte original : « I think that at least my experience with standards is that, first of all, it tends to stay reasonably far away from the law... Not super far away. But there isn't as much looking into how the standards are done with a very strong focus on regulation. So it means that they are not going to be swayed by country access, legal perspectives or something. It sometimes comes up, but it doesn't tend to dominate discussions. »

196 Traduction de l'auteur. Texte original : « weary giants of flesh and steel ».

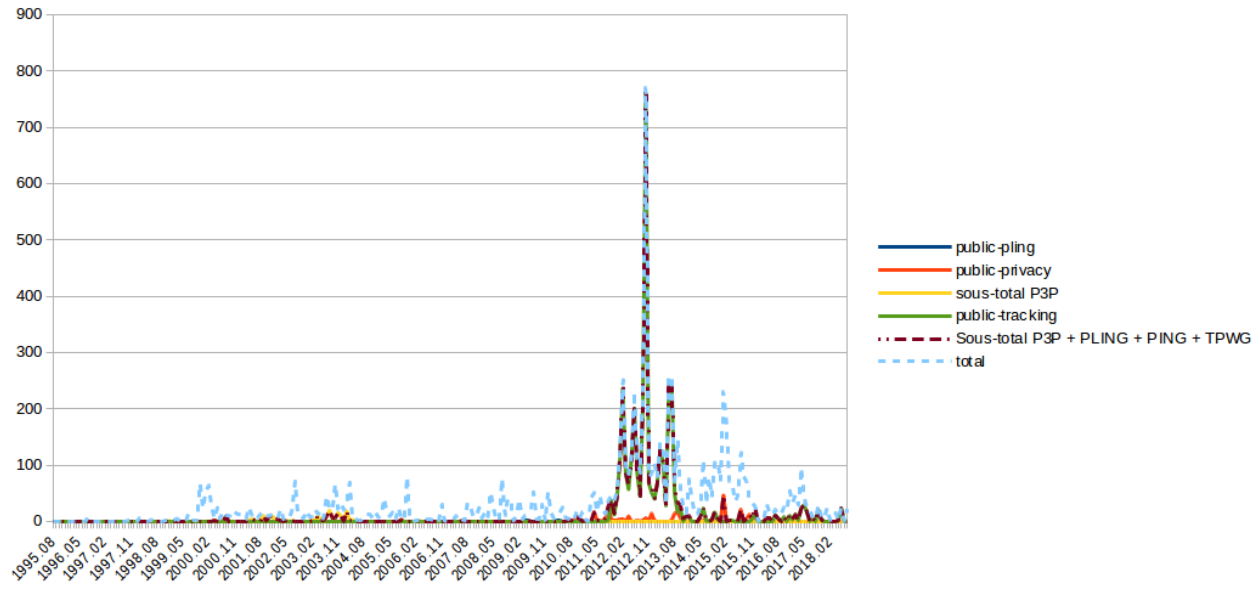


Figure 41 : *Évolution de l'emploi du terme « law » au cours du temps sur les* mailing-lists *du W3C*

Entre 2011 et 2013, nous voyons une intense activité autour du terme « *law* » au sein du groupe *public-tracking*. La lecture du contenu des échanges sur cette période montre en effet d'intenses réflexions et débats sur le rapport entre le standard *Do Not Track* et les différents régimes juridiques applicables en particulier à la publicité ciblée.

Nous pouvons aussi observer la mobilisation d'arguments juridiques dans les débats du TPWG sur la définition du terme « *tracking* », et, en filigrane, sur la nécessité ou non d'exiger aux *first-parties* qu'ils réagissent au signal DNT:1.

Jonathan Mayer insista par exemple au début de la controverse sur le « *tracking* » sur l'importance du respect des frontières organisationnelles dans l'organisation des flux de données, selon lui, pour respecter le droit tant européen qu'états-unien de la protection *de la* vie privée :

> « Les frontières organisationnelles sont un fondement de multiples domaines réglementaires et de politique publique [*policy*]. […] Les frontières organisationnelles sont très importantes pour la protection de la vie privée en ligne […]. L'un des choix de vie privée les plus efficaces qui soient offerts à un consommateur – et qui revient dans d'innombrables textes de loi relatifs à la vie privée aux États-Unis et ailleurs – est d'imposer dès le départ une limite sur les organisations qui ont un accès illimité à leurs

données[197]. » (*public-tracking*, e-mail de Jonathan Mayer du 25 octobre 2011)

Cet argument a permis d'insister sur le fait qu'*a minima*, un signal DNT:1 devait empêcher un site appartenant à une personne physique ou morale autre que celle du site dont l'adresse a été entrée par l'internaute dans la barre d'adresse de son navigateur, d'accéder à des données personnelles le concernant.

Un peu plus tard, un ingénieur de Google a insisté sur l'importance pour lui que les définitions contenues dans les projets de spécifications *Do Not Track* soient compatible avec les définitions des mêmes termes dans des textes de loi des États-Unis ou de l'Union européenne :

> « Et que se passe-t-il lorsque nous proposons notre propre interprétation de « marquage commun » [*"commonly branded"*], et que cinq ans plus tard, de nouveau régulateurs, aux États-Unis ou dans l'Union européenne, en proposent une autre[198] ? » (*public-tracking*, e-mail de Sean Harvey, e-mail du 27 octobre 2011)

Cet argument lui a permis d'obtenir l'abandon d'une proposition qui consistait à n'interdire que les flux de données personnelles de l'internaute en dehors d'un ensemble de sites « partageant la même marque » (« *commonly branded* »). Dans les documents TCS et TPWG, l'expression de sites qui « partagent une même marque » (« *commonly branded* ») a été remplacée par celui de « contexte » (« *context* »).

À peu près un mois après cet échange, Ninja Marnau, juriste qui travaillait à l'époque pour l'autorité de protection des données du Land de Schleswig-Holstein[199], a ouvertement brandis la menace de la loi. Écrire dans les recommandations du TPWG qu'un *first-party* peut être exempté d'obéir à la volonté de l'internaute qui lui transmet un signal DNT: 1 inciterait les sites web qui se fonderaient dessus à enfreindre la directive e-Privacy de l'Union européenne :

> « Si vous acceptez de ne pas inclure le *first-party tracking*, vous décidez de ne pas répondre aux exigences de l'article 5, paragraphe 3, de la directive E-Privacy au sujet des

197 Traduit de l'anglais. Texte original : « Organizational boundaries are a cornerstone of many areas of regulatory law and policy. […] Organisational boundaries are particularly important for online privacy […]. One of the most effective privacy choices available to a consumer – which turns up in countless privacy regulations in the U.S. and elsewhere – is a limit on which organizations have unfettered access to their data in the first place. »

198 Traduit de l'anglais. Texte original : « And what happens when we come up with our interpretation of "commonly branded" and five years later a new set of regulators in the united states or an EU country come up with a different one? »

199 L'*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*.

first parties. Occasion manquée[200]. » (*public-tracking*, e-mail de Ninja Marnau du 30 novembre 2011)

Cet argument n'a cependant pas eu le succès escompté. Shane Wiley, l'ingénieur de l'entreprise Yahoo qui y dirige l'équipe de protection de la vie privée, membre de l'IAPP, lui a en effet aussitôt répondu avec d'autres arguments de nature juridique. Il rappela d'abord qu'au 30 novembre 2011, au moment où se déroule cet échange de courriers électroniques, la directive e-Privacy n'était selon ce qu'il venait d'apprendre pas encore transposée partout. Il ne souhaitait donc pas en tirer de conclusions qu'il jugeait hâtives :

« Avec seulement 14 États-membres sur 27 ayant transposé la directive ePrivacy ou proposé des lois en ce sens (ce qui était requis pour avant le 25 mai 2011), je pense qu'il est beaucoup trop tôt pour soulever cette question dans le cadre du débat sur le DNT[201]. » (*public-tracking*, e-mail de Shane Wiley du 30 novembre 2011)

Puis, n'étant pas lui-même juriste et parlant à quelqu'un qui travaille dans une autorité de protection des données, il légitima son propos en rappelant qu'il était en train de participer à un événement de l'IAPP, l'association internationale des professionnels de la protection de la vie privée. Il y avait obtenu des nouvelles plus fraîches, et de la bouche même de personnes d'autorités de protection des données. Implicitement, il déniait par ce biais à Ninja Marnau sa légitimité à parler au nom d'une autorité de protection des données :

« Je suis à l'événement de l'IAPP EU et il y a des désaccords considérables, même entre autorités de protection des données, concernant les vraies intentions de la directive ePrivacy et la manière dont cela devrait être géré en pratique avec les utilisateurs (personnes concernées[202]). » (*public-tracking*, e-mail de Shane Wiley du 30 novembre 2011)

Enfin, il enfonça le clou par son analyse de la directive e-Privacy, à laquelle « la plupart des autorités de contrôle auxquelles il a parlé » adhèrent, en indiquant que celles-ci admettraient

200 Traduit de l'anglais. Texte original : « If you agree on not including first party tracking, you decide to not address in which way soever the requirements of Art. 5 III of the E-Privacy Directive concerning first parties. Lost opportunity. »

201 Traduit de l'anglais. Texte original : « With only 14 of 27 member states having transposed or suggest current laws already the amended ePrivacy Directive (was required by May 25th 2011 by law), I believe it's far too early to draw upon that perspective in the DNT discussion. »

202 Traduit de l'anglais. Texte original : « I'm at the IAPP EU event and there is considerable disagreement even across DPA's as to the true intentions of the ePrivacy Directive and how this should be managed in practice with users (data subjects). »

une présomption de légitimité pour les cookies (et autres données) déposées par un *first-party* sur le terminal d'un internaute :

> « La directive ePrivacy ne requiert pas de consentement pour l'utilisation d'un cookie « légitime » pour fournir un service, et la plupart des autorités de protection des données considèrent que cela s'applique à l'utilisation de cookies *first-party* : seuls les cookies publicitaires de *third-parties* sont réellement visés par la directive ePrivacy[203]. » (*public-tracking*, e-mail de Shane Wiley du 30 novembre 2011)

Shane Wiley a été contraint d'utiliser d'autres arguments juridiques, et pas n'importe quel autre type d'argument, qui contredisaient ceux de Ninja Marnau pour maintenir l'exclusion des *first-parties* du champ d'application matériel des recommandations du TPWG.

Un autre point de débat pendant la controverse sur le « *tracking* » avait été de savoir s'il s'agissait seulement d'un mécanisme pour interdire l'affichage de publicité ciblée, ou si cela devait aussi s'appliquer à la collecte de données nécessaire en amont de l'affichage de publicités. Jacob Kohnstamm, président du G29, envoya un courrier à Alain Heureux, président de la branche européenne de l'IAB, et à Angela Wills-Wade, vice-présidente de l'*European Advertising Standards Alliance* (EASA). Ce courrier a été communiqué au TPWG par un e-mail de John Simpson, de Consumer Watchdog, le 5 mars 2012. Il contenait une expression de soutien au projet DNT et développait les conditions selon lesquelles le standard DNT pourrait selon le G29 être utilisé pour recueillir un consentement juridiquement valable d'internautes pour faire de la publicité comportementale. Enfin, il indiquait que pour Jacob Kohnstamm comme pour ses collègues européens à la tête d'autorités de protection des données, lorsqu'un internaute active le signal DNT: 1, ce n'est pas simplement à l'affichage de publicités ciblées qu'il s'oppose, mais également à la collecte de données comportementales à son sujet. Ce faisant, cette lettre du G29 est venue mettre un terme à une partie du débat sur la définition du terme « *tracking* », qui ne pouvait dès lors plus se limiter au seul affichage de publicité ciblée (Kohnstamm, 2012c).

À la question sur les arguments qu'il utilisait pour convaincre des membres du W3C de s'intéresser à la protection de la vie privée dès la conception des standards du Web, Rigo Wenning a répondu : « Avec la régulation, avec la régulation de la vie privée européenne ».

203 Traduit de l'anglais. Texte original : « The ePrivacy Directive does not require consent for "legitimate" cookie use to deliver a service and most DPAs I've spoken to have felt this covers 1st party cookie use and that only "3rd party advertising cookies" are the true target of the ePrivacy Directive. »

Une des difficultés principales, sinon la difficulté principale, pour les personnes impliquées dans PING, est de convaincre d'autres gens de consacrer du temps, de l'énergie et des ressources à participer à leurs travaux. C'est pour cela que certains y identifient l'idée selon laquelle de toutes façons la « vie privée » serait une cause perdue comme étant un des principaux contre-arguments auxquels ils doivent faire face[204].

Or, le recours à l'argument juridique, ou à la menace du législateur, paraît bel et bien efficace pour mobiliser des personnes et des ressources sur des thématiques de protection de la vie privée, et même pour fournir une base de discussion en vue d'aboutir à un consensus. Les lignes directrices de l'OCDE de 1980 ont notamment été évoquées par un enquêté comme ayant fourni une base de discussion capable de mettre d'accord des acteurs des deux bords de l'Atlantique[205], et le RGPD avait donné une nouvelle impulsion aux discussions[206]. Rigo Wenning abonda dans ce sens :

> « Tout a radicalement changé. Parce que maintenant... auparavant, quand la CNIL, parce que Google avait réuni tous ses comptes sur un seul compte, la CNIL était contre, Google a dit : je m'en fous. Et puis la CNIL a sorti sa sanction maximale, qui était de 150 000 euros, et puis Google a souri une toute petite seconde de débourser le prix d'un timbre, et puis aujourd'hui, donc à partir du 25 mai, il refont l'expérience, ça va leur coûter 4 milliards. » (Entretien avec Rigo Wenning)

Il est aussi revenu sur le rôle de la FTC et de la pression législative dans la mobilisation d'acteurs de l'industrie pour lancer le projet P3P, et sur le coup d'arrêt que l'élection de George W. Bush, qui fit retomber la pression législative, constitua pour le projet :

> « Politiquement, le jeu pour les Américains, c'était que y avait une proposition de loi sur la vie privée et que toute l'industrie a besoin en fait de la *self-regulation* ; on va faire du P3P, vous allez voir, c'est beaucoup mieux qu'une loi […]. À un moment donné ça a changé un peu de politique […] aux États-Unis, et donc le projet de loi a été abandonné, et au moment où ça a été abandonné, tout le monde quittait le groupe de travail. Parce que ce n'était plus la peine » (Entretien avec Rigo Wenning)

Vincent Toubiana comme Sid Stamm ont insisté sur le rôle de la pression du législateur et de régulateurs comme la FTC aux États-Unis, pour convaincre notamment des acteurs de l'industrie publicitaire en ligne à soutenir le projet *Do Not Track* :

204 Cf. section 5.6.5.
205 Entretien W3C1
206 Entretien W3C1

« Ils voyaient pas l'intérêt de faire quelque chose de privacy friendly s'il y avait pas une régulation pour faire du privacy friendly […] Sans régulation y a pas moyen de pousser les bonnes pratiques. » (Entretien avec Vincent Toubiana)

« Depuis le départ, l'industrie publicitaire, au moins aux États-Unis, voulait être autour de la table. […] Et la raison était que la *Federal Trade Commission* soutenait plus ou moins le travail du W3C pour standardiser cette idée de Do Not Track. Et cela suggérait à l'industrie, qui est en très grande partie auto-régulée : « travaillez avec ces technologues, décidez ensemble de ce que vous allez faire, ou bien nous déciderons à votre place ». C'est un très bon exemple, vous savez, de pression législative[207]. » (Entretien avec Sid Stamm)

Notons enfin que plusieurs personnes travaillant ou ayant travaillé dans des autorités de protection des données participent aux travaux du PING et du TPWG, comme Vincent Toubiana, Rob van Eijk, Simon Rice ou encore Tara Whalen. Ils ne sont que rarement intervenus pour imposer quelque chose en utilisant leur position d'autorité, mais ce qu'ils disent a toujours eu un poids certain dans la discussion. Certaines entreprises membres du W3C, et certains participants, sont aussi responsables de traitements, et ont intérêt à investir dans des standards dont la mise en œuvre n'augmente pas leurs coûts de mise en conformité avec la loi, ou, pire, risque de leur fermer des marchés.

Ainsi, contrairement aux apparences, aux préjugés, ou même à ce qui peut être dit ou perçu par les personnes qui participent aux travaux du W3C, le droit est loin d'être absent des discussions au W3C. Il est même très présent dans les discussions du TPWG, où il peut être mobilisé comme argument pour peser sur l'issue des discussions et modifier les textes sur lesquels travaille le groupe.

Lorsque les conditions politiques externes au W3C sont réunies, la pression du législateur ou du régulateur se fait sentir. Si les publicitaires et les éditeurs en ligne participent au TPWG, c'est sous la pression de la FTC et d'appels de certains parlementaires à légiférer. C'est aussi parce qu'il existe en Europe une réglementation spécifique sur la vie privée dans les communications électroniques, la directive 2002/58/CE dite « e-Privacy », qui impose le recueil du consentement pour placer certaines données, tels que certains cookies, permettant de tracer les utilisateurs. En avril 2018, la charte du groupe TPWG a même été prolongée pour laisser au groupe le temps de tenir compte du résultat des débats relatifs aux législations de l'UE sur la proposition de

207 Traduit de l'anglais. Texte original : « From the beginning, the advertising industry, at least in the United States, was very keen to be at the table. […] And the reason was because the Federal Trade Commission had more or less endorsed the W3C's efforts to standardise this Do Not Track thing. And that suggested to the industry that is actually currently self-regulated for the most part: get in the room with these technologists, and decide with them what you're gonna do, or we're gonna decide for you. It was legislative pressure, you know, at its best. »

règlement e-Privacy[208] qui doit remplacer la directive 2002/58/CE actuellement en vigueur (*public-tracking*, e-mail de Xueyuan du 10 avril 2018). En effet, cette proposition contient des dispositions à ses articles 9 et 10 qui décrivent des mécanismes très similaires au projet de DNT. Finalement, la perspective d'une adoption rapide de cette proposition de règlement s'éloignant, la pression est retombée et le TPWG a officiellement été fermé début 2019 (e-mail de Xueyuan du 17 janvier 2019). Nous pouvons faire l'hypothèse qu'une relance sérieuse des négociations sur le projet de règlement e-Privacy pourra être un argument mobilisé par des personnes souhaitant rouvrir les discussions sur le *Do Not Track*.

Ceci étant dit, au W3C, toutes les lois ne se valent pas. Bien que nous n'ayons pas lu de façon exhaustive toutes les discussions sur IRC ou sur les *mailing-lists* du W3C, nous pouvons dire que dans aucun des nombreux e-mails que nous avons lus, il n'y était fait référence à des normes de droit positif en vigueur ailleurs qu'aux États-Unis, au Canada, ou en Europe. Malgré la participation de Japonais, de Russes et de Chinois au PING et au TPWG, nous n'avons pas trouvé de références au droit de ces pays.

5.6.5. À la recherche des contre-arguments

Jusqu'ici, nous avons essentiellement présenté des arguments utilisés par des acteurs du PING ou du TPWG pour appuyer une demande de renforcement de la protection de la vie privée dans la conception de standards du Web au W3C. Nous avons bien vu quelques cas de discours qui visaient à négocier à la baisse le contenu des mesures de protection, par exemple dans l'exemple ou Chris Pedigo, de l'OPA, a mobilisé la théorie contextuelle de la vie privée pour obtenir que les « *first parties* » ne soient pas soumis à des obligations spécifiques lorsqu'ils reçoivent un signal DNT:1[209]. Dans un autre cas, nous avons vu Shane Wiley contrer par d'autres arguments juridiques ceux avancés par Ninja Marnau en faveur de l'imposition d'obligations aux « *first parties* » dans les projets de spécifications de DNT[210]. Mais même ces deux exemples ne sont pas des exemples d'arguments de fond contre le droit *à la* vie privée et sa prise en compte dans la rédaction de standards du Web.

Les personnes interrogées dans la campagne d'entretien ont toutes répondu qu'ils n'avaient jamais rencontré de personne au W3C disant ouvertement être contre le droit *à la* vie privée. Il est difficile de trouver dans *public-privacy* des messages argumentant contre une plus grande prise en compte de la protection de la vie privée dans les standards produits par le W3C.

208 Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques») (procédure : 2017/0003(COD))

209 Cf. sections 5.5.4. et 5.6.2.

210 Cf. section 5.6.4.

Cela ne devrait pas nous étonner : le PING regroupe en effet au sein du W3C des personnes qui, volontairement et souvent bénévolement, investissaient du temps et de l'énergie en faveur de cette cause[211]. Cela est un peu moins vrai dans le cas du TPWG, et nous y trouvons d'ailleurs des personnes qui mobilisent des arguments pour éviter un standard DNT qu'ils trouvent trop contraignant[212]. Mais en définitive, la seule façon de réellement observer les contre-arguments à la vie privée qui circulent au sein du W3C en prenant le PING comme poste d'observation principal a été d'observer des discussions sur *public-privacy* au sujet de ces contre-arguments, et d'interroger les participants sur les arguments qu'ils doivent contrer.

En faisant ce travail, nous pouvons assez vite constater qu'en réalité tout le monde, au W3C, n'est pas d'accord sur le degré d'importance, de priorité, à accorder à la protection de la vie privée. Un contre-argument que les enquêtés du PING ont évoqué est celui qui consiste à dire que la protection de la vie privée des internautes serait une « cause perdue » ; et si c'est une cause perdue, si l'ère chevaleresque de la vie privée est derrière nous, alors pourquoi perdre du temps à lutter comme Don Quichotte contre des moulins ?

Cet argument de la cause perdue n'est pas nécessairement un argument techno-utopiste, transhumaniste, ou inspiré par la philosophie du *Quantified Self*[213]. Il se fonde néanmoins sur l'idée, exprimée par Vint Cerf lors d'une audition devant la FTC (Cerf, 2013), que la vie privée, bonne ou mauvaise, désirable ou indésirable, serait historiquement située, et surtout située dans le passé. Seulement, puisqu'on ne pourrait lutter contre le « progrès » (de la technologie), alors pourquoi ne pas plutôt dépenser son énergie à créer de nouveaux outils et services qui plairont aux utilisateurs ? Services qui peuvent être ou ne pas être inspirés par des philosophies comme le transhumanisme ou le *Quantified Self*, mais là n'est tout compte fait pas là question.

Un des enquêtés, en réponse à une question demandant s'il avait entendu des arguments contre le droit *à la* vie privée circuler au sein du W3C, répondit :

> « Je pense qu'il existe […] parfois un état d'esprit où : ah ouais, la privée c'est sans importance, ou, parfois, quand on leur parle de *fingerprinting*, ils nous répondent : oui, mais c'est peut-être **juste une cause perdue** [*lost cause*], c'est trop tard, le *fingerprinting* est déjà bien établi et ce n'est pas la peine de modifier notre fonctionnalité extraordinaire pour régler ce problème de vie privée[214]. » (Entretien W3C5)

211 Cf. section 5.4.4.
212 Cf. section 5.5.4.
213 Cf. section 2.4.1.
214 Traduit de l'anglais. Texte original : « I think that there is […] sometimes a mindset of: oh yeah, privacy is irrelevant, or, sometimes we talk to them about fingerprinting, and they answer: yeah maybe **it's just a lost cause**, maybe that's just too late, fingerprinting has kind of been around, and we should not have to change our awesome feature to address this privacy issue. »

En cherchant dans l'archive de la liste de discussion *public-privacy* les termes « lost cause », nous pouvons trouver une série d'e-mails ayant pour titre « Séance de groupe TPAC – Est-ce que le *fingerprinting* du *user agent* est une cause perdue[215] ? ». Le premier e-mail du fil de discussion, envoyé le 21 octobre 2012 par Christine Runnegar, coprésidente du PING, annonçait que le 18 du même mois, Brad Hill, de PayPal, avait soumis une proposition de session pour le TPAC de 2012 intitulé « *Is user fingerprinting a lost cause?* ». Le sens de cette proposition n'était pas de convaincre que la lutte contre le fingerprinting était une cause perdue, mais de susciter un débat lors du rendez-vous annuel du W3C pour, au contraire, donner à des orateurs du PING ou d'ailleurs l'occasion de contrer cette idée.

L'e-mail de Christine Runnegar a suscité de nombreuses réactions dans les quatre jours qui ont suivi. L'e-mail ci-dessous, de David Singer, de la compagnie Apple, montre par exemple une discussion avec Mike O'Neill, de la compagnie Baycloud, où ils ont débattu de la meilleure façon de répondre à l'argument de la cause perdue :

> « > David,
> >
> > Je suppose que cela aurait dû être : « tenter de mettre fin au *fingerprinting* de l'agent
> > utilisateur est-il une cause perdue ? ».
>
> Merci. C'est une question plus facile. Nous vivons dans un monde sordide [*ugly world*] de mesures et contre-mesures. J'imagine, si les scripts font partie de l'équation, qu'il faut également poser la question des empreintes utilisateur (*user finger-print*) (par exemple : la saisie, ou les schémas de clics d'utilisateurs propres à chaque individu, etc.).
>
> >
> > Je suis d'accord avec ce que tu dis au sujet du DNT, mais je pense que les navigateurs
> > pourraient jouer un rôle plus autoritaire, et aider à mettre en œuvre ce que les
> > utilisateurs souhaitent en termes de vie privée. Si les utilisateurs spécifient une
> > préférence en termes de DNT, pourquoi ne pas mettre en place des fonctionnalités qui
> > empêchent la prise d'empreintes digitales numériques, qui bloquent les cookies de 3e
> > partie [*third party cookies*], etc. Cela ne serait pas un jeu sans fin de coup rendu pour
> > coup rendu (*endless quid pro quo*) parce que cela deviendrait rapidement peu
> > économique pour les mauvais acteurs de persévérer.
>
> Oui, la question qui revient toujours est celle de savoir ce que l'on fait des sites qui ne mettent pas en œuvre le DNT ou ne sont pas en conformité. **L'Internet ne sera plus jamais un endroit où la confiance est la norme. Cependant, la situation actuelle peut très certainement être améliorée : il n'existe aucune raison de continuer sur la lancée actuelle** où des personnes honnêtes et respectables, et des entreprises honnêtes et respectables, sont hostiles ou méfiantes les unes envers les autres. Réduire le problème

215 Traduction de l'auteur. Les termes techniques qui n'ont pas d'équivalent en français ne sont pas traduits. Texte original : « TPAC breakout session – Is user agent Fingerprinting a lost cause? »

aux « acteurs malveillants » de chaque côté serait un progrès considérable[216]. » (*public-privacy*, e-mail de David Singer du 24 octobre 2012)

L'extrait ci-dessus permet au passage d'illustrer encore le rôle de l'argument de la confiance, dont il était question dans en section 5.6.3, dans la stratégie argumentative des défenseurs de la vie privée du W3C.

Le compte-rendu détaillé des discussions nous montre que la session organisée au TPAC de 2012, dont il est question dans ce courriel, n'a finalement pas été un réel débat contradictoire, les participants ayant dans l'ensemble été des personnes déjà convaincues par la nécessité de s'attaquer au fingerprinting, que cela soit, d'ailleurs, une cause perdue ou non. Des questions ont été posées pour savoir si quelqu'un voulait prendre la parole et expliquer pourquoi la vie privée, ou la lutte contre le fingerprinting, serait une cause perdue. L'utilisateur « dom » demanda à ce que les « *non-privacy advocates* » prennent la parole, mais en vain. Toutefois, il ressort du compte-rendu de la discussion que la présence d'acteurs dans des groupes du W3C qui affirment que cette lutte est futile faisait consensus parmi les personnes présentes à cette réunion du TPAC de 2012 (W3C, 2012).

Nous n'avons pas retrouvé dans les e-mails de la discussion sur la définition du « *tracking* » cet argument de la cause perdue.

En cherchant dans les archives de toutes les *mailing-lists* du W3C, nous avons fini par trouver des occurrences du terme de recherche « *lost cause* » dans *www-tag*, la liste de discussion publique du TAG. Mark Nottingham avait envoyé un e-mail le 22 mai 2015 pour demander des retours sur un document de travail, hébergé sur Github, « *TAG Feedback on Fingerprinting Guidance for Web Authors [Draft]* ». Ce dernier, daté du 25 février 2015, commence par la

---

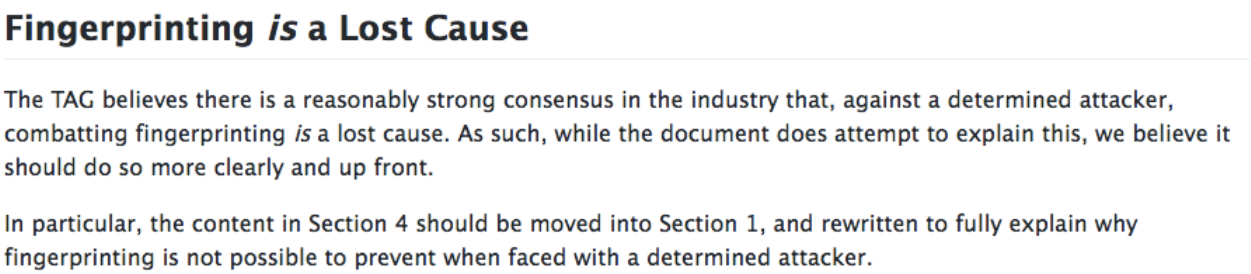
216 Traduit de l'anglais. Texte original : « > David,
>
> I assume it should have been is "is trying to stop user-agent fingerprinting
> a lost cause?".

Thanks. That is a more addressable question. It's certainly a measure-counter-measure world, and ugly. I assume, if scripts fit into the equation, we should also ask about user finger-printing (e.g. typing and pointer usage patterns unique to individuals, and so on).

>
> I agree what you say about DNT, but I think browsers could take a more
> authoritarian role, and help ensure what users want in terms of privacy. If
> users specify a DNT preference why not enable features that inhibit
> fingerprinting, block 3rd party cookies etc. It would not be an endless quid
> pro quo because it would quickly become uneconomic for most of the bad
> actors to continue.

Yes, there is always the question of what you do with sites that don't implement DNT or are non-conformant, agreed. **The internet will never again be a place where trust is the norm. On the other hand, we can surely improve on the situation today: there is no underlying reason to continue with today's situation** where honest, respectable people and honest, respectable businesses behave with hostility or distrust to each other. Reducing the problem to 'bad actors' on both sides would be a huge improvement. »
Texte mis en gras par l'auteur.

phrase « Fingerprinting *is* a Lost Cause » (« le *fingerprinting* est une cause perdue ») en grands caractères gras, le verbe être (« *is* ») étant en italique pour marquer une insistance :



Fingerprinting *is* a Lost Cause

The TAG believes there is a reasonably strong consensus in the industry that, against a determined attacker, combatting fingerprinting *is* a lost cause. As such, while the document does attempt to explain this, we believe it should do so more clearly and up front.

In particular, the content in Section 4 should be moved into Section 1, and rewritten to fully explain why fingerprinting is not possible to prevent when faced with a determined attacker.

Figure 42 : *Extrait de capture d'écran de la page https://github.com/w3ctag/design-reviews/blob/master/2015/05/fingerprint.md (consultée le 31 juillet 2018)*

Cet exemple démontre que l'argument selon lequel la vie privée est une cause perdue circule bel et bien, même s'il est difficile d'en retrouver la trace dans des discussions publiques.

Cet argument doit être relié à la question de la capacité à mobiliser des personnes volontaires pour faire le travail de veille, de conseil et d'évaluation d'impact du PING. Il faut parvenir à faire en sorte que les gens s'investissent dans cette cause, alors que le retour sur investissement individuel est perçu comme faible[217]. L'enquêté qui avait, le premier, évoqué ce discours sur la cause perdue, précisait d'ailleurs bien qu'il relevait plus d'un débat sur les priorités de l'investissement des membres et participants du W3C, que d'un débat de fond sur la désirabilité ou la définition de la vie privée ou du droit *à la* vie privée :

> « Je ne suis pas sûr si cela correspond à des avis divergents sur la vie privée ou à des priorités différentes à ce sujet[218]. »(Entretien W3C5)

Existe-t-il alors un autre contre-argument aux efforts des membres du PING, ou au droit *à la* vie privée, qui circule au sein des arènes du W3C ?

Un autre contre-argument parfois évoqué est celui qui consiste à défendre un projet qui pourrait créer un risque en matière de protection de la vie privée, en insistant sur son apport bénéfique à l'utilisateur :

> « Je pense que nous entendons souvent la perspective selon laquelle certaines pratiques de collecte de données sont bonnes pour l'utilisateur […]. Certaines personnes pensent : oh c'est mieux pour l'utilisateur parce que cela permet à davantage de données d'être collectées afin de fournir ensuite de meilleurs services. À l'inverse, d'autres personnes pensent : non ce n'est pas mieux pour l'utilisateur car toute donnée supplémentaire

217 Entretien W3C10.

218 Traduction de l'auteur. Texte original : « I'm not sure if it corresponds to different views on privacy or if it just corresponds to different priorities about it. »

collectée sur lui peut être utilisée contre lui[219]. » (Entretien W3C5)

Cet argument est le plus proche, dans notre corpus sur le W3C, de l'argument de la coalition industrielle des négociations sur le RGPD en faveur d'un « équilibre » entre droit *à la* vie privée et compétitivité économique fondée sur l'innovation ; ici, il s'agit d'un équilibre à trouver entre le désir éprouvé par la figure de l'utilisateur[220] de plus de « vie privée », opposé au désir de cette même personne réelle ou supposée de toujours plus d'innovation. Il a notamment été mobilisé dans des discussions au sein du TPWG par des acteurs issus de l'industrie de la publicité, pour qui la publicité ciblée est un bien pour l'internaute, car elle permet de ne pas lui faire perdre de temps avec des réclames sans aucun rapport avec ses goûts ou ses envies, tout en finançant le modèle économique fondé sur la *dataveillance* du Web 2.0[221].

Il partage toutefois avec l'argument du contrôle de l'internaute sur ses données une caractéristique : l'un comme l'autre se présentent comme l'expression d'un souci du bien-être de l'utilisateur en tant qu'individu doté du droit de voir ses préférences respectées. Cette conception est facilement compatible avec l'approche individualiste du paradigme libéral de la vie privée. Les « *privacy advocates* » peuvent alors tenter de démontrer à leur interlocuteur que la fonctionnalité qu'ils veulent mettre en œuvre est en réalité dangereuse, indésirable pour l'utilisateur, et que ce dernier ne la souhaite en fait pas, surtout si elle met sa vie privée en danger.

Un dernier contre-argument, qui nous a été rapporté en entretien, pourrait être résumé en une question : où est le mal (« *where is the harm* ») ? Vincent Toubiana a ainsi raconté en entretien la façon dont cet argument avait été mobilisé au sein du TPWG par les adversaires d'un DNT strict :

> « Pas la collecte de données. Ça a été vraiment pendant très très longtemps, eux ont défini ce point-là comme étant, voilà : le tracking c'était l'affichage de publicité ciblée, et si y a pas d'affichage de publicité ciblée, il peut pas y avoir de préjudice. […] Parce que la société qui collecte les données a priori elle est sûre, y a pas de problème de confiance. Le seul préjudice qu'il peut y avoir, c'est si y a de la publicité ciblée qui a été mal amenée à une personne, et que ça peut révéler à son entourage les sites qu'elle a précédemment visité, là effectivement il y a un problème de vie privée. » (Entretien avec Vincent Toubiana)

Dans la discussion sur la définition du terme « *tracking* », plusieurs e-mails[222] évoquent la question du préjudice subi (ou non) par un internaute en raison de tel ou tel comportement de « tracking ». Le thème est en réalité très rarement mobilisé ouvertement pour restreindre la portée de la norme DNT. Nous le retrouvons tout de même dans un e-mail de Chris Pedigo de l'OPA du

219 Traduit de l'anglais. Texte original : « I think we often hear the perspective of some sorts of data collection practices are good for the user […]. Some people think: oh it's better for the user because it allows for more data to be collected to provide better services, versus other people saying: no it's not better for the user because all that extra data that is collected can be used in ways against them. »

220 Cf. section 5.6.1.

221 Entretien W3C5 et e-mail de Chris Pedigo du 30 novembre 2011 sur *public-tracking.*

222 Par exemple : e-mails de Sean Harvey du 24 octobre 2011, de David Wainberg du 25 octobre 2011, de Kevin Smith du 9 décembre 2011, de Rob van Eijk du 5 septembre 2012 sur la liste de discussion *public-tracking.*

30 novembre 2011 sur *public-tracking*, où celui-ci dit s'interroger sur le mal qu'il y aurait pour un site web de connaître les comportements de ses visiteurs. Après tout, poursuit-il, un épicier ne connaît-il pas les habitudes de consommation de ses chalands ? Cette question du préjudice est ici, dans son discours, reliée à celle de contexte ; c'est la sortie d'une information de son contexte légitime qui la rend dangereuse. Là où il y aurait donc « *harm* » (« préjudice »), ce n'est que lorsque l'épicier va suivre son client chez lui pour voir ce qu'il y fait, ou demander aux autres commerçants ce qu'il a acheté. Il concluait alors logiquement :

> « Ainsi, l'OPA soutient fermement une exemption pour le recueil de données d'un consommateur avec lequel l'entreprise interagit directement à des fins de marketing visant ce consommateur, dans un but de fonctionnement général et de personnalisation du site[223]. » (*public-tracking*, Chris Pedigo, e-mail du 30 novembre 2011)

Ainsi, notre corpus, complété par des entretiens, nous a permis de trouver des arguments utilisés par des acteurs du W3C pour minimiser l'importance d'y accorder du temps et de l'énergie, par exemple parce que ce serait une « cause perdue ». D'autres arguments, comme ceux développés dans le dernier exemple cité, qui pose la question de la réalité du préjudice subi par les internautes pistés, ont été mobilisés à l'appui d'une proposition de définition de la notion de « *tracking* » plus permissive que celle que certains défenseurs de la vie privée auraient envisagée.

Mais alors que nous nous serions attendu à trouver des arguments d'inspiration néolibérale, ou techno-utopiste voire transhumaniste, à l'encontre même de l'idée que le droit *à la* vie privée et/ou *à la* protection des données à caractère personnel serait désirable, nous n'en avons pas trouvé pendant notre enquête de terrain sur le W3C en prenant le PING comme point d'observation.

Les contre-arguments opposés à la stratégie argumentative des défenseurs de la vie privée du PING ou œuvrant au sein du TPWG ont réussi à remettre en cause une partie de leurs revendications. Le projet *Do Not Track* est même, à l'heure actuelle, resté lettre morte, même si une reprise des négociations sur le règlement e-Privacy dans l'UE pourrait le relancer. D'autres projets ont toutefois réussi. Nous avions vu que la recommandation sur la géolocalisation (W3C Geolocation API) contient, à la demande des défenseurs de la vie privée, des dispositions sur la protection de la vie privée. Depuis la fin de notre enquête de terrain, le TAG, qui coordonne les travaux de standardisation des groupes de travail du W3C, et qui dispose d'un poids certain, a modifié son questionnaire sur la sécurité et la vie privée pour y indiquer qu'y répondre était obligatoire pour tout projet désirant obtenir le statut de recommandation officielle (W3C TAG Security and Privacy 2019). Enfin, nous avons aussi déjà vu que la « vie privée » était devenu un

223 Traduit de l'anglais. Texte original : « Accordingly, OPA strongly supports an exemption for the collection of data from a consumer with whom the company interacts directly for the purposes of marketing to that consumer and for the general operation and personalization of the site. »

thème de discussion solidement ancré au W3C depuis la fin des années 2000, et pas uniquement dans des groupes dédiés à cette question[224].

Au demeurant, quel que soit le constat d'échec ou de réussite que nous pouvons faire des efforts des défenseurs de la vie privée du W3C, l'étude que nous avons menée depuis le PING et le TPWG nous permet de tirer un certain nombre de conclusions sur les conceptions de la « vie privée » mobilisée par les acteurs qui ont rédigé les documents de ces groupes et sur leurs stratégies argumentatives, qui à leur tour nous permettent d'avancer dans la réponse à notre question de recherche et dans le test de nos hypothèses.

5.7. Conclusion du chapitre

Nous venons de voir que plusieurs groupes de travail (*working groups* et *interest groups*) ont œuvré, au sein du W3C, à faire en sorte que les standards adoptés par cet organisme, qui sont une part de la *Lex Informatica* identifiée par Joël Reidenberg (1997), soient les plus protecteurs possibles de la « vie privée » (« *privacy* »). Entre 2011 et tout début 2019, deux groupes ayant pour but d'intégrer des mécanismes de protection de la « vie privée » dans les standards du Web ont coexisté au sein du W3C : le TPWG et le PING.

Ces groupes correspondent à deux façons d'aborder la protection de la vie privée et la protection des données à caractère personnel. Le TPWG développait un standard techno-politique qui se veut un outil d'action publique (*techno-policy standard* au sens de Nick Doty et Deirdre Mulligan (Doty et Mulligan, 2013)), tandis que le PING joue un rôle de conseil, de partage d'expertise, et d'évaluation d'impact des recommandations produites par d'autres groupes du W3C.

Identifier les controverses autour de la production normative de ces groupes est rendu difficile par certaines contraintes qui encadrent leur fonctionnement. En effet, comme toute expression de dissensus risque de mettre en péril l'intégralité des travaux d'un groupe, celle-ci est très fortement dissuadée. En effet, nous avons vu[225] que c'est le consensus entre membres d'un groupe de travail, formulé dans des termes qui se veulent et qui sont perçus comme « techniques », qui confère sa légitimité aux textes performatifs des recommandations du W3C.

224 Cf. figure 29.
225 Cf. section 5.5.2.

La compréhension de ces caractéristiques très particulières des arènes de standardisation dans la gouvernance d'Internet permet de se rendre compte que ce n'est pas parce que les controverses publiques et apparentes sont exceptionnelles qu'il n'y a pas de dissensus et de rivalités tant sur le plan axiologique qu'en matière d'intérêts (eux-mêmes construits à travers des filtres cognitifs), qui structurent des formes de controverses implicites.

Ce constat permet d'éclairer l'apparente absence de débat sur la définition de la vie privée, ou du droit *à la* vie privée au sein du PING et du TPWG. Selon les participants interrogés, un tel débat, qui n'est pas perçu comme opérationnel, ferait perdre du temps, et surtout, il mettrait en péril l'unité du groupe et fragiliserait le consensus. Les travaux universitaires de certains participants à cette arène, comme Nick Doty, qui affirment que le concept de « *privacy* » est « essentiellement contesté » (Mulligan, Koopman et Doty, 2016) fournissent une justification théorique au refus de définition. Quant au débat qui, sur la liste de discussion *public-tracking* du TPWG, a retardé de plusieurs années le consensus pour l'adoption des projets de recommandation du standard *Do Not Track*, il est présenté comme l'exemple même de pourquoi il ne faut pas se lancer dans un débat sur la définition du terme « *privacy* ».

Cette « vie privée » est, pour les défenseurs de la vie privée du W3C, une caractéristique d'un système technique (comme le Web) qui doit offrir à l'internaute la maîtrise de ses données (« *user control* »). Cette maîtrise passe par la médiation de logiciels, généralement les navigateurs web, désignés par le terme de « *user agent* » et qui doivent outiller son agencéité.

Cette formule de « *user control* » était aussi utilisée pour définir de façon opérationnelle la « *privacy* ». La « vie privée » est alors présentée comme une modalité par laquelle une personne peut décider du contrôle de l'accès à soi et aux informations qui la concernent. En d'autres termes, il s'agit, mais avec d'autres mots, du « droit à l'auto-détermination informationnelle » défendu par les défenseurs de la vie privée du Conseil de l'Europe, de l'OCDE et des « discussions » sur le RGPD.

Nous pouvons donc conclure que conformément à notre troisième hypothèse, les mécanismes de contrôle ou d'auto-détermination des internautes proposés et discutés au W3C ont bien pour but de garantir un maintien de l'efficacité de la protection de la « *privacy* », ou « vie privée ». Les dispositions protégeant l'« *user control* » servent ainsi à prescrire le développement de logiciels qui doivent outiller l'internaute pour lui permettre de gérer le risque informationnel d'éclatement des cloisons contextuelles contraignant la circulation de ses données personnelles.

Ces mécanismes de contrôle, à l'instar *Do Not Track*, revêtent aux dires des défenseurs de la vie privée une deuxième fonction : assurer la *confiance* de l'utilisateur dans le système technique du Web et des marchés qui font de la vente de biens ou services en ligne. Comme la

coalition de la « *privacy community* » au Conseil de l'Europe, à l'OCDE puis au cours du processus d'adoption du RGPD, les défenseurs de la vie privée du W3C ont donc mobilisé l'argument de la confiance de façon stratégique pour faire accepter leurs revendications au-delà des frontières de leur coalition de cause.

Les références fréquentes à la théorie de la vie privée contextuelle d'Helen Nissembaum, qui critique la théorie libérale de la vie privée et notamment la centralité qui y est faite de l'idée d'un possible consentement des individus[226], pourrait nous amener à entrevoir la possibilité d'une remise en cause, au sein du W3C, du caractère paradigmatique de cette théorie au moins dans cet organisme. De fait, elle a en effet permis aux acteurs de l'industrie de la publicité de très nettement diminuer le niveau d'exigence du projet *Do Not Track* par rapport à ce qu'auraient voulu les défenseurs de la vie privée du W3C, en supprimant la possibilité pour un utilisateur d'employer ce mécanisme pour consentir (ou refuser de consentir) à la collecte et à la rétention de données par un *first-party*, c'est-à-dire par le site dont il a lui-même requêté l'adresse directement dans son navigateur. Malgré tout, cette stratégie argumentative n'a pas remis en cause l'idée fondamentale du *Do Not Track*, qui était de fournir un outil de *consentement* aux internautes en tant qu'*individus* en droit d'exprimer leurs propres préférences, et de voir ces dernières respectées, là où Helen Nissenbaum se montre critique à l'égard de la possibilité pour un individu de consentir de façon libre et éclairée au traitement de ses données à caractère personnel. L'idée de consentement est restée au cœur du projet.

La façon dont la théorie contextuelle de la vie privée a en effet été mobilisée par les défenseurs de la vie privée fait qu'elle en a assez largement perdu son potentiel de remise en cause des fondements du paradigme libéral de la vie privée, et donc sa place paradigmatique. En effet, la solution qu'ils ont proposé pour faire en sorte que l'intégrité des contextes dans lesquels les internautes acceptent de révéler des informations sur eux soit respectée, a justement été de fournir à ces derniers du « contrôle utilisateur » (« *user control* »), donc une possibilité rendue effective par des moyens techniques inscrits dans l'architecture même du Web de consentir ou de refuser le partage d'information. Les concepts issus de la théorie d'Helen Nissembaum se retrouvent ainsi réinterprétés d'une façon qui les rend conformes au paradigme libéral de la vie privée.

Par ailleurs, convaincre les autres de la désirabilité ou du bien fondé du droit *à la* vie privée, ou d'adopter telle ou telle conception de la « vie privée », ne semble pas être le principal défi à relever pour les défenseurs de la vie privée du W3C. Leur priorité, selon ce qu'il ressort des entretiens, est de convaincre de nouveaux acteurs d'investir des ressources pour participer aux travaux, notamment d'évaluation d'impact. La participation au PING est en effet volontaire, et dans bien des cas, bénévole. Les membres du PING doivent composer avec l'argument selon lequel la protection de la vie privée est une cause perdue. Or, à quoi bon s'engager pour une

226 Cf. section 2.3.5.

cause perdue ? Parmi les arguments mobilisés pour y répondre, outre la nécessité de garantir la confiance des internautes, le rappel de la Loi, et en particulier du droit européen de la protection des données à caractère personnel, était beaucoup plus fréquemment employé que nous ne nous y serions attendus.

En effet, la perception de sens commun, mais aussi celle exprimée par plusieurs enquêtés lors de campagne d'entretiens, décrit des arènes de standardisation d'Internet, dont le W3C, comme totalement déconnectées du droit dur, et agissant en marge de l'État, sans aucun égard à son action. Cette autonomie est d'ailleurs revendiquée par des documents comme le Tao de l'IETF (Hoffman, 2012), la déclaration d'indépendance du cyberespace (Barlow, 1996). L'IETF, qui a inspiré le W3C, s'est construit en opposition à une perception d'ingérence étatique dans une gouvernance d'Internet qui souhaite s'en émanciper (Russell, 2006). Or il y a certes une différence culturelle entre les arènes politiques de nature étatique (ou intergouvernementale ou supranationale) et les arènes de standardisation technique qui relèvent de la gouvernance d'Internet (Kleinwächter, 2012), mais il ressort de données de corpus et d'entretiens qu'il ne faut pas exagérer la césure entre le W3C et la sphère étatique ou le droit. En réalité, des arguments juridiques sont régulièrement mobilisés, à la fois pour légitimer un amendement proposé à un texte de recommandation, et pour convaincre des acteurs d'investir du temps et de l'argent pour travailler à l'amélioration de la prise en compte de la protection de la vie privée dans les standard du Web. Certains régulateurs, comme la FTC et les autorités européennes de protection des données, mais aussi certains législateurs, n'ont pas hésité à chercher à influencer les discussions du W3C. Textes de droit dur et discours juridiques sont donc loin de ne pas avoir d'incidence dans les arènes de standardisation d'Internet en général, et du Web en particulier, même s'il y a de fortes inégalités selon les juridictions sur les droits qui ont ou non de l'influence, puisque seules des sources juridiques états-uniennes, canadiennes et européennes ont été citées et avancées comme argument sur la nécessité de faire quelque chose pour s'y adapter.

Ainsi la différence d'approche initialement postulée dans la première hypothèse entre droit et informatique dans la définition de ce qu'est cette « vie privée » qu'il conviendrait (ou non) de protéger n'est pas corroborée par les observations faites sur les discours circulant au sein du W3C comparés à ceux des terrains exposés dans les deux chapitres précédents, sur l'adoption des Lignes directrices de l'OCDE, de la Convention 108 du Conseil de l'Europe, et le RGPD.

Enfin, puisqu'ils adhèrent au paradigme libéral de la vie privée, et contrairement à ce qu'affirmaient Mascetti et al. (Mascetti et al., 2013), les informaticiens défenseurs de la vie privée du W3C n'opèrent pas de distinction *a priori* et absolues entre des informations qui seraient à protéger car relevant de la « vie privée » et celles qui, moins sensibles, pourraient ne pas faire l'objet de régulation par des standards techno-politiques. C'est bien à l'utilisateur qu'est confiée la mission de contrôler ce qui, pour lui, est privé. En outre, comme nous allons le

démontrer dans le chapitre suivant, les membres du PING ont adopté une définition de la notion de donnée à caractère personnel directement empruntée à la définition juridique européenne.

Chapitre 6 : Focus sur les controverses définitionnelles autour de la notion de « donnée à caractère personnel »

6.1. Introduction : la « donnée à caractère personnel » comme objet de controverses

Après avoir présenté différentes conceptions concurrentes de la « vie privée » en chapitre 2, nous avons vu dans le chapitre 3 le rôle central, parmi elles, du paradigme libéral de la vie privée dans la construction de la « protection des données » comme formule faisant référence à l'action publique liée à un nouveau problème public, autour des années 1970 en Europe. Cette conception libérale est restée paradigmatique lors des négociations sur l'adoption du RGPD entre 2009 et 2016, où coalition industrielle et coalition des défenseurs de la vie privée se sont affrontées pour obtenir un texte avec des mesures concrètes qui reflètent leur propre système de convictions[1]. Enfin, nous venons de voir le rôle d'acteurs inspirés par ce même paradigme libéral de la vie privée dans les groupes qui sont en charge de l'élaboration de standards techniques en matière de « *privacy* » au W3C[2].

Dans ce dernier chapitre, nous allons aborder une controverse définitionnelle juridique dont nous avons pu observer le déploiement sur l'ensemble de nos terrains : celle sur la définition de la « donnée à caractère personnel ». Comme annoncé dans l'introduction générale, nous tiendrons compte dans l'analyse de cette controverse du fait qu'elle n'a pas seulement porté sur le sens général donné à la à la notion, mais bien au texte même de la définition. Chaque mot, chaque signe de ponctuation, peut faire l'objet d'une exégèse porteuse d'enjeux sémantiques et juridiques considérables. En effet, la mécanique de la qualification juridique est un processus intellectuel par lequel une situation réelle pouvant être décrite en langage courant se voit traduite, « qualifiée », en un vocabulaire juridique précis. Son résultat produit des conséquences sur l'interprétation juridique de la situation et le choix des normes de droit applicables. Or, dans ce processus, les professionnels du droit peuvent prendre appui sur chacun des mots contenus dans la disposition juridique à appliquer pour faire valoir leurs arguments (Latour, 2004 ; Magnon, 2008).

1 Cf. chapitre 4.
2 Cf. chapitre 5.

L’une des définitions les plus importantes contenues dans le RGPD est celle de la notion de « donnée à caractère personnel ». En effet, en vertu de son article 2 paragraphe 1, ce règlement ne s’applique – sauf exceptions énumérées au paragraphe suivant – qu’« au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ». Des définitions de la notion de donnée à caractère personnel d’une part, et de la notion de « traitement automatisé en tout ou partie » d’autre part, dépend donc le champ d’application du droit *de la* protection des données à caractère personnel. À titre d’illustration, c’est pour cela que lorsque Google fut mis en cause en 2012 par plusieurs autorités européennes, dont la CNIL française, un des arguments produits en défense par cette société a été que les activités qui lui étaient reprochées n’auraient pas véritablement porté, en droit, sur des choses *qualifiables* de « données à caractère personnel ». Il s’agit d’une affaire où il lui était reproché, entre autres, de collecter à des fins de publicité personnalisée des données à caractère personnel sur des utilisateurs inscrits mais non-authentifiés au moment de leur navigation sur les services de Google et des utilisateurs non inscrits sans leur consentement libre et éclairé. Google, en affirmant ne pas être en mesure d’identifier par leurs noms les personnes concernées par ces traitements, contesta qu’il s’agît de données à caractère personnel, et par conséquent, la compétence de la CNIL de lui infliger une amende en vertu de la loi informatique et libertés française. La CNIL lui répondit en faisant référence au texte de la définition contenue dans la loi informatique et libertés modifiée par une loi de 2004[3] et reprenant la définition à l’article 2 de la directive 95/46/CE, selon laquelle des données sont *qualifiées* de données à caractère personnel dès lors qu’elles permettent d’identifier « directement ou indirectement » des personnes physiques « identifiées ou identifiables »[4].

Pour déterminer si un texte normatif de protection des données à caractère personnel s’applique à une situation, la première étape est donc de déterminer s’il est possible de *qualifier* un objet présent dans la circonstance de fait de « donnée à caractère personnel ». C’est pourquoi, plus que la définition de la notion de « traitement » de données, la définition de la notion de « donnée à caractère personnel » génère une ligne de tension, un point de clivage, autour desquels s’organisent les discours des différentes coalitions de cause qui cherchent à exercer une influence sur le sous-système de politique publique de l’UE de protection des données. En effet, si la vie privée se définit comme l’objet du droit *à la* vie privée[5], les controverses sur la rédaction de la définition de ce qui est protégé par un texte comme le RGPD, qui est censé garantir tant le droit *à la* vie privée que le droit *à la* protection des données à caractère personnel, peuvent alors porter sur le contenu de ce qui relève (ou non) de la « vie privée ».

3 Loi du 6 août 2004 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés (France)

4 Voir la Délibération n° 2013-420 du 3 janvier 2014 de la formation restreinte de la CNIL prononçant une sanction pécuniaire à l’encontre de la société Google Inc.

5 Cf. Introduction générale.

Nous verrons que contrairement à ce que suggère la troisième hypothèse, la définition de la « donnée à caractère personnel » adoptée dans les documents normatifs produits dans nos terrains marque une rupture nette avec la conception d'une « vie privée » définie comme espace – physique et informationnel – qui doit être tenu à l'écart du regard du public. En ce sens, les données à caractère personnel peuvent se concevoir comme étant l'objet de la protection du droit *à la* protection des données à caractère personnel, catégorie distincte du droit *à la* vie privée dans la Charte des droits fondamentaux de l'Union européenne. Pourtant, si nous adoptons, comme dans le paradigme libéral, le point de vue selon lequel la « vie privée » est un droit au contrôle de l'accès à soi, ou encore un droit à l'auto-détermination informationnelle, alors la définition de la notion de donnée à caractère personnel du droit *de la* protection des données s'inscrit bien dans le prolongement du droit *à la* vie privée.

Enfin, nous avons vu dans l'exposé de notre première hypothèse[6] que l'une des façons dont il est dit que droit et informatique diffèrent dans leurs approches de la protection des données à caractère personnel, serait dans l'usage d'acceptions divergentes de la notion de « donnée à caractère personnel ». Étudier les controverses définitionnelles autour de cette dernière, dans deux terrains dominés par des acteurs socialisés au droit puis dans un troisième où les acteurs socialisés à l'informatique sont majoritaires est donc aussi une façon de tester cette hypothèse de départ.

6.2. L'invention de la notion juridique de « donnée à caractère personnel »

La première loi de protection des données, adoptée par le Land de Hesse en 1970[7], ne comportait pas de définition de la notion de « donnée à caractère personnel ». La première définition dans un texte juridique définitivement adopté se trouve dans la loi suédoise de 1973 sur les données[8], qui définissait une « *personuppgift* » (donnée personnelle) comme une « information relative à une personne unique[9] ». Elle revêt déjà un caractère personnaliste et individualiste qui en fait l'une des traductions dans une mesure concrète du paradigme libéral de la vie privée, aux côtés des notions de consentement et d'auto-détermination informationnelle. La définition contenue actuellement dans le RGPD étend cette définition et la précise, mais ne l'a pas remise en cause.

6 Cf. l'exposition des hypothèses dans l'introduction générale.
7 Hessische Datenschutzgesetz, 7 octobre 1970 (GVBl. I S. 625) (Hesse).
8 Datalag (1973:289) (Suède).
9 Texte en suédois : « upplysning som avser enskild person ».

Selon Spiros Simitis, dont nous avons évoqué dans le chapitre 3 le rôle dans l'invention de la « protection des données », l'association des mots « donnée » et « personnelle » s'est d'abord répandue parmi les utilisateurs de ces données :

> « C'est vrai, mais dans le sens où, bien sûr, lorsque les discussions sur l'automatisation ont commencé, ils utilisaient dans ces discussion les mots « donnée personnelle » (*"personal data"*). Et les données personnelles étaient utilisées parce que les données personnelles étaient perçues comme un objet permettant pour ainsi dire de développer certaines politiques publiques, de fonder certaines politiques publiques, pour expliquer pour qui ces politiques publiques seraient pertinentes. Et comme à l'époque il était déjà question de données personnelles, en Allemagne, nous avons créé le mot *Datenschutz*[10]. » (Entretien avec Spiros Simitis)

La formule de « donnée à caractère personnel » remonte ainsi au moins au tout début des années 1970, voire, dans le vocabulaire de certains statisticiens et informaticiens, aux années 1950 et 1960. Notre recherche sur les origines de ce terme s'est toutefois limitée à retrouver l'origine de la notion *juridique* de « donnée à caractère personnel ».

À ce stade, il convient de préciser que le vocable de « donnée nominative » utilisé dans la loi française de 1978 est à comprendre comme la traduction en droit national de la notion de « donnée à caractère personnel » développée au niveau européen. Contrairement à ce que défend Jessica Eynard (2013), n'est pas comme une « notion autonome », puisque – comme elle le rappelle elle-même – ces notions ont la même définition, la même interprétation, et sont comme nous allons le voir la traduction d'un même référentiel : celui du paradigme libéral de la vie privée. Situant notre recherche dans une perspective européenne, qui nous paraît être un échelon plus pertinent que l'échelon national pour l'étude des politiques publiques de protection des données[11], nous n'utiliserons donc pas le terme de « donnée nominative » qui n'est, de toutes façons, que la première traduction en droit français de la notion de « donnée à caractère personnel » importée de la loi suédoise et des travaux du Conseil de l'Europe dans les années 1970.

La définition actuelle de la notion de « donnée à caractère personnel » a pris forme très tôt, dès 1972 et 1973, dans les groupes d'experts de l'OCDE et du Conseil de l'Europe[12].

10 Traduction de l'auteur. Texte original : « It is true, but in the sense that of course, when the discussions on automation from, when automation started, they used in those discussions the words "personal data". And the personal data was used because the personal data was seen as an object permitting so to say to develop certain policies, to base certain policies, to explain for whom those policies would be relevant. And because at the time it was already spoken of personal data, in Germany, the word *Datenschutz* was created. »

11 Cf. sections 1.2.3.1., 1.2.4.2., 3.4. et 4.1.2.

12 Cf. section 3.4.

Quelques discussions à leur sujet ont pu persister, mais le consensus qui avait alors émergé, et qui s'incarnait déjà dans la définition suédoise de 1973, n'a jamais été remis en cause avec succès. Cela est confirmé tant par les participants interrogés dans le cadre de la campagne d'entretiens sur l'histoire du droit *de la* protection des données[13], que par l'étude des documents d'archives collectés sur cette période[14], ainsi que par le tableau de l'évolution textuelle de cette définition à travers les textes juridiques étudiés[15]. Deux éléments essentiels ont été clairement définis dès ces années-là : d'une part, le fait qu'il s'agisse de données relatives à des personnes physiques, et d'autre part, que dès lors qu'un tel lien est établi, le contenu de ces données n'a pas d'incidence sur leur qualification juridique de « données personnelles ».

6.2.1. Des données relatives à des « personnes »

Le fait que la protection des données à caractère personnel concerne les droits fondamentaux de l'*individu* n'a rien d'une évidence, et a fait débat pendant toutes les années 1970 dans les arènes étudiées dans le chapitre sur la généalogie du droit *à la* protection des données à caractère personnel[16]. Pendant longtemps, la protection de la vie privée a été assurée par des dispositions juridiques plus ou moins éparses, qui visaient avant tout à protéger un espace et un groupe. Avec des principes comme l'inviolabilité du domicile, ou encore le secret des correspondances, c'est la vie privée du foyer, de la famille, qui était ainsi protégée. L'article 8 de la CEDH, ou l'article 7 de la Charte des droits fondamentaux de l'UE, annonce aussi protéger le droit *à la* vie privée *et familiale*.

Juridiquement, le terme de « personne » peut désigner à la fois une « personne physique », c'est-à-dire un être humain, soit une « personne morale », c'est-à-dire un groupe qui se voit doté d'une « personnalité juridique » (Castets-Renard, 2018). L'une des premières questions auxquelles les rédacteurs de la définition juridique de la notion de « donnée à caractère personnel » ont dû répondre a été de définir à quel type de « personnes » le syntagme « personnel » faisait référence.

La loi fédérale suisse du 19 juin 1992[17] définit la notion de « donnée à caractère personnel » comme « toutes les informations qui se rapportent à une personne identifiée ou identifiable » (art. 3 sous a)), et la « personne concernée » comme « la personne physique ou

13 Cf. section 1.2.3.3.
14 Cf. section 1.2.3.2. et liste des documents d'archives utilisés en bibliographie.
15 Cf. annexe 2.
16 Cf. chapitre 5.
17 Loi fédérale sur la protection des données du 19 juin 1992, Suisse. Version consolidée au 21 juin 2019.

morale au sujet de laquelle des données sont traitées ». L'article 3 de la loi sur la protection des données en vigueur au Liechtenstein jusqu'en 2018 reprenait la même définition[18].

Cette solution est restée marginale. Elle a d'ailleurs fini par disparaître au Liechtenstein avec l'entrée en vigueur au 1er janvier 2019 d'une nouvelle loi de protection des données reprenant la définition du RGPD[19], même si elle reste en vigueur en Suisse au moment d'écrire ces lignes.

Nous trouvons la trace de nombreuses réflexions des années 1960 et 1970 qui vont dans le sens de la solution retenue en Suisse et au Liechtenstein. L'idée était de protéger le droit *à la* vie privée non seulement des individus, mais également des groupes d'individus.

Le projet de convention internationale pour la protection « de la vie privée personnelle et industrielle » de l'Association internationale des avocats (Conseil de l'Europe, CCJ/Prot.Priv. (71) 1) porte, comme son nom l'indique, à la fois sur la vie privée des personnes physiques et des personnes morales. Toutefois, elle est divisée en quatre parties, dont deux concernent la vie privée des personnes physiques, et deux celle des personnes morales, aucune disposition n'étant commune aux deux. La seconde partie du projet de convention, sur les banques de données électroniques, ne définit pas la notion de « donnée à caractère personnel », mais confère déjà le droit à la « personne concernée » d'avoir accès aux informations la concernant, et, dans certains cas, de consentir (ou non) à « l'extraction » de ses données.

Pour la *British Computer Society*, dans un rapport datant de 1971, le droit *à la* vie privée concernait autant les individus que les groupes :

> « Le Comité sur la vie privée de la *British Computer Society* propose que soit introduite une loi qui définisse les droits de la personne, qu'il s'agisse d'un individu, d'un groupe ou d'une institution, au regard de la vie privée d'informations la concernant, lorsqu'elles sont détenues par des tiers ou traitées par elles[20]. » (BCS, 1971, p. 1)

Le projet de loi fédérale ouest-allemande de 1972 prévoyait aussi d'inclure les données sur les personnes morales dans la définition de la notion de « donnée à caractère personnel » :

18 *Datenschutzgesetz (DSG) vom 14. März 2002*, Liechtenstein.

19 *Datenschutzgesetz (DSG) vom 4. Oktober 2018*, Liechtenstein.

20 Traduction de l'auteur. Texte original : « The British Computer Society Privacy Committee submits that legislation should be introduced to define the rights of the person, whether an individual, group or institution, with respect to the privacy of information relating to him, when held by others or handled by them. »

> « Par « donnée à caractère personnel » [*personal data*] nous entendons des éléments particuliers concernant la condition personnelle ou matérielle d'une personne physique ou morale en droit privé identifiée ou identifiable d'une association de personnes identifiée ou identifiable (ci-après : la « personne concernée » [*person concerned*]. Les établissements publics, services et autorités administratives exerçant des fonctions similaires, qui sont ou appartiennent à des entreprises de droit public, sont considérées comme équivalentes à des personnes telles que définies dans la phrase 1[21]. » (Section 2, Referentenentwurf Bundes-Datenschutzgesetz 1972, Conseil de l'Europe. EXP/Prot.Priv./ EDB (73) 2)

Le brouillon de la résolution du Conseil de l'Europe n° 22 de 1973[22] incluait les données relatives aux personnes morales dans son champ d'application. Les « données à caractère personnel » étaient ainsi décrites dans la note explicative qui l'accompagnait comme « des donnée concernant des personnes physiques ou morales »[23] (Conseil de l'Europe, EXP/Prot.Priv./ EDB (72) 14, p. 7). Toutefois, plusieurs délégations nationales se sont opposées à ce que les personnes morales bénéficient d'un droit *à la* protection des données à caractère personnel. Des observations datées du 28 février 1973 nous indiquent que la délégation française s'est jointe à cette position ; il y est écrit que « les dangers du stockage d'informations sont indéniablement plus grands dans le cas [des individus] que [des personnes morales], même si, techniquement, il semblerait que le principe proposé puisse être appliqué aux deux[24] » (Conseil de l'Europe, CCJ/SC.Prot.Priv. (73) 2, p. 3). Les résolutions de 1973 et 1974 sur la protection des données à caractère personnel, comme ensuite la Convention 108, ne concernent donc, *in fine*, que les personnes physiques.

Le projet britannique de loi « sur la surveillance par les données[25] », de 1969, ne prévoyait que l'octroi d'un droit d'accès aux personnes physiques aux données qui les concernent. Les droits conférés par la loi adoptée en Hesse en 1970[26] s'adressait à des personnes physiques. Il en va de même pour la loi suédoise de 1973[27] et la loi française de 1978[28]. Même si l'article 3 paragraphe 1 sous b) de la Convention 108 précise que les États signataires peuvent étendre par

21 Traduction de l'auteur. Texte original : « By « personal data » are meant particulars concerning the personal or material condition of an identified or identifiable natural or juristic person in private law or of an identified or identifiable association of persons (hereinafter termed « the person concerned »). Public undertakings, services or administrative bodies exercising similar functions, which are or belong to public-law corporations, shall be considered equivalent to the persons referred to in sentence 1. »

22 Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé.

23 Traduit de l'anglais : « data concerning physical or legal persons. »

24 Texte original : « […] the dangers from stored information are undeniably greater in the case of the former than the latter; technically speaking, however, it would seem that the propose principle could apply to both. »

25 Data Surveillance Bill 1969, Royaume-Uni.

26 Hessische Datenschutzgesetz, 7 octobre 1970 (GVBl. I S. 625) (Hesse)

27 Datalag (1973:289) (Suède)

28 Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (France)

une déclaration son champ d'application « à des informations afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique », cette possibilité n'a que très peu été employée[29].

Selon les souvenirs de Peter Hustinx évoqués en entretien, pour la plupart des participants aux groupe d'experts du Conseil de l'Europe, la reconnaissance d'un droit *à la* vie privée aux personnes morales – et notamment aux entreprises – « était en fait un non-sens, pour le dire gentiment[30] ».

Pour Spiros Simitis, l'exclusion des données relatives aux personnes morales se justifiait par le rattachement de cette matière juridique au corpus pré-existant du droit de la personnalité :

> « En tant que juriste, si vous regardez les lois telles qu'elles étaient à l'époque, [en tant que] juriste allemand, comme les juristes d'autres pays, [et] que vous réfléchissiez, [vous vous poseriez la question suivante] : quel est le lien entre la protection des données et les lois que nous avons déjà ? Si vous regardez la Loi française, par exemple, ou la Loi allemande, ou les lois italiennes, et ainsi de suite, nous avions déjà, depuis longtemps, une longue tradition de ce que nous [appelons en allemand] : *Persönlichkeitsrecht*, le droit de

29 Le Conseil de l'Europe tient à jour une liste d'États signataires de la Convention 108 ayant déclaré étendre le champ d'application de la convention aux personnes morales. La Suisse et le Liechtenstein font partie de ces pays, de même que l'Arménie, l'Autriche, la Bulgarie, Saint-Marin et la France (la liste n'est pas exhaustive). Mais dans le cas du Liechtenstein, la loi ne définit plus les données personnelles comme des données relatives aux personnes physiques *ou morales* depuis l'entrée en vigueur de la loi de protection des données du 4 octobre 2018 (*Datenschutzgesetz vom 4. Oktober 2018*). Le droit autrichien définit les données personnelles comme « alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen », c'est-à-dire « toutes les informations qui se rapportent à des personnes physiques identifiées ou identifiables » (art. 36 paragraphe 2, premier alinéa de la loi fédérale de protection des données (*Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten*), dans sa version consolidée au 20 juin 2019). Concernant la France, la raison pour laquelle elle est indiquée comme appliquant la Convention 108 aux entreprises est que par la délibération n° 84-28 du 3 juillet 1984, la CNIL a considéré qu'un fichier d'entreprises relevait du champ d'application de la loi informatique et libertés. Mais cela ne résultait pas d'une extension de la notion de donnée « nominative » aux données relatives aux personnes physiques, mais du fait que le fichier visé en l'espèce contenait les noms de dirigeants d'entreprises, ce qui en faisait, du même coup, un « fichier de données nominatives ». À Saint-Marin, la loi du 21 décembre 2018 sur la protection des données (*Legge 21 dicembre 2018 n° 171 - Protezione delle persone fisiche con riguardo al trattamento di dati personali*) a pour objet « la protection des personnes physiques au regard du traitement de leurs données personnelles » (*« [la] protezione delle persone fisiche con riguardo al trattamento dei dati personali* », art. 1 §1 de la loi précitée) et définit une « donnée à caractère personnel » comme étant relative à des personnes physiques identifiées ou identifiables (art. 2 paragraphe 1 sous a) de la loi précitée).
La liste tenue à jour par le Conseil de l'Europe ne peut donc pas – ou peut-être plus – être considérée comme fiable. Même le Liechtenstein, qui considérait jusqu'à très récemment les données relatives aux personnes morales comme personnelles, s'est aligné sur la définition retenue par le reste des pays de l'EEE.
Voir : https://www.coe.int/fr/web/data-protection/national-information (page consultée le 20 juin 2019).

30 Traduit du néerlandais : « eigenlijk onzin, vriendelijk gezegd ».

protéger la personnalité d'une personne. Et la protection des données en fait en fait partie[31]. » (Entretien avec Spiros Simitis)

De plus, toujours selon Spiros Simitis, le droit de la personnalité, qui comprendrait le droit *à la* protection des données à caractère personnel, sont des droits constitutionnels, fondamentaux, dont les sujets doivent demeurer des personnes physiques, et non des personnes morales :

« […] la protection de la personnalité est purement un droit constitutionnel applicable à des personnes individuelles[32] […] » (Entretien avec Spiros Simitis)

Michael Kirby a également rappelé dans un témoignage qu'il a récemment publié sur l'histoire de la protection des données que la « vie privée » des personnes morales et des personnes physiques soulèvent des questions distinctes qu'il conviendrait de traiter séparément :

« Lorsque j'exerçais à la Haute Cour d'Australie, dans *Lenah Game Meats Pty Ltd v Australian Broadcasting Corporation ('Lenah')*, une tentative fut réalisée pour renverser, ou pour invalider, ou pour ré-examiner le principe de l'affaire *Taylor*. J'aurais été tout à fait prêt à accepter de le faire. Néanmoins, le cas d'espèce soulevait une question sur le droit potentiel d'une entreprise à la vie privée. Il y a bien longtemps, en menant son enquête sur la vie privée, l'ALRC avait pointé que le droit à la « vie privée » par des personnes morales (des entreprises) soulevaient des questions qui étaient distinctes et séparées des questions de droits humains normalement soulevées en relation à des revendications individuelles à la vie privée[33] » (Kirby, 2017, p. 15)

À l'exception notable du droit du Liechtenstein jusque fin 2018, et de la Suisse, la notion de « donnée à caractère personnel » a donc toujours été définie dans les textes définitivement

31 Traduction de l'auteur. Texte original : « As a lawyer, if you look at the laws [as] they were at the time, [as a] German lawyer, as lawyers in other countries [and] reflected: where is the link of data protection to the laws we already have? If you look at French law for instance, or at the German law, or at the Italian laws and so on, we had before, for a very long time, with a very long tradition, what we [call in German]: *Persönlichkeitsrecht*, the right to protect the personality of a person. And data protection is in fact a part of that. »

32 Traduction de l'auteur. Texte original : « […] the protection of the personality is purely a constitutional right applicable to the individual persons […] ».

33 Traduction de l'auteur. Texte original : « During my service on the High Court of Australia, in *Lenah Game Meats Pty Ltd v Australian Broadcasting Corporation ('Lenah')*, an attempt was made to overcome, or to have overruled, or re-examined the principle in *Taylor's case*. I would have been most ready to agree to doing so. However, the case in question arose in a potential claim for privacy by a corporation. Long before, in undertaking its investigation of privacy, the ALRC had pointed out that claims to 'privacy' by legal persons (corporations) raised issues that were distinct and separate from the human rights issues normally addressed in relation to individual claims to privacy. »

adoptés comme étant une donnée « relative » à un individu[34]. Mais qu'est-ce qui fait d'une donnée qu'elle est « relative » à un individu ? Quelle doit être la force de ce lien pour pouvoir la *qualifier* de « personnelle » ? La rédaction des définitions de la loi suédoise de 1973 et des résolutions de 1973 et 1974 du Conseil de l'Europe ne le précisaient pas[35].

Au sens actuel du RGPD, une donnée est « à caractère personnel » dès lors qu'elle concerne une personne physique « identifiée ou identifiable », « directement ou indirectement ». Cette précision est importante. Sans elle, le champ d'application matériel du droit *de la* protection des données à caractère personnel aurait pu être réduit aux seules données comportant le nom de la personne, ou d'autres éléments très directement identifiants, comme les données biométriques ou des numéros d'identification tel que, en France, le numéro d'inscription au répertoire des personnes physiques (NIR) plus connu sous le nom de numéro de sécurité sociale.

Bien que le contenu de sa définition soit un calque des définitions circulant dans les arènes spécialisées du Conseil de l'Europe et de l'OCDE, la loi Informatique et Libertés française adoptée en 1978 a traduit l'expression « donnée à caractère personnel » par celle de « donnée nominative ». Cela a pu prêter à confusion en laissant entendre qu'une « donnée à caractère personnel » pouvait ne pas être « nominative » si elle ne contenait pas le nom de la personne concernée. André Vitalis, Henri Delahaie et Félix Paoletti ont donc tenu à clarifier ce point dans un extrait reproduit ci-dessous d'un livre rédigé sur commande de la CNIL à l'occasion des dix ans de cette autorité :

> « Le caractère nominatif des informations est le critère essentiel d'application de la loi du 6 janvier 1978. L'article 4 considère comme nominatives, « les informations qui permettent sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent ». L'identification peut donc être assurée directement par le nom patronymique et le prénom, quoique avec des risques d'homonymie, ou indirectement, par toute autre indication. […] Dans l'esprit même du texte de loi, la Commission donne une interprétation très large de la notion « d'informations nominatives ». » (CNIL, 1988, pp. 41-42)

Retrouver manuellement l'identité de la personne sur laquelle porte une donné en la recoupant avec d'autres jeux d'informations était une opération hautement chronophage. Avec l'arrivée de l'ordinateur, garantir un anonymat robuste devint nettement plus difficile. Cet état de fait a été rappelé dans un jugement du Tribunal constitutionnel fédéral de RFA de 1983 :

34 Voir, à l'annexe 2 la définition suédoise de 1973 de la notion.
35 Cf. annexe 2.

« D'après le droit général de la personne – article 2 paragraphe 1, en relation avec l'article 1 paragraphe 1 de la constitution allemande (*Grundgesetz*) – un recensement de la population doit être anonyme. Ceci a aussi été établi par la Cour constitutionnelle fédérale par sa décision du 16 juillet 1969 sur la constitutionnalité d'une statistique représentative (Bundesverfassungsgericht 27, 1 – « Recensement par échantillonnage) ») et a été considéré comme acquis dans les recensement par échantillonnage de cette époque. L'exigence d'anonymat de la *Grundgesetz* nécessite qu'aucune relation entre les données prélevées et des personnes identifiables ou des groupes de personnes ne puisse être établie. Une donnée efficacement anonymisée et à la disponibilité strictement délimitée empêcherait toute reconstitution d'un lien avec l'individu. Si au contraire l'anonymisation n'était pas ou mal garantie, cela rendrait possible une utilisation de données se rapportant à des individus ou des groupes de personnes pour n'importe quel but extérieur. Ainsi, l'individu pourrait être dépouillé de son libre consentement et devenir l'objet du contrôle et de l'exercice d'une volonté étrangère. Dans les recensements de populations, les données n'étaient pas anonymisées, mais restaient dans tous les cas liées à des personnes. Cela s'applique aussi quand le nom est omis. **Selon l'état confirmé des recherches, des données apparemment anonymisées de façon inviolable pourraient aujourd'hui être facilement repersonnalisées en utilisant des méthodes mathématiques simples.** La ré-identification serait particulièrement facile à l'aide du numéro du foyer ainsi que de la liste de numéro, qui sont utilisés pour procéder au recensement de population sans base légale. »[36] (BverfG 15/12/1983 Volkszählungsurteil, pt. 110)

La définition proposée dans le projet de loi fédérale de protection des données de RFA en 1972 précisait que la définition de la notion de « donnée à caractère personnel » devait concerner les personnes « identifiées ou identifiables[37] ». Cette conception juridique de la notion de « donnée à caractère personnel » rappelle celle des informaticiens de la *British Computer Society* qui, en 1972, rappelaient le risque de ré-identification de données paraissant anonymes dans leur façon de définir la notion d'« information personnelle » :

« Information personnelle : Déclaration de la forme -

36 Traduit de l'allemand par Nebiha Guiga. Texte original : « Aus dem allgemeinen Persönlichkeitsrecht des Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG folge für eine Volkszählung das Gebot der Anonymität. Dies habe auch das Bundesverfassungsgericht in seiner Entscheidung vom 16. Juli 1969 zur Verfassungsmäßigkeit einer Repräsentativstatistik (BVerfGE 27, 1 - Mikrozensus) festgestellt und beim damaligen Mikrozensus als gegeben vorausgesetzt. Das Anonymitätsgebot des Grundgesetzes erfordere, daß kein Zusammenhang zwischen erhobenen Daten und individualisierbaren Personen oder Personengruppen hergestellt werden könne. Ein wirksam anonymisiertes und in seiner Verfügbarkeit strikt begrenztes Datum könne auf die Einzelperson keinerlei Rückwirkung haben. Sei die Anonymität dagegen nicht oder nicht voll gewährleistet, so mache eine Befragung Daten über individuelle Personen und Personengruppen für beliebige fremdbestimmte Zwecke verfügbar. Dadurch könne die Einzelperson der freien Selbstbestimmung beraubt und zum Gegenstand fremder Willensausübung und Kontrolle werden. Bei der Volkszählung würden die Daten nicht anonymisiert, sondern blieben in allen Fällen personenbezogen. Dies gelte auch dort, wo der Name entfalle. Nach dem gesicherten Stand der Forschung könnten scheinbar undurchbrechbare Anonymisierungen heute mit einfachen mathematischen Verfahren repersonalisiert werden. Besonders leicht sei die Reidentifizierung mit Hilfe der Haushaltskennummern sowie der Zählerlisten, die für die Durchführung der Volkszählung ohne gesetzliche Grundlage vorgesehen seien. »

37 Cf. annexe 2.

Nom de l'individu, information factuelle.

L'information factuelle peut être implicite ou donnée par le contexte : par exemple, si une bande magnétique contient uniquement une liste de noms et qu'il est dit que c'est une liste de prisonniers.

L'identité individuelle peut être submergée dans des statistiques apparemment anonymes, mais si elle peut être extraite alors il faut considérer qu'elle y est présente[38]. » (British Computer Society, 1972, p. 12)

Les définitions contenues dans les Lignes directrices de l'OCDE de 1980 et la Convention 108 de 1981 contiennent toutes deux les mots « identifiée ou identifiable » :

Art. 1 sous b) des Lignes directrices de l'OCDE	**Article 2 sous a) de la Convention 108 du Conseil de l'Europe**
Toute information relative à une personne physique identifiée ou identifiable	Toute information concernant une personne physique identifiée ou identifiable («personne concernée»)

Tableau 15 : *Définitions de la notion de « donnée à caractère personnel » dans les Lignes directrices de l'OCDE et dans la Convention 108 du Conseil de l'Europe.*

La définition française de la « donnée nominative » contenait quant à elle les mots « directement ou non ». Au niveau européen, les termes « directement ou indirectement » ont été insérés en 1995 dans la définition de la « donnée à caractère personnel », à l'article 2 sous a) de la directive 95/46/CE. Depuis, dans l'Union européenne, les données sont personnelles si elles permettent de faire un lien avec une personne « identifiée ou identifiable », « directement ou indirectement » :

« Toute information concernant une personne physique **identifiée ou identifiable** (personne concernée); est réputée identifiable une personne qui peut être identifiée, **directement ou indirectement**, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale » (art. 2 sous a) de la directive 95/46/CE)

38 Traduction par l'auteur. Texte original : « Personal Information : Statement of the form - Individual name, factual statement.
The factual statement may be implied or given by context: for example, if a magnectic tape containing only a list of names is said to be a list of prison inmates.
The individual identity may be submerged in apparently anonymous statistics, but if it can be extracted then it must be considered to be there. »

Ces mots se retrouvent aussi dans la définition de la notion de « donnée à caractère personnel » de l'article 4 du RGPD.

6.2.2. Les données qui relèvent de l'intimité, ou toute donnée ?

Une seconde question tranchée dès le début des années 1970 consistait à savoir si les données qu'il faut protéger sont celles qui relèvent de la vie privée ou de l'intime, qu'il aurait alors fallu pouvoir délimiter dans une définition claire attachée à celle de la notion de donnée à caractère personnel, ou bien si toutes les données portant sur des personnes, quel que soit leur contenu, doivent être soumises au droit *de la* vie privée (ou *de la* protection des données). Nous verrons que si les tentatives initiales de définition penchaient en faveur de la première option, le choix du Conseil de l'Europe, dans la Convention 108, trancha en faveur de la seconde.

Plusieurs tentatives précoces de définition de la notion juridique de « donnée à caractère personnel » limitaient son champ à des données qui contiennent des informations relevant de la « vie privée » ou de « l'intimité » des personnes. Dans le projet de loi fédéral de RFA de 1972, les données personnelles étaient par exemple définies comme :

> « Par « donnée à caractère personnel » [*personal data*] nous entendons **des éléments particuliers concernant la condition personnelle ou matérielle** d'une personne physique ou morale en droit privé identifiée ou identifiable d'une association de personnes identifiée ou identifiable (ci-après : la « personne concernée » [*person concerned*]. Les établissements publics, services et autorités administratives exerçant des fonctions similaires, qui sont ou appartiennent à des entreprises de droit public, sont considérées comme équivalentes à des personnes telles que définies dans la phrase 1[39]. » (Section 2, Referentenentwurf Bundes-Datenschutzgesetz 1972, Conseil de l'Europe. EXP/Prot.Priv./EDB (73) 2)

Une autre disposition du même projet de loi montrait qu'il ne visait à s'appliquer qu'aux situations relevant strictement du droit *à la* vie privée. Il était en effet précisé que les informations publiquement accessibles, donc appartenant déjà à la sphère publique, devaient être exclues de son champ d'application :

39 Traduction de l'auteur. Texte original : « By "personal data" are meant particulars concerning the personal or material condition of an identified or identifiable natural or juristic person in private law or of an identified or identifiable association of persons (hereinafter termed "the person concerned"). Public undertakings, services or administrative bodies exercising similar functions, which are or belong to public-law corporations, shall be considered equivalent to the persons referred to in sentence 1. »
Texte mis en gras par l'auteur.

> « Rien dans cette loi ne sera interprétée comme protégeant des données personnelles qui peuvent être directement obtenues de sources généralement accessibles[40]. » (Section 3 (2) du projet de loi fédérale de 1972, Conseil de l'Europe. EXP/Prot.Priv./EDB (73) 2)

Un peu plus tard, Jean-Paul Costa, expert de la délégation française auprès du groupe d'experts du Conseil de l'Europe sur la protection de la vie privée vis-à-vis des banques de données électroniques, rédigea une proposition qui dessinait là encore les contours d'une définition restreinte à la protection de la sphère privée de la notion de « donnée à caractère personnel » :

> « données […] relatives à la vie privée ou à l'intimité [*private life or privacy*] d'individus qu'elles concernent, et particulièrement les informations concernant leurs races, relations, opinions politiques, mœurs, santé ou casiers judiciaires[41]. » (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 17, p. 14)

Cette définition restreinte à une description de la sphère privée, soit par liste énumérative de son contenu, comme dans celle de Jean-Paul Costa, ou bien par opposition à la sphère publique composée de ce qui a déjà été rendu public, comme dans la proposition allemande, a cependant vite cédé la place à une définition englobante, c'est-à-dire portant sur *toute* donnée relative à une personne.

Cela est dû à deux arguments, l'un de nature philosophique et l'autre de nature technique.

L'argument philosophique tient à la difficulté pour des personnes inspirées par le libéralisme utilitariste de définir *ex ante*, une fois pour toutes, et pour tout le monde, ce qui relève ou non de l'intime (voir à ce sujet : Eynard, 2013, p. 55-67). Cela est au cœur de ce que paradigme libéral de la vie privée de la « *privacy community* » a désigné depuis par de « droit à l'autodétermination informationnelle ». Le rappel de la définition de la « vie privée » proposée par Alan Westin dans le rapport de la *British Computer Society* remis au comité Younger en 1971, dont des membres participèrent aux travaux du Conseil de l'Europe, illustre – parmi d'autres exemples qui auraient pu être choisis – la place occupée par ce paradigme :

40 Traduction de l'auteur. Texte original : « Nothing in this Act shall be construed as protecting personal data which can be directly obtained from generally accessible sources. »

41 Traduction de l'auteur. Texte original : « data […] as relates to the private life or privacy of individuals whom it concerns, and particularly information concerning their race, religion, political opinions, morals, health or past judicial record. »

« « La vie privée est la revendication d'individus, de groupes ou d'institutions qui déterminent pour eux-mêmes quand, comment et dans quelle mesure de l'information les concernant peut être communiquée à d'autres ». - *Privacy and Freedom* par Alan F. Westin[42] » (British Computer Society, 1971, p. 2)

Selon Peter Hustinx, qui aborda ce sujet en entretien :

« […] en 1950, la vie privée était : la maison, les courriers, la correspondance, la vie familiale. Ces concepts […] avaient une certaine évidence. Mais cela devient moins évident à mesure que l'on se penche sur ce qu'est la vie privée. Et surtout le privé en dehors de la maison. Donc l'incertitude du concept de privé quand des données circulent. Qu'est-ce qui tombe vraiment sous la notion de vie privée[43] ? » (Entretien avec Peter Hustinx)

Ce sont ces interrogations, qui, toujours selon Peter Hustinx, ont conduit les membres du groupe d'experts de l'OCDE à s'accorder sur l'idée que les principes de base de la protection des données[44] devraient s'appliquer à *toutes* les données relatives à des personnes, quel que soit leur contenu :

« Nous étions d'accord que certains principes devaient être applicables dans tous les cas. Celui d'exactitude, d'exhaustivité, de pertinence, qu'il devait toujours y avoir un but légitime, et quelques autres[45] [...] » (Entretien avec Peter Hustinx)

Notons malgré tout que parmi cet ensemble englobant de donnée à caractère personnel, certaines ont très tôt été considérées comme particulièrement « sensibles », nécessitant une forme de protection renforcée en raison du risque que leur traitement ferait courir (Gellert, 2016). Ainsi, l'article 1 d'un projet de Convention nordique sur le traitement des données de caractère personnel soumis à la lecture des membres du Groupe d'experts sur l'utilisation des ordinateurs de l'OCDE énonçait :

42 Traduction de l'auteur. Texte original : «"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others". - Privacy and Freedom by Alan F. Westin »

43 Traduit du néerlandais : « […] in 1950 was privéleven: huis, brieven, briefwisseling, familieleven. Die begrippen […] hadden een zekere evidentie. Maar naarmate je kijkt naar wat privéleven is, was het onduidelijk. En vooral wat privé buiten het huis plaatsvindt. Dus de onduidelijkheid van het begrip privé als gegevens gaan stromen. Wat valt nou wel en niet onder privéleven? »

44 Cf. section 3.4.4.

45 Traduit du néerlandais : « « Men was het erover eens dat in alle gevallen bepaalde beginselen van toepassing moesten zijn. Dus die van juistheid, en volledigheid, en relevantie, en er zou altijd een legitiem doel moeten zijn, en nog een paar andere beginselen. »

« La présente convention vise les systèmes de traitement électronique de données qui traitent des données de caractère personnel. Elle s'applique également aux autres systèmes de traitement des données dans la mesure où ils contiennent :

(i) des données concernant la nationalité, la race, les opinions politiques ou les croyances religieuses des individus ;

(ii) des données concernant des activités criminelles des individus et les sanctions pénales encourues ;

(iii) des données concernant le comportement sexuel ;

(iv) des données concernant les enquêtes pour l'octroi de crédit et la solvabilité ;

(v) des données concernant l'attribution d'une aide sociale, d'une assistante sociale et d'autres interventions analogues ;

(vi) d'autres données de caractère nettement intime ou personnel » (OCDE, DSTI/CUG/79.9, 1ère révision, Annexe III, p. 32)

L'article 6 de la Convention 108 définit la notion de « catégorie particulière de données », qui recouvre « les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle » (art. 6 de la Convention 108), et indique que ces dernières ne peuvent être traitées sans « garanties appropriées » supplémentaires par rapport aux simples « données à caractère personnel ». En France, ces « garanties appropriées » reposaient (et reposent d'ailleurs toujours) essentiellement sur le consentement de la personne concernée :

« Il est interdit de mettre ou conserver en mémoire informatisée, sauf accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales des personnes. » (art. 31 de la loi Informatique et Libertés française, version initiale du 6 janvier 1978)

Le fait qu'une donnée ne comporte aucune de ces informations *a priori* « sensibles » ne les exclut toutefois en rien de la qualification de « donnée à caractère personnel », et donc du champ d'application du droit *de la* protection des données alors en train d'être développé. Le renforcement de la place du consentement de la personne concernée comme critère de licéité d'un traitement de données, lors de l'adoption de la directive 95/46/CE, illustre comment ce nouveau corpus de règles juridiques accorde ainsi à l'individu la faculté de déterminer par lui-même ce qu'il souhaite accepter comme collecte et utilisation des données le concernant, et donc de

déterminer ce qui, pour lui, relève ou non de sa vie privée. Qu'il existe un corpus de données personnelles jugées sensibles dont la protection est renforcée *a priori* n'y change rien, d'autant qu'une personne demeure libre de divulguer celles qui la concernent sur la base de son consentement.

L'autre argument en faveur d'une définition de la notion de « donnée à caractère personnel » qui désigne *toute* donnée relative à une personne physique identifiée ou identifiable directement ou indirectement est de nature plus technique. Il est lié aux évolutions des capacités de traitement informatiques : les capacités de recoupement des informations dont sont capables les ordinateurs, par rapport aux anciennes méthodes de traitement de l'information, permettent non seulement de ré-identifier des jeux de données ayant l'apparence de l'anonymat, mais aussi d'enrichir ces données. Cela a très vite été perçu comme rendant très difficile de définir à l'avance ce qui est une donnée sensible ou pas, sachant qu'une donnée qui en soi ne paraît pas sensible peut le devenir lorsqu'elle est couplée avec d'autres informations :

> « En particulier avec le traitement automatique de données, vous ne savez peut-être pas, au moment où la donnée est collectée, qu'elle est ou qu'elle deviendra sensible dans une étape future[46]. » (Entretien avec Michael Kirby)

> « […] certaines données qui sont inoffensives lorsqu'elles sont considérées de manière séparée peuvent être corrélées d'une façon qui fasse de leur disponibilité une menace pour la vie privée[47]. » (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 14, p. 5)

Ces arguments se sont conjugués avec ceux plus philosophiques en faveur du droit à l'auto-détermination informationnel. Comme le résumait Stefano Rodotà lors de son intervention à la conférence de l'OCDE de 1974 :

> « […] Il faut souligner que le droit à une certaine intimité perd constamment du terrain dans les définitions du droit à la vie privée au profit de la possibilité donnée à l'individu d'exercer un contrôle sur la communication des informations qui le concernent […]. C'est au contrôle et non plus au secret qu'il faut donner la place. […]
>
> Il devient de plus en plus difficile de définir le type d'informations dont le citoyen est prêt à se dessaisir, c'est-à-dire à fournir, en renonçant définitivement à exercer le moindre

46 Traduction de l'auteur. Texte original : « Especially with automated data, you may not know at the time that the data is collected that it is or will at some stage in the future become sensitive »

47 Traduction de l'auteur. Texte original : « […] certain data which are inoffensive when considered separately may be correlated in such a fashion that their availability may become a threat to privacy »

contrôle sur le traitement qu'elles subiront, et sans savoir entre quelles mains elles tomberont. Cette attitude s'explique par le fait que l'information qui semble la plus anodine à première vue peut s'avérer nuisible pour l'intéressé si elle est intégrée à d'autres données. » (Rodotà, 1974, p. 149-159)

Par précaution, il conviendrait alors d'appliquer un minimum de règles à toutes les données à caractère personnel, quel que soit leur contenu. Cette logique entraîna l'adoption de définitions englobantes de la notion de donnée à caractère personnel, décorrélées de la question de la sphère privée ou de l'intime.

Cette définition englobante illustre un processus d'autonomisation du droit *à la* protection des données personnelles du droit *à la* vie privée à partir des années 1970 :

« Le concept de « donnée à caractère personnel » est défini comme « toute information concernant une personne physique identifiée ou identifiable (« personne concernée »). Cela veut dire que la « protection des données » est *plus large*[48] que la « protection de la vie privée », parce que cela concerne aussi d'autres droits et libertés fondamentaux, et toutes sortes de données *indépendamment*[49] de leur relation à la vie privée, et elle est en même temps *plus limitée*[50] parce qu'elle ne concerne que le traitement d'informations personnelles, les autres aspects de la protection de la vie privée étant négligés[51]. » (Hustinx, 2013, p. 4-5).

Ce processus est fortement influencé à la fois par l'émergence de ce droit constitutionnel à l'auto-détermination informationnelle dérivé du principe de dignité de la personne humaine de la Loi fondamentale ouest-allemande, et par la nécessité de constituer un corpus de règles juridiques qui définissent un équilibre entre le droit *à la* vie privée et le droit *à la* liberté d'expression en matière de circulation d'informations portant sur des individus[52].

Or, nous avons vu que cette tension entre le droit *à la* vie privée et le droit *à la* protection des données à caractère personnel d'une part, et le droit *à la* liberté d'expression d'autre part,

48 En italique dans le texte.
49 En italique dans le texte.
50 En italique dans le texte.
51 Traduction de l'auteur. Texte d'origine en anglais : « The concept of 'personal data' is defined as 'any information relating to identified or identifiable individual ('data subject')'. This means that 'data protection' is *broader* than 'privacy protection' because it also concerns other fundamental rights and freedoms, and all kinds of data *regardless* of their relationship with privacy, and at the same time, *more limited* because it merely concerns the processing of personal information, with other aspects of privacy protection being disregarded. »
52 C'est un point sur lequel Peter Hustinx a fortement insisté en entretien.

était un des éléments centraux de l'opposition entre États-Uniens et Européens de droit continental dans le groupe d'experts de l'OCDE qui a rédigé les Lignes directrices[53]. Le texte définitif est le reflet d'une position de compromis. En effet, il est pleinement compatible avec le projet de ce qui allait devenir très peu de temps après la Convention 108 du Conseil de l'Europe. Les principes de la protection des données sont repris dans les Lignes directrices, et la définition de la notion de « donnée à caractère personnel » y est englobante. Toutefois :

> « Les présentes lignes directrices ne devraient pas être interprétées comme interdisant : […]
>
> b) d'en exclure l'application à des données de caractère personnel qui, manifestement, ne présentent aucun risque pour la vie privée et les libertés individuelles [...] » (art. 3 des Lignes directrices de l'OCDE)

Cette rédaction permettait une interprétation selon laquelle le droit *de la* protection des données ne devait s'appliquer qu'en présence d'informations relevant de la « vie privée », et éviter de restreindre la liberté d'expression en présence de données personnelles qui ne relèveraient pas de cette catégorie. Comme le résume Michael Kirby, qui présidait le groupe ayant rédigé ce texte entre 1978 et 1980 :

> « [L'OCDE] a adopté un ton très large et englobant, mais en a ensuite réduit la portée en faisant référence aux cas innocents, qui ne gênaient pas, où le texte serait allé trop loin, ce qui n'est pas inhabituel dans ce type d'exercice de rédaction[54]. » (Entretien avec Michael Kirby)

Dans le même temps, cette rédaction contenta les Européens de droit continental qui purent adopter un droit *de la* protection des données à caractère personnel opérationnalisant un droit nouveau *à la* protection des données à caractère personnel, sans imposer cette nouvelle catégorie de sens (et de droit) aux signataires qui souhaitaient, à l'instar des États-Unis, s'en tenir à la protection du droit *à la* vie privée.

La Cour de justice des communautés européennes (CJCE), renommée Cour de justice de l'Union européenne (CJUE) par le traité de Lisbonne, a eu l'occasion de rappeler à plusieurs reprises que dans l'UE, la notion de « donnée à caractère personnel » ne doit pas être confondue avec celle de « donnée relative à la vie privée ».

53 Cf. section 3.7.

54 Traduction de l'auteur. Texte original : « [The OECD] adopted a very broad and embracing genus, but it then cut back that genus by reference to innocent, or untroubling, overreach, that's not an unusual type of drafting. »

6.3. La définition de la notion de donnée à caractère personnel en débat devant la Cour de justice de l'Union européenne

6.3.1. Le rôle de la Cour de justice de l'Union européenne dans le droit *de la* protection des données à caractère personnel en Europe

La judiciarisation fait partie du registre d'actions des groupes d'intérêt (Grossman et Saurugger, 2012). Il peut s'agir d'attaquer une décision concernant un projet des puissances publiques auquel s'oppose le groupe d'intérêt, comme par exemple dans les cas de recours d'associations de riverains contre des projets d'aménagements locaux. Il peut s'agir de recours en responsabilité contre l'État ou une entreprise visant à obtenir l'indemnisation d'un préjudice. Ceci peut être utile soit pour obtenir la réparation effective du préjudice subi par une ou des victimes, comme lorsque l'association néerlandaise *Mothers of Srebrenica* a obtenu en 2017 la reconnaissance de la responsabilité de l'État néerlandais dans le massacre de Srebrenica par la Cour d'Appel de La Haye[55]. Dans d'autres cas, il s'agit de demander des dédommagements pécuniaires afin de faire pression financièrement sur la partie attaquée, comme ce fut le cas dans l'affaire opposant en France l'UFC-Que Choisir à Facebook, où cette association avait obtenu la condamnation de l'entreprise au titre du préjudice moral collectif subi par les consommateurs-utilisateurs de ce réseau social du fait des clauses abusives de ses conditions générales d'utilisation[56]. Il peut également s'agir d'attaquer un acte juridique de portée général, comme une loi ou un règlement, ou, dans le cas de l'Union européenne, un acte de droit dérivé tel qu'une directive ou un règlement. Enfin, il peut s'agir, au cours d'un procès, de demander à un juge de cassation de remettre en cause une interprétation ayant fait jurisprudence d'un texte juridique, ou, en son absence, d'essayer d'établir dans celle-ci une interprétation allant de le sens de ses intérêts.

Plusieurs affaires ont ainsi été portées jusqu'à la Cour de justice de l'Union européenne, et ont eu une incidence sur l'interprétation ayant autorité de la chose jugée du texte de la définition de la notion de « donnée à caractère personnel », notamment là où demeuraient les marges de manœuvre que nous allons identifier après avoir rappelé les compétences et les procédures particulières de ce tribunal.

55 Gerechtshof Den Haag (Pays-Bas) 27 juin 2017 « Mothers of Srebrenica », affaires 200.158.313/01 et 200.160.317/01 (ECLI:NL:GHDHA:2017:1761)

56 Tribunal de grande instance de Paris (France) 9 avril 2019 « UFC-Que Choisir contre Facebook », 14/07298

La Cour de justice des Communautés européennes a été instituée par le traité CECA en 1951. En 1957, elle est devenue un organe commun partagé entre la CECA, la CEE et l'Euratom. Depuis décembre 2009 et l'entrée en vigueur du traité de Lisbonne, elle a changé de nom pour devenir la Cour de justice de l'Union européenne. L'article 19 paragraphe 1 TUE définit la mission de la CJUE comme étant d'assurer « le respect du droit dans l'interprétation et l'application des traités ». Elle n'est pas le juge de droit commun du droit de l'Union. Ce rôle revient aux juges nationaux. De plus, les traités n'établissent aucune hiérarchie entre les juges de la CJUE et les juges nationaux. La CJUE n'est donc pas à proprement parler une cour suprême (Jacqué, 2018, p. 434).

Il existe plusieurs procédures de saisine de la CJUE[57], dont les principales sont le recours en manquement, le recours en annulation et le renvoi préjudiciel.

Les recours en manquement (art. 258 à 260 TFUE) sont dirigés par la Commission européenne ou un État membre[58] contre un État membre ne respectant pas ses obligations au regard du droit de l'Union. C'est cette procédure qui a été utilisée en 2000 par la Commission européenne contre le Luxembourg, qui n'avait pas transposé à temps la directive 95/46/CE[59], ou encore contre l'Allemagne pour non-respect du principe de l'indépendance des autorités de protection des données en 2007[60].

Le recours en annulation, dirigé contre une décision de l'Union, est prévu à l'article 263 TFUE. Il peut être dirigé dans un délai de deux mois à compter de la publication ou de la notification de l'acte attaqué, qui peut être un acte législatif, un acte du Conseil, de la Commission, de la Banque centrale européenne (à l'exception des recommandations et des avis), du Parlement et du Conseil, et des organes ou organismes de l'UE dès lors qu'ils sont « destinés à produire des effets juridiques à l'égard des tiers » (art. 263 TFUE). En dehors des « requérants privilégiés » (Sauron et Réguer-Petit, 2018, p. 122) que sont le Parlement européen, la Commission et le Conseil, une personne physique ou morale qui souhaiterait attaquer en annulation un acte de l'Union doit prouver, en vertu de l'art. 263 TFUE, qu'elle est soit « destinataire » soit « directement et individuellement » concernée par la mesure. Ces critères sont interprétés de façon très stricte par la Cour[61], ce qui limite considérablement la possibilité pour des particuliers d'attaquer directement devant elle un acte illégal de l'Union. Les recours en annulation formés par des particuliers, comme les recours en carence (faute par inaction d'une institution de l'Union), en responsabilité, et ceux de la fonction publique européenne sont traités en première instance par le Tribunal de l'UE et sont susceptibles de recours auprès de la CJUE.

57 Pour plus de détails sur les procédures devant la CJUE, voir : Sauron et Réguer-Petit, 2018.
58 L'utilisation de la procédure de recours en manquement par un État membre est extrêmement rare.
59 CJCE 4 octobre 2001 « Commission contre Luxembourg » Aff. C-450/00.
60 CJUE 9 mars 2010 « Commission contre Allemagne » Aff. C-518/07.
61 Voir : CJCE 15 juillet 1963 « Plaumann contre Commission » Aff. 25/62 et CJCE 25 juillet 2002 « Unión de Pequeños Agricultores » Aff. C-50/00 P.

La difficulté résultant de l'étroitesse des conditions de l'intérêt à agir auprès de la CJUE pour les particuliers oblige les groupes d'intérêt à privilégier la voie des renvois préjudiciels. Ce type de recours est prévu à l'article 267 TFUE. Il permet à la Cour de répondre à des questions de juridictions nationales sur l'interprétation des traités de l'UE ou sur la validité et l'interprétation des actes dérivés. N'importe quelle juridiction peut poser une question préjudicielle à la CJUE. Cela suspend la procédure le temps que la CJUE statue. Les juridictions nationales dont les décisions ne sont pas susceptibles de recours ont l'obligation, en application du TFUE, de saisir la CJUE lorsqu'une question d'interprétation sur le droit primaire (les traités) et dérivé (directives, réglements, décisions) de l'UE, ou sur la validité d'un acte de droit dérivé, est soulevée.

C'est ainsi qu'en 2014, Maximilien Schrems, un militant autrichien, a obtenu de la Haute cour irlandaise[62] qu'elle transmette à la CJUE deux questions sur l'interprétation de certaines dispositions de la directive 95/46/CE, dans le cadre d'une procédure dans laquelle il souhaitait faire interdire le transfert de données à caractère personnel de l'UE vers les États-Unis, suite aux révélations d'Edward Snowden sur la coopération d'entreprises américaines avec les programmes de surveillance de masse de la NSA :

> « 1) Eu égard aux articles 7, 8 et 47 de la Charte et sans préjudice des dispositions de l'article 25, paragraphe 6, de la directive 95/46, le Commissaire indépendant chargé d'appliquer la législation sur la protection des données saisi d'une plainte relative au transfert de données à caractère personnel vers un pays tiers (en l'occurrence vers les États-Unis), dont le plaignant soutient que le droit et les pratiques n'offriraient pas des protections adéquates à la personne concernée, est-il absolument lié par la constatation contraire de l'Union contenue dans la décision 2000/520?
>
> 2) Dans le cas contraire, peut-il ou doit-il mener sa propre enquête en s'instruisant de la manière dont les faits ont évolué depuis la première publication de la décision de la Commission? » (CJUE 6 octobre 2015, « Schrems contre Data Protection Commissioner », aff. C-362/14, pt. 36)

Dans sa décision, la CJUE a répondu à la seconde question par une phrase courte mais lapidaire : « [l]a décision 2000/520 [Safe Harbor] est invalide ». Or, le tribunal auteur d'un renvoi préjudiciel est lié par la réponse, qui revêt pour lui « autorité de chose jugée »[63]. L'acte déclaré illégal ne disparaît certes guère de l'ordre juridique de l'Union, comme cela aurait été le cas suite à un recours en annulation ayant prospéré, mais aucun juge ne peut plus l'appliquer. De surcroît, la déclaration d'illégalité est réputée rétroactive, même si le principe de sécurité juridique peut

62 High Court (Irlande) 18 juin 2014, « Maximilian Schrems v. Data Protection Commissioner », 2013-765JR.

63 Selon la CJUE : « […] un arrêt par lequel la Cour a statué à titre préjudiciel sur l'interprétation ou la validité d'un acte pris par une institution de la Communauté tranche, avec l'autorité de la chose jugée, une ou plusieurs questions de droit communautaire et lie le juge national pour la solution du litige au principal » (CJCE 5 mars 1986 « Wünsche », Aff. 69/85, pt. 13).

venir limiter la portée de cette rétroactivité (Jacqué, 2018, p. 808-811). En pratique, le renvoi préjudiciel a donc été une façon pour Max Schrems de contourner les limites posée par l'article 263 TFUE et d'obtenir quand même l'annulation de fait d'un acte : la décision « Safe Harbor », qui permettait à certaines entreprises participant volontairement à un programme piloté par la FTC de se voir librement transférer des données à caractère personnel depuis l'UE[64].

Le renvoi préjudiciel a également été utilisé par des groupes d'intérêt qui ont obtenu par ce biais une déclaration d'invalidité de la directive 2006/24/CE[65] qui obligeait les fournisseurs de services de communications électroniques accessibles au public – c'est-à-dire les fournisseurs d'accès à Internet – à conserver de six à vingt-quatre mois les métadonnées de connexion de leurs utilisateurs, et à les rendre disponible aux autorités de police[66].

Enfin, le renvoi préjudiciel permet de contourner l'impossibilité pour les particuliers de saisir eux-même la CJUE pour un recours en manquement contre un État-membre, en leur permettant de demander à la Cour de statuer sur l'invalidité d'un acte de droit national vis-à-vis du droit de l'Union. C'est ainsi qu'en 2011, deux groupes d'intérêt espagnols, l'*Asociación Nacional de Establecimientos Financieros de Crédito* (ASNEF) et la *Federación de Comercio Electrónico y Marketing Directo* (FECEMD), obtinrent de la CJUE une réponse à une question préjudicielle déclarant illégales des dispositions d'une loi nationale restreignant par rapport à la directive 95/46/CE la possibilité de recourir au motif de l'intérêt légitime du responsable du traitement pour traiter des données à caractère personnel[67].

C'est principalement à l'occasion de renvois préjudiciels que la CJUE a pu jouer un rôle dans la clarification de définitions de la directive 95/46/CE[68]. Dans un arrêt de 2018, elle a précisé au sujet de la notion de « fichier » que « [l]'article 2, sous c), de la directive 95/46 doit être interprété en ce sens que la notion de « fichier », visée par cette disposition, couvre un ensemble de données à caractère personnel collectées dans le cadre d'une activité de prédication de porte-à-porte, comportant des noms et des adresses ainsi que d'autres informations concernant les personnes démarchées, dès lors que ces données sont structurées selon des critères déterminés permettant, en pratique, de les retrouver aisément aux fins d'une utilisation ultérieure. Pour qu'un tel ensemble relève de cette notion, il n'est pas nécessaire qu'il comprenne des fiches, des listes spécifiques ou d'autres systèmes de recherche. » (CJUE 10 juillet 2018 « Jehovan todistajat », aff. C-25/17, §2).

64 Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique.

65 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

66 Voir : CJUE 8 avril 2014 « Digital Rights Ireland » Aff. C-293/12 et C-594/12.

67 CJUE 24 novembre 2011 « ASNEF et FECEMD » Aff. C-468/10 et C-469/10.

68 À l'heure de rédiger ces lignes, il est encore trop tôt pour avoir des jurisprudences sur le RGPD.

Plusieurs jugements de la CJUE portent sur des questions d'interprétation de la notion de « donnée à caractère personnel ». Le présent sous-chapitre est le fruit d'un travail de veille juridique sur les décisions de la CEDH et de la CJUE ayant un rapport avec le droit *de la* protection des données à caractère personnel, qui a donné lieu à la rédaction tenue à jour d'un guide de la jurisprudence européenne, dont une version a été publiée aux *Cahiers du COSTECH* (Rossi, 2017c). Nous avons sélectionné ici les affaires qui ont été l'occasion pour les parties à un procès devant la CJUE de défendre leur interprétation de la définition rédigée à l'article 2 sous a) de la directive 95/46/CE. L'essentiel de celles-ci ont précédé l'adoption du RGPD. Les débats pendant ces procès ont eu lieu soit avant soit en parallèle avec les « discussions » sur ce règlement. Ils permettent de comprendre l'état du droit et de la jurisprudence sur la définition de la notion de « donnée à caractère personnel » à ce moment-là, et d'établir ce qu'étaient à ce moment les marges d'incertitude juridique, c'est-à-dire les mots de la définition qui pouvaient encore donner lieu à des interprétations concurrentes sans que l'une d'entre elle n'ait été investie par la CJUE de l'attribut de « vérité » octroyé par « l'autorité de la chose jugée »[69].

Nous verrons que les débats juridiques devant la Cour se sont concentrés sur deux groupes de mots de la définition contenue dans la directive 95/46/CE : « toute information » et « identifiée ou identifiable […] directement ou indirectement ».

6.3.2. « Toute information … » : le rappel de la définition

Il n'existe pas, dans la Convention européenne des droits de l'Homme (Convention EDH), de droit distinct *à la* protection des données à caractère personnel. La Convention 108 a pour but de protéger le « droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant » (art. 1 de la Convention 108 du Conseil de l'Europe). Ainsi, pour la CEDH, les infractions au droit *à la* protection des données sont des infractions au droit *à la* vie privée protégé par l'article 8 de la Convention EDH[70], et le simple fait d'enregistrer des informations sur une personne constitue une ingérence[71] qui doit être « prévue par la loi », poursuivre un « objectif légitime » et être « nécessaire dans une société démocratique[72] ». Pour autant, la CEDH ne limite pas le champ des informations sur des individus dont la collecte constitue une ingérence à l'article 8 de la Convention EDH aux seules données portant sur la vie privée ou sur l'intimité. Dans un arrêt de 2000, qui précède les premières décisions de la CJUE sur le sujet, elle a ainsi rappelé que :

69 Selon l'adage latin : *res iudicata veritas est* : la chose jugée est vérité.
70 Voir : CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04, pt. 103.
71 Voir : CEDH 26 mars 1987 « Leander contre Suède » Req. 9248/81, pt. 48.
72 Voir : CEDH 26 mars 1987 « Leander contre Suède » Req. 9248/81 et CEDH 4 décembre 2008 « S. et Marper contre Royaume-Uni » Req. 30562/04 et 30566/04.

> « […] la mémorisation de données relatives à la « vie privée » d'un individu entre dans le champ d'application de l'article 8 § 1 [de la Convention EDH] […] A cet égard, elle souligne que le terme « vie privée » ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables ; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de « vie privée » […]. Cette interprétation extensive concorde avec celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, entrée en vigueur le 1er octobre 1985, dont le but est « de garantir, sur le territoire de chaque Partie, à toute personne physique (…) le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant » (article 1), ces dernières étant définies comme « toute information concernant une personne physique identifiée ou identifiable » (article 2) » (CEDH 16 février 2000, « Amann contre Suisse » Req. 27798/95, pt. 65)

Comme la CEDH, la CJUE a jugé que les informations qui portent sur des personnes physiques sont des données à caractère personnel indépendamment de la nature de leur contenu. Elle le justifie en partie en citant la jurisprudence de la CEDH à ce sujet, mais surtout, par le fait que le texte de la directive 95/46/CE ne laisse pas de marge d'interprétation à ce sujet :

> « […] il doit être considéré, d'une part, que le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel, reconnu par les articles 7 et 8 de la charte, se rapporte à toute information concernant une personne physique identifiée ou identifiable (voir, notamment, Cour eur. D. H., arrêts Amann c. Suisse du 16 février 2000, Recueil des arrêts et décisions 2000-II, § 65 […]) et, d'autre part, que les limitations susceptibles d'être légitimement apportées au droit à la protection des données à caractère personnel, correspondent à celles tolérées dans le cadre de l'article 8 de la CEDH » (CJUE 9 novembre 2010 « Volker et Eifert contre Hesse » Aff. C-92/09 et C-93/09, pt. 52)

> « La notion de «données à caractère personnel» employée à l'article 3, paragraphe 1, de la directive 95/46 englobe, conformément à la définition figurant à l'article 2, sous a), de celle-ci, «toute information concernant une personne physique identifiée ou identifiable». Cette notion comprend assurément le nom d'une personne joint à ses coordonnées téléphoniques ou à des informations relatives à ses conditions de travail ou à ses passe-temps. » (CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, pt. 24)

Enfin, la CJUE a bien insisté dans une décision de 2015 sur la distinction à opérer entre la notion de « donnée relative à la vie privée » du règlement 1049/2001/CE relatif à l'accès du

public aux documents des institutions de l'UE, et la notion de « donnée à caractère personnel » de la directive 95/46/CE et du règlement 45/2001/CE sur la protection des données[73]. Ce faisant, elle rejetait un moyen des associations ClientEarth et Pesticide Action Network Europe, qui faisaient valoir que « le fait pour un expert d'émettre, à titre professionnel, un avis scientifique ne relève pas de la notion de vie privée »[74], et se rangeait à l'opinion de l'avocat général Pedro Cruz Villalón, selon lequel :

> « Conformément à l'article 2, sous a), du règlement nº 45/2001, on entend par «données à caractère personnel» «toute information concernant une personne physique identifiée ou identifiable». En l'espèce, d'une part, les personnes concernées seraient identifiées dès que leur nom serait communiqué et, d'autre part, une certaine information les concernant serait en outre fournie, à savoir les observations concrètes qu'elles ont présentées dans un cas d'exercice de leur activité professionnelle. Les éléments définissant la notion de «données à caractère personnel» sont donc clairement réunis, car les observations présentées par les experts constituent une «information concernant une personne physique identifiée» ou, si l'on préfère, une information sur chacun de ces experts, parfaitement identifiés par leurs noms. » (Cruz Villalón, 2015, pt. 37)

Dans un autre arrêt daté de fin 2017, la CJUE a rappelé que la notion de donnée personnelle « n'est pas restreinte aux informations sensibles ou d'ordre privé, mais englobe potentiellement toute sorte d'informations, tant objectives que subjectives sous forme d'avis ou d'appréciations, à condition que celles-ci « concernent » la personne en cause[75] ».

Dans d'autres décisions, la CJUE a indiqué que les adresses IP[76], un registre de temps de travail[77], des images de personnes enregistrées dans le cadre d'un dispositif de vidéosurveillance[78], des copies d'examen[79] ou encore des métadonnées de communication[80] sont aussi des données à caractère personnel.

La façon dont l'article 2 sous a) de la directive de 1995 a été rédigé, qui parle clairement de « toute information », n'a donc pas permis à des stratégies de remise en cause devant la CJUE l'inclusion d'informations ne relevant pas de l'intimité ou de la vie privée des personnes

73 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 32.
74 CJUE 16 juillet 2015 « ClientEarth contre EFSA » Aff. C-615/13P, pt. 25.
75 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 34
76 CJUE 24 novembre 2011 « Scarlet contre SABAM » Aff. C-70/10, pt. 51
77 CJUE 30 mai 2013 « Worten contre ACT » Aff. C-342/12
78 CJUE 11 décembre 2013 « Frantisek Rynes » Aff. C-212/13, pt. 21 et CJUE 14 février 2019 « Sergejs Buivids » Aff. C-345/17, pt. 31
79 CJUE 20 décembre 2017 « Peter Nowak contre Data Protection Commissioner » Aff. C-434/16
80 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15, pts. 97-100

concernées dans la notion de « donnée à caractère personnel » de prospérer. Par contre, plusieurs affaires ont été l'occasion de revenir sur d'autres aspects de cette définition, qui laissent une plus grande marge de manœuvre à l'interprétation des parties.

6.3.3. « identifiée ou identifiable, directement ou indirectement » : les adresses IP sont-elles des données à caractère personnel ?

En 2011, la CJUE a été amenée à répondre à la question de savoir si des adresses IP sont des données à caractère personnel, comme le prétendait la société Scarlet, un fournisseur d'accès à Internet (FAI) belge qui souhaitait s'opposer à la demande de la Société belge des auteurs, compositeurs et éditeurs (SABAM) de mettre en place un système de filtrage des communications en *peer-to-peer* pour empêcher les échanges de fichiers portant atteinte au droit d'auteur[81]. L'un des arguments de Scarlet pour s'opposer à la demande de la SABAM était qu'un tel système impliquerait le traitement d'adresses IP et donc de données à caractère personnel, tout en contrevenant au le droit de l'UE *de la* protection des données à caractère personnel[82].

L'avocat général de la CJUE, dans ses conclusions, rappela que tant l'EDPS que le G29 avaient pris publiquement position pour qualifier les adresses IP de données à caractère personnel (Cruz Villalón, 2011, pt. 76). Il précisa aussi qu'« une adresse IP peut être qualifiée de donnée à caractère personnel dans la mesure où elle peut permettre l'identification d'une personne, par référence à un numéro d'identification où à tout autre élément qui lui soit propre » (Cruz Villalón, 2011, pt. 78). La SABAM n'a pas semblé contester ce point, et la CJUE a reconnu dans son arrêt que les adresses IP sont des données à caractère personnel[83].

Scarlet était un FAI. Ces derniers détiennent les informations permettant de lier l'adresse IP (statique ou dynamique) à l'utilisateur final. Mais qu'en est-il des responsables du traitement[84] qui contrôlent des données contenant des quasi-identifiants qui, croisés avec d'autres données auxquelles ils n'ont pas accès, permettraient d'identifier les personnes concernées ? En effet, dans de telles circonstances, ces données sont, *de facto*, anonymes pour *ce* responsable du traitement, même si, dans l'absolu, elles ne sont *de facto* que pseudonymes. Mais alors, *de jure*, sont-elles anonymes, ou bien personnelles ?

81 CJUE 24 novembre 2011 « Scarlet contre SABAM » Aff. C-70/10.
82 CJUE 24 novembre 2011 « Scarlet contre SABAM » Aff. C-70/10, pt. 26.
83 CJUE 24 novembre 2011 « Scarlet contre SABAM » Aff. C-70/10.
84 Pour rappel, il s'agit des personnes physiques ou morales qui déterminent les moyens et les finalités des traitements de données à caractère personnel, incluant la collecte, la conservation, la modification et de façon générale l'exploitation de ces données.

Les adresses IP dynamiques, par contraste avec les adresses IP statiques, ne sont attribuées que pour une durée déterminée. Une même adresse IP dynamique peut être associée à des équipements différents au cours du temps. Elle est réaffectée dynamiquement en fonction des besoins. Elle n'identifie donc pas toujours le même appareil.

Selon le point de vue objectif, ou absolu, une adresse IP dynamique est nécessairement une donnée à caractère personnel à partir du moment où il existe, quelque part, des données qui peuvent être utilisées par recoupement pour identifier la personne détenant l'appareil qu'elle identifie à un instant donné. Mais selon le point de vue relatif, cette adresse n'est une donnée à caractère personnel que pour les responsables du traitement qui détiennent toutes les informations requises pour ré-identifier la personne, même si cela demanderait un effort conséquent de sa part (Zuiderveen Borgesius, 2017).

En 2016, la CJUE a été saisie pour une affaire qui concernait l'enregistrement par des sites web des adresses IP des internautes les visitant[85]. À l'inverse de Frederik Zuiderveen Borgesius (2017), il nous semble que la CJUE a plutôt plutôt tranché dans cette affaire en faveur du point de vue relatif. Elle précisa en effet que pour déterminer si une adresse IP dynamique était une donnée à caractère personnel *du point de vue d'un site web*, il fallait que son fournisseur dispose « des moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet »[86].

Fin 2017, dans un arrêt qui a permis de confirmer que les copies d'examen sont des données à caractère personnel susceptibles d'être l'objet de l'exercice d'un droit d'accès par des personnes concernées[87], la CJUE a semblé adopter une position objective, en affirmant qu'« il n'est pas requis que toutes les informations permettant d'identifier la personne concernée se trouvent entre les mains d'une seule personne »[88]. Mais elle n'a pas indiqué ce qu'il se passait lorsque la personne qui détient une partie des données nécessaire à l'identification n'a pas le droit de demander à l'autre personne détenant l'autre partie de la lui communiquer. Est-ce qu'il s'agit toujours de données à caractère personnel ?

Notons que comme ces deux derniers jugements, en 2016 et 2017, ont été prononcés après l'adoption définitive du RGPD, ils apportent des éléments de précision qui n'ont pas pu être pris en compte dans les « discussions » sur le RGPD entre 2009 et 2016.

85 CJUE 19 octobre 2016 « Breyer contre Allemagne » Aff. C-582/14.
86 CJUE 19 octobre 2016 « Breyer contre Allemagne » Aff. C-582/14, pt. 49.
87 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16.
88 CJUE 20 décembre 2017 «Peter Nowak contre Data Protection Commissioner» Aff. C-434/16, pt. 31.

6.3.4. Conclusion partielle sur la jurisprudence de la CJUE sur la notion de « donnée à caractère personnel »

La CJUE a été le lieu d'une mise en débat de la notion de « donnée à caractère personnel ».

Dans ce cadre, elle a rappelé que sa définition, telle que rédigée dans la directive de 1995, ne permettait pas de l'interpréter dans un sens qui exclurait de son champ les informations ne relevant pas de la sphère privée ou de l'intimité des personnes.

Elle a également rappelé que, textuellement, elle s'applique aux données concernant une personne physique « identifiée ou identifiable […] directement ou indirectement » (art. 2 sous a) de la directive 95/46/CE). Dès lors, les données pseudonymes, c'est-à-dire ne contenant pas de données directement identifiantes comme le nom de la personne, mais, par exemple, un numéro d'identification, ou l'empreinte unique mais irréversible du nom, peuvent entrer dans le champ de cette définition. Une donnée est à caractère personnel dès lors que le responsable du traitement est en mesure de ré-identifier la personne, même indirectement. Mais la jurisprudence est moins tranchée sur le point de savoir si une donnée est à caractère personnel lorsque c'est un tiers qui, potentiellement, peut retrouver « directement ou indirectement » la personne physique « identifiable ».

Cela contribue à expliquer les tentatives des deux coalitions rivales des « discussions » sur le RGPD[89] de s'assurer de l'inclusion d'une rédaction de la définition tranchant le débat entre approche absolue ou relative dans un sens favorable à leurs intérêts.

6.4. Les débats sur la définition de « donnée à caractère personnel » à inclure dans le texte du RGPD

6.4.1. La proposition initiale de la Commission européenne

Nous avons déjà vu dans le chapitre 4 que la définition de la notion de « donnée à caractère personnel » a été l'un des principaux points de controverse des « discussions » sur le RGPD[90]. Cela était notamment la conséquence du fait que ce dernier allait s'appliquer « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier » (art. 2 du RGPD). Toucher à la définition de cette notion centrale du RGPD, c'était donc en étendre ou, au contraire, en restreindre le champ d'application territorial. Modifier la définition dans le texte même de la Loi, c'était s'assurer de décisions administratives et

89 Cf. section 4.2.
90 Cf. section 4.3.4.

judiciaires qui ne pourront s'inscrire que dans le champ des interprétations rendues possibles par ce texte, et aussi profiter d'une fenêtre d'opportunité pour remettre en cause des décisions jurisprudentielles fondées sur des formulations antérieures désormais abrogées.

La proposition initiale de la Commission simplifiait la notion de « donnée à caractère personnel » pour la faire dépendre de celle de la notion de « personne concernée[91] ». S'il s'agit d'une modification importante sur la forme, elle reprenait sur le fond la définition contenue dans la directive de 1995, qui elle-même s'inspirait de celle de la Convention 108, tout en apportant quelques précisions tendant à encourager une interprétation conforme à la conception absolue de la notion. Cela devait notamment servir à garantir l'inclusion des activités de marketing personnalisé en ligne dans le champ d'application matériel de la directive (Zuiderveen Borgesius, 2016).

Le tableau ci-dessous montre les différences entre la définition de la directive 95/46/CE et la proposition initiale de la Commission de définition de la notion de donnée personnelle dans le RGPD :

Définition de 1995 (art. 2)	**Définition à l'art. 4 de la proposition initiale de RGPD de la Commission européenne**
a) «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;	**(1) «personne concernée»:** une personne physique identifiée **ou une personne physique qui peut être identifiée**, directement ou indirectement, **par des moyens *raisonnablement* susceptibles d'être utilisés par le responsable du traitement *ou par toute autre personne physique ou morale***, notamment par référence à un numéro d'identification, **à des données de localisation, à un identifiant en ligne** ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, **génétique**, psychique, économique, culturelle ou sociale ; **(2)** «données à caractère personnel»: toute information se rapportant à une personne concernée ;

Tableau 16 : *Comparaison entre les définitions de la notion de donnée à caractère personnel dans la directive 95/46/CE et dans la proposition initiale de RGPD de la Commission européenne*

91 Cf. annexe 2.

La délégation française au Conseil, en plus de se dire défavorable à cette inversion de l'ordre de présentation des notions de « donnée à caractère personnel » et de « personne concernée » (Conseil de l'UE, document 9897/12, p. 60), souligna l'importance sémantique de la proposition soulignée dans le tableau ci-dessus, qu'elle jugeait indésirable :

> « Sur le paragraphe (1), qui définit la « personne concernée », la délégation française s'interroge sur l'inclusion de personnes physiques qui pourraient être identifiées par des « moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale ».
>
> Cette extension par rapport à la directive 95/46/CE est une source d'incertitude juridique et elle s'apparente à une extension bien trop large du champ d'application, puisque l'usage qui pourrait être fait par « toute autre personne physique ou morale » d'information qui ne serait pas « identifiante » pour le responsable du traitement lui-même devrait alors être prise en compte[92]. » (Conseil de l'UE, document 9897/12, p. 60)

Les mots « par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale », conservés au considérant 26 de la version finale adoptée en 2016, allaient en effet ancrer la définition dans une perspective absolue, que seul l'adverbe « raisonnablement » – qui laissait finalement un large éventail d'interprétations au régulateur et au juge – venait nuancer.

6.4.2. « *Singling out* » : la proposition d'amendement de European Digital Rights

Les défenseurs de la vie privée étaient favorables à l'adoption d'une définition aussi absolue que possible de la notion de « donnée à caractère personnel ». Le but était de s'assurer de l'inclusion, dans le champ d'application du droit *de la* protection des données, des données qui, même si elles n'intéressent pas le responsable du traitement pour son rapport à un individu identifié, pourraient permettre – même indirectement et même à un autre – de remonter à l'individu en question. Il s'agit donc d'une prise en compte de la difficulté technique à parvenir à

92 Traduction de l'auteur. Texte original : « On point (1), which defines the "data subject", the French delegation wonders about the inclusion of natural persons who may be identified "by means reasonably likely to be used by the controller or by any other natural or legal person".
This extension by comparison with Directive 95/46/EC is a source of legal uncertainty and would appear to be much too broad an extension of the scope, since the use which "any other natural or legal person" might make of information which would not be "identifying" for the controller himself would then have to be taken into account. »

ce que Paul Ohm a défini comme un anonymat « robuste », absolument irréversible pour qui que ce soit (Ohm, 2010). Il s'agissait aussi de s'assurer de l'inclusion de techniques de ciblage dans laquelle le but n'est pas tant d'identifier les personnes concernées que d'être en mesure de les distinguer de la masse de données, pour agir sur elles, par exemple pour leur faire parvenir de la publicité personnalisée.

Dans son avis n° 4 de 2007 sur le concept de données à caractère personnel, le G29 avait écrit qu'une personne est selon lui identifiable au sens de la définition de la notion de « donnée à caractère personnel » y compris lorsque, bien que n'étant pas « identifiée », il est possible de la « distinguer » (en anglais : « *to single out* ») à partir des données en question :

> « […] il convient de relever que si l'identification ou le nom constitue, dans la pratique, le moyen le plus répandu, un nom n'est pas toujours nécessaire[93] pour identifier une personne, notamment lorsque d'autres « identifiants » sont utilisés pour distinguer quelqu'un[94]. » (G29, 2007, p. 15)

Dans l'avis 16/2011 sur le code de bonnes pratiques de l'AEEP et de l'IAB en matière de publicité comportementale en ligne, le G29 a rappelé sa position en utilisant à nouveau une forme conjuguée du verbe « *to single out* », traduite cette fois-ci dans la version française de l'avis par « différenciation » :

> « L'utilisation de ces identifiants uniques permet le suivi des utilisateurs d'un ordinateur donné, et ce même lorsque les adresses IP sont supprimées ou rendues anonymes. En d'autres termes, ces identifiants uniques permettent une « différenciation » des personnes concernées aux fins du suivi de la navigation de l'utilisateur sur différents sites internet et, partant, constituent des données à caractère personnel. » (G29, 2011, p. 9)

D'autres avis du G29 montrent que la doctrine des autorités de protection des données de l'UE était favorable à l'approche absolutiste de la définition de la donnée à caractère personnel (G29, 2010 et 2014b).

Pour les défenseurs de la vie privée, le verbe « *to single out* » utilisé dans ce contexte signifie être capable, dans un jeu de données, d'isoler les éléments qui se rattachent à une même personne des autres, sans que l'on cherche à identifier cette personne :

93 Surligné dans le texte d'origine.
94 *Idem*

> « […] distinguer [*singling out*] une personne implique d'identifier cette personne, même si le responsable du traitement ne peut pas lier de nom à la donnée qu'il traite au sujet d'un individu[95]. » (Zuiderveen Borgesius, 2016, p. 7 [sous presse])

> « C'est tout traitement de données personnelles d'une manière qui pourrait permettre à un individu d'être identifié comme un individu disposant de certaines caractéristiques, à l'inverse d'un individu avec un nom[96]. » (Entretien avec Joe McNamee)

Comme nous venons de le voir avec des exemples tirés de deux avis du G29, ce terme a pu être traduit par « identification » ou « différenciation » de la personne, mais nous trouvons aussi « individualisation » (G29, 2015, p. 5) ou encore « ciblage » (cons. 26 du RGPD). Pour faciliter la lecture, nous utiliserons donc les mots anglais pour désigner cette expression.

Pour s'assurer que même les données qui ne permettent que de « *single out* » un individu soient couvertes par la définition de la notion de « donnée à caractère personnel », la coalition des défenseurs de la vie privée a proposé d'inclure ce verbe dans la définition même cette notion dans le RGPD. L'ONG *Bits of Freedom* proposa par exemple l'amendement suivant à la définition de « personne concernée » contenue dans la proposition de la Commission européenne, de laquelle devait initialement dépendre celle de « donnée à caractère personnel » :

Proposition de définition originale	**Proposition de *Bits of Freedom***
'Data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably to be likely to be used by the controller or any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical,	'Data subject' means an identified natural person or a natural person who can be identified **or singled out**, directly or indirectly, by means reasonably to be likely to be used by the controller or any other natural or legal person, in particular by reference to an identification number **or a unique identifier**, location data, online identifier or to one or

95 Traduction de l'auteur. Texte original : « […] singling out a person implies identifying this person, even if the data controller cannot tie a name to the data it processes about an individual. »

96 Traduction de l'auteur. Texte original : « It's any processing of personal data in a way which could allow an individual to be identified as an individual with certain characteristics, as opposed to an individual with a name. »

physiological, genetic, mental, economic, cultural or social identity of that person[97]	more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

Tableau 17 : *Proposition d'amendement de* Bits of Freedom *de la notion de « personne concernée ». Amendement 24, page 12 du document Amendments DP Regulation Bits of Freedom.pdf (corpus Lobbyplag, BITSOFFREEDOM1)*

EDRi proposa un amendement similaire (Corpus Lobbyplag, EDRI2, 2012, amendement 63, p. 49), que l'ONG justifiait par l'argument des avancées techniques qui permettraient de ré-identifier de plus en plus facilement des jeux de données pourtant en apparence anonymes ou anonymisés :

> « Pour garantir une bonne protection, il est important que les termes « données à caractère personnel » et « personne concernée » ne soient pas définis de façon trop étroite. Le règlement devrait clairement s'appliquer aux données qui ne permettent que « la différenciation » [*singling out*] et il devrait être clair que les identifiants en-ligne doivent dans la plupart des cas être considérés comme des données à caractère personnel. Comme la technologie avance en permanence, les attaques de ré-identification [*de-anonymisation attacks*] vont devenir de plus en plus sophistiquées. Disposer d'une définition ample des « données à caractère personnel » et des « personnes concernées » est important pour garantir une protection efficace à long-terme dans le futur [*future-proof protection*][98]. » (Corpus Lobbyplag, EDRI2, 2012, p. 50)

Pour Joe McNamee, d'EDRi, la chose se justifiait sur le plan moral par le fait que même si, selon certaines définitions, la vie privée, l'intimité, ou le droit d'être laissé tranquille de la personne n'est pas atteint par les méthodes de ciblage non-identifiantes, l'application de telles techniques à la publicité comportementale affecte les personnes concernées par sa visée manipulatrice :

97 Traduction officielle en français : « «personne concernée»: une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ; »

98 Traduction de l'auteur. Texte original : « To ensure good protection, it is important that the terms 'personal data' and 'data subject' are not defined too narrowly. The Regulation should clearly apply to data that only allow 'singling out' and it should be clear that online identifiers should in most cases be considered personal data. Since technology is steadily advancing, de-anonymisation attacks will become more sophisticated. Having wide definitions of 'personal data' and 'data subject' is important for future-proof protection. »

« Je pense que ce concept a eu du succès. Pourquoi est-il important ? Si vous regardez le scandale de Facebook au sujet des élections […] : cela n'a pas d'importance de savoir que M. Smith, ici, est de 5 River Street dansle Minnesota et M. Smith de 5 River Street. Mais le problème est la capacité à l'identifier comme quelqu'un de susceptible de recevoir ce message, et d'être manipulable non pas sur la base de qui il est, mais de ce qu'il est. […] Imaginez si vous pouvez être distingué [*singled out*] et manipulé sans votre consentement ou à votre insu, et que cela n'était même pas pris en compte dans le droit de la protection des données [*this wasn't even a concept that data protection law would cover*]. Ce serait ridicule[99] ! » (Entretien avec Joe McNamee)

« Il y a un lobby qui est tout à fait sympathique à l'idée que manipuler des gens et les distinguer [*singling out*] pour un traitement particulier serait une bonne chose[100]. » (Entretien avec Joe McNamee)

En 2015, dans une annexe à des courriers adressés au représentant permanent de la Lettonie, pays en charge de la présidence tournante du Conseil, à Jan Philipp Albrecht, rapporteur du RGPD, et à Věra Jourová, commissaire européenne à la justice, en vue du trilogue, le G29 insista à son tour sur la nécessité selon lui d'inclure les termes « *to single out* » dans la définition :

« Une personne physique est considérée comme identifiable lorsque, au sein d'un groupe de personnes, elle peut être distinguée des autres et, par conséquent, faire l'objet d'un traitement différent. Autrement dit, la notion d'identifiabilité devrait inclure l'individualisation des particuliers.

Le groupe de travail est favorable à l'insertion d'un considérant précisant que la capacité d'individualiser la personne concernée et de la soumettre à un traitement différent est un moyen de l'identifier. » (G29, 2015, p. 5)

La combinaison entre la lecture de la définition à l'article 4 du RGPD, qui porte toujours sur les données relatives à des personnes physiques y compris identifiables indirectement, et celle de l'article 22, qui encadre le profilage et les décisions automatisées, semble satisfaire Joe

99 Traduction de l'auteur. Texte original : « I think it was successful as a concept. Why is it important? If you look at the Facebook scandal around the […] elections: there is no value in knowing that Mr. Smith here is from 5 River Street, Minnesota, is called Mr. Smith from 5 River Street. But the matter is the ability to identify him as somebody susceptible to receiving this message, and being manipulable on the basis of not who he is, but what he is. […] Imagine if you could be singled out and manipulated without your consent or knowledge, and if this wasn't even a concept that data protection law would cover. How ridiculous would that be? » (Entretien avec Joe McNamee).

100 Traduction de l'auteur. Texte original : « There is a lobby that is quite friendly to the notion that manipulating people and singling out people for a particular treatment would be a good thing. »

McNamee. Selon lui, l'objectif d'inclure sans autre interprétation possible la publicité comportementale dans le champ d'application matériel du RGPD a été atteint malgré l'échec de la proposition de la coalition de la « *privacy community* » d'inclure le verbe « *to single out* » directement dans la définition de la notion de « donnée à caractère personnel » :

> « Si vous prenez […] les définitions de concepts clef et les définitions des bases légales pour les traitements, et le droit d'opposition, et, dans une mesure qui ne me satisfait pas, l'article sur le profilage, alors vous aboutissez […] probablement à suffisamment de protection pour garantir que l'identification [*singling out*] est en fait bel et bien quelque chose de pris en compte [*is covered*] jusqu'à un certain point[101]. » (Entretien avec Joe McNamee)

6.4.3. L'« approche fondée sur le risque », l'anonymisation et la pseudonymisation

La coalition industrielle était opposée à l'introduction des mots « *single out* » proposée par les défenseurs de la vie privée et, de façon générale, à une interprétation absolue de la notion de donnée à caractère personnel, qui serait trop large et couvrirait trop d'objets :

> « L'un des principaux problèmes avec tout ce débat était d'essayer de définir la donnée à caractère personnel. Parce que c'est souvent une zone grise, vous savez… Tellement, je crois, que la proposition initiale était très restrictive et couvrait beaucoup de domaines dans lesquels il y avait des inquiétudes que ça finirait même par s'immiscer dans les transmissions de données de machine à machine[102] […] » (Entretien Euro5)

Ainsi, dès 2008, soit l'année ayant précédé le début des « discussions » sur le RGPD, Google avait publié un billet de blog émettant des doutes sur le fait que toutes les adresses IP soient des données à caractère personnel, indiquant que dans bien des cas, une personne détenant une adresse IP ne dispose pas des autres informations nécessaires l'identification de la personne à l'origine des paquets auxquels se cette adresse est attachée (Whitten, 2008).

---

101 Traduit de l'anglais. Texte original : « If you take […] the definitions of key concepts and the definitions on the legal bases for processing, and the right to object, and to an extent that I'm not very happy with, the profiling article, you end up with […] probably enough protection to ensure that singling out is in fact something that is covered to some extent. »

102 Traduction de l'auteur. Texte original : « One of the issues with this whole debate was trying to define personal data. Because it's often a grey zone, you know… So much, I think, the initial proposal was really very restrictive and encompassing a lot of areas whereas there were some concerns that it was almost creeping into machine-to-machine data […] ».

En 2013, l'AmCham EU a proposé une formulation qui définissait un test d'identifiabilité relatif au responsable du traitement, et excluait les données que ce dernier n'était normalement pas en mesure de ré-identifier du champs des « données à caractère personnel » :

2. Definition of personal data / Processing for security and anti-abuse purposes

Proposal for a regulation
Article 4, Paragraphs 1, 2 and *2a, 2b (new)*

Text proposed by the Commission	*AmCham EU Amendment*
(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means ***reasonably likely to be used by*** the controller ***or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;***	(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means ***available in the effective control of*** the data controller ***and as part of a specific processing operation in its regular course of business in a way that permits the controller to confirm the identity of the data subject with any appropriate means;***
(2) 'personal data' means any information relating to a data subject;	(2) 'personal data' means information relating to a data subject ***that makes identification by the controller reasonably possible;***

Figure 43 : *Proposition d'amendement de l'AmCham EU aux définitions des notions de « personne concernée » et de « donnée à caractère personnel » (extrait de : Corpus Lobbyplag, document AMCHAMEU1, 2013, p. 11)*

L'un des principaux arguments utilisés par la coalition industrielle était que la définition absolue de la notion de « donnée à caractère personnel » ne correspondrait pas à la « réalité technique », et, ce faisant, entraînerait des coûts importants nuisibles à la croissance économique (Zuiderveen Borgesius, 2016)[103]. Le modèle économique de nombreux services en ligne – ou « services de la société de l'information » selon les termes de la directive 98/34/CE[104] alors en vigueur – était en effet basé sur l'affichage de publicité comportementale.

103 Cf. section 4.4.

104 Directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques. Voir également la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur

Pour défendre ce modèle économique en le soustrayant au champ d'application matériel du RGPD, la coalition industrielle avait obtenu l'insertion de considérants affirmant que les responsables du traitement pourraient se passer du consentement de la personne pour effectuer du ciblage publicitaire sur la base de données pseudonymes et non directement identifiantes dans la version du RGPD issue du premier rapport de la commission LIBE[105]. Cette disposition n'a toutefois pas trouvé sa place dans le texte définitif adopté en avril 2016 (Zuiderveen Borgesius, 2016, p. 12 [sous presse]).

Un autre élément central dans la stratégie argumentative de la coalition industrielle était l'idée d'« approche basée sur le risque[106] ». En réponse à la consultation de 2009 de la Commission européenne, la *Direct Marketing Association* britannique a décrivait en ces termes la définition de la notion de « donnée à caractère personnel » de la directive de 1995 :

> « La définition des données personnelles dans la directive est peut-être trop large, dans le sens où elle capture parfois des cas marginaux par inadvertance. […] Il serait probablement une bonne idée d'introduction un critère de risque de préjudice à la définition[107]. » (Consultation de 2009, document DMA1, 2009, p. 3)

L'idée était donc d'avoir une définition qui permette de soustraire du champ des « données à caractère personnel » des cas « sans risques ». La remise en cause l'inclusion dans ce champ de « toutes » les données, et pas uniquement les données relevant de l'intimité ou de la sphère privée, aurait aussi pu être revendiquée au nom de cet objectif. Nous n'avons cependant pas trouvé de trace d'une telle tentative dans les documents du corpus formulant une proposition de définition que nous avons lus. Cela pourrait s'expliquer par le fait que cet aspect semble plus solidement ancré, à la fois dans le texte de la définition et dans la jurisprudence de la CJUE, que la question de son caractère relatif ou absolu. De plus, un argumentaire consistant à dire que seules les données relevant de la protection de la vie privée, et donc de l'article 7 de la Charte des droits fondamentaux de l'UE, sans tenir compte de son article 8 qui protège les données à caractère personnel *en général*, aurait été juridiquement périlleux. Enfin, il existait déjà une différentiation entre les données à caractère personnel en général et celles qui, étant donné leur contenu, étaient de nature plus « sensible » (art. 8 de la directive 95/46/CE, art. 9 du RGPD).

105 Considérants 38 et 58a de la proposition de RGPD telle qu'amendée en première lecture par le Parlement européen.

106 Cf. section 4.3.5.

107 Traduction de l'auteur. Texte original en anglais : « The definition of personal data in the Directive is possibly too broad in that it sometimes inadvertently captures marginal cases. […] It might be a good idea to introduce a risk of harm criteria to the definition. »

Plusieurs groupes d'intérêt de la coalition industrielle, dont la *Business Software Alliance* et l'ICDP, ont donc plutôt axé leur stratégie sur la proposition, dès avant la publication de la Commission, d'un nouveau concept : la « donnée pseudonyme ». Selon l'ICDP, son introduction dans le texte de ce qui allait devenir le RGPD devait concrétiser l'objectif évoqué dans le courrier de la *Direct Marketing Association* que nous venons de citer :

> « L'une des possibilités pour traiter ces aspects pourrait être l'introduction d'une définition harmonisée de donnée personnelle indirecte ou pseudonyme, qui pourrait bénéficier de règles de protection des données allégées, étant donné que le traitement de ce type de données présente habituellement des risques très bas pour la vie privée[108]. » (Corpus Lobbyplag, document ICDP1, 2011, p. 5)

L'entreprise Yahoo! a rédigé un *policy paper* spécifique pour argumenter en faveur de l'introduction d'une définition de la donnée « pseudonyme ». Il y est écrit qu'en plus des catégories de « donnée à caractère personnel » et de « données sensibles », « les services de la société de l'information a de plus en plus cherché à trouver de nouvelles formes de données pour mener à bien des activités utiles qui peuvent profiter de qualités « d'unicité » sans avoir besoin de connaître « l'identité »[109]. » (Corpus Lobbyplag, document YAHOO1, 2012, p. 1). Le document précise bien que les données pseudonymes peuvent permettre de distinguer[110] une personne unique d'un jeu de données, mais prétend que les risques associés sont moindres qu'en cas de donnée directement identifiante, et que les bénéfices économiques et sociétaux de leur utilisation à des fins statistiques seraient importants. Il s'agit aussi, en creux, mais de façon tout à fait nette, d'arguments développés pour contrer la proposition des défenseurs de la vie privée concernant l'inclusion dans la notion de « donnée à caractère personnel » des données qui permettent de « *single out* » quelqu'un. En effet, Yahoo! proposait d'inscrire aux considérants 23 et 24 de la proposition initiale que les principes de la protection des données ne devraient pas s'appliquer en présence de données « pseudonymes » ou « rendues anonymes de telle sorte que la personne concernée ne peut plus être identifiée » (le document utilise les deux formulations en les utilisant de façon interchangeable) (Corpus Lobbyplag, document YAHOO1, 2012, p. 1).

---

108 Traduction de l'auteur. Texte original en anglais : « One possibility to deal with these aspects could be to introduce a harmonised definition of indirect or pseudonymous personal data that could benefit from lighter data protection requirements as the processing of such type of data usually present very low risks to privacy. »
Notons que la formulation retenue dans cette lettre rappelle de très près le contenu du texte d'un *position paper* de l'ICDP de 2011 (voir : Corpus Lobbyplag, ICDP1, 2011, p. 5).

109 Traduction de l'auteur. Texte original en anglais : « […] information society services have increasingly looked to new forms of data to carry out useful activities that can leverage 'uniqueness' without having to know 'identity'. »

110 Le verbe « *to single out* » n'est pas utilisé, mais lorsque le document parle d'« unicité » (« *uniqueness* »), c'est bien de personnes qui ont été « *singled out* » dans un jeu de données indirectement identifiant qu'il s'agit concrètement.

Cette proposition suscita la méfiance d'autres acteurs, dont Viviane Reding, la commissaire en charge du dossier, qui prit le soin de préciser dans l'un de ses discours que, pour elle :

> « Les données pseudonymes ne doivent pas devenir un cheval de Troie au cœur du Règlement, permettant la non-application de ses dispositions[111]. » (Reding, 2014)

Le rapport de la commission LIBE proposa finalement l'insertion d'une définition de la notion de « pseudonymisation ». Les défenseurs de la vie privée s'y montrèrent finalement favorables, rejoignant en surface les positions de la coalition industrielle. Le contenu qu'ils ont donné à sa définition était toutefois l'inverse de ce qu'auraient souhaité les « lobbies », puisqu'il rattache fermement les données pseudonymes, c'est-à-dire dont les identifiants directs comme un nom ont été ôtés, à la notion de « donnée à caractère personnel » :

> « 5) «pseudonymisation», **le traitement de données à caractère personnel**[112] de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable » (art. 4 du RGPD)

Pour le G29, la « pseudonymisation » devait même être définie de sorte à en faire une obligation supplémentaire, au lieu d'en faire un critère d'abaissement du niveau d'exigences comme le demandaient les acteurs de la coalition industrielle (G29, 2012a, p. 12). C'est de fait ce dont dispose la version adoptée en lecture définitive du RGPD.

6.4.4. Le compromis inscrit dans le RGPD

Conformément aux vœux de la coalition industrielle, une définition de la « donnée pseudonyme » a donc été insérée dans le texte final du RGPD. Mais, comme le dit Frederik Zuiderveen Borgesius, le RGPD « traite la pseudonymisation surtout comme une mesure de sécurité »[113] (Zuiderveen Borgesius, 2016, p. 12 [sous presse]), et comme nous venons de le voir, le contenu de la définition de cette nouvelle notion la définissant comme faisant partie de

111 Traduction de l'auteur. Texte original en anglais : « pseudonymous data must not become a Trojan horse at the heart of the Regulation, allowing the non-application of its provisions. »

112 Texte mis en gras par l'auteur.

113 Texte original : « treats pseudonymisation primarily as a data security measure ».

l'ensemble plus général de la définition de « donnée à caractère personnel », cela renforce *in fine* le caractère absolu de cette dernière.

Une autre différence par rapport à la proposition initiale de la Commission est que, conformément aux souhaits des délégations française[114], slovaque[115] et britannique[116], les définitions de « donnée à caractère personnel » et « personne concernée » ont finalement été rétablies dans l'ordre de présentation de la directive 95/46/CE. Les principales différences entre la définition de 1995 et la définition définitive dans le RGPD sont mises en valeur ci-dessous :

Définition de 1995 (art. 2)	**Définition du RGPD (art. 4)**
a) «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;	1) «données à caractère personnel», toute information **se rapportant à** une personne physique identifiée ou identifiable (**ci-après dénommée** «personne concernée»); est réputée être **une «personne physique** identifiable» **une personne physique qui** peut être identifiée, directement ou indirectement, notamment par référence **à un identifiant, tel qu'un nom,** un numéro d'identification**, des données de localisation, un identifiant en ligne,** ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, **génétique**, psychique, économique, culturelle ou sociale;

Tableau 18 : *Comparaison entre la définition de la notion de « donnée à caractère personnel » dans la directive 95/46/CE et dans la version adoptée en lecture finale du RGPD*

Enfin, le considérant 26 de la proposition évoque les cas de données qui permettent de « *single out* » une personne :

> « Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, **il convient de**

114 Voir : Position française, Conseil de l'UE, 2012, document 9897/12, p. 60.
115 Voir : Position slovaque, Conseil de l'UE, 2012, document 9897/12, p. 95.
116 Voir : Position britannique, Conseil de l'UE, 2012, document 9897/12, p. 117.

prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, **tels que le ciblage**. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche. »[117] (considérant 26 du RGPD)

Ce considérant, en utilisant dans sa version anglaise le verbe « *to single out* », répond à l'une des revendications de la coalition des défenseurs de la vie privée, sans pour autant l'intégrer à la définition même de la notion de « donnée à caractère personnel » dans un article du règlement. Or, les considérants n'ont pas la même densité juridique qu'un article. Seuls les articles créent des droits et obligations en droit positif. Toutefois, ils sont complémentaires aux articles et viennent leur apporter des précisions. Il est nécessaire de prendre en compte l'article et les considérants qui le complètent pour interpréter une disposition d'un texte législatif de l'Union (Klimas et Vaičiukaitė, 2008). En ce sens, l'inclusion dans un considérant qui peut éclairer l'interprétation de la définition de la notion de « donnée à caractère personnel » à l'article 4 du RGPD est une forme de demie-victoire pour la revendication de la coalition des défenseurs de la vie privée.

En conclusion de cette étude des controverses définitionnelles sur la notion de « donnée à caractère personnel » au cours des « discussions » sur le RGPD, nous pouvons affirmer que les groupes d'intérêt se sont avant tout positionnés sur le débat entre une conception absolue et un conception relative de la définition de la notion de donnée à caractère personnel. La coalition industrielle favorisait une définition visant à exclure les données pour lesquelles un responsable du traitement n'est pas en capacité d'identifier facilement la personne concernée avec les seuls éléments à sa disposition. Cela visait entre autres, tout comme la volonté d'inclure une définition de la donnée pseudonyme, à exclure clairement du champ d'application du RGPD les activités de marketing ciblé (Zuiderveen Borgesius, 2016), qui sont au cœur du modèle économique du Web (Zuboff, 2018). Les défenseurs de la vie privée, eux, ont demandé à ce qu'il soit clairement

117 Dans la version française de ce considérant, le mot « ciblage » traduit les termes présents dans la version anglais de « *singling out* ». Le verbe « *to single out* », que ce soit à l'infinitif ou dans une forme conjuguée, était absent de la directive 95/46/CE.

inscrit dans le texte du RGPD que le simple fait qu'une donnée soit capable « d'isoler » (« *to single out* ») une personne physique particulière dans un jeu de données soit suffisant pour la qualifier de donnée à caractère personnel, justement afin de s'assurer que toutes les activités de profilage et de marketing ciblé soient dans le champ d'application matériel du droit *de la* protection des données à caractère personnel et que le débat entre une définition relative et une définition absolue de la notion de donnée à caractère personnel soit enfin tranché de façon claire en faveur de la conception absolue.

Alors que la « discussion » sur le RGPD était en cours dans le sous-système de politiques publiques de l'UE dédié à la protection des données, les participants au *Privacy Interest Group* (PING) et au *Tracking Protection Working Group* (TPWG) du W3C travaillaient à l'élaboration de standards techniques protecteurs de la « vie privée ». Nous nous sommes demandé si leurs travaux se basaient sur la même définition de la notion de « donnée à caractère personnel » que celle du RGPD.

6.5. La reprise de la notion de donnée à caractère personnel dans les discussions issue du droit européen par le W3C

Les acteurs du W3C interrogés ont dans leur grande majorité exprimé l'idée que le droit n'avait pas d'influence directe sur leur travail de standardisation. Pourtant, des arguments juridiques ont bel et bien été échangés dans le cadre de discussions au sein du *Tracking Protection Working Group* (TPWG) et du *Privacy Interest Group* (PING)[118]. Le schéma ci-dessous montre en outre une augmentation en occurrences absolues de l'emploi des termes « *data protection* » (protection des données) et « *personal data* » (donnée personnelle) dans les échanges de courriels sur les listes de diffusion *public-tracking* et *public-privacy* du W3C. Cette augmentation devient notable à partir de janvier 2012, date de publication de la proposition de RGPD de la Commission européenne :

118 Cf. section 5.6.4.

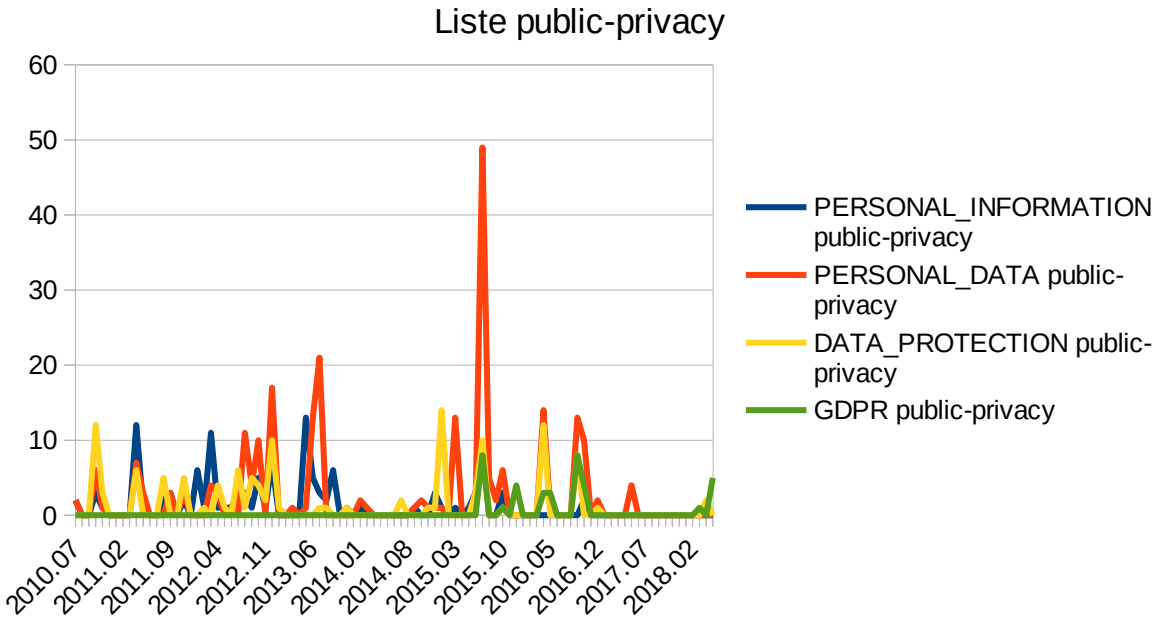


Figure 44 : *Évolution en nombre d'occurrences absolues de l'emploi de certains mots dans la liste de discussion* public-privacy

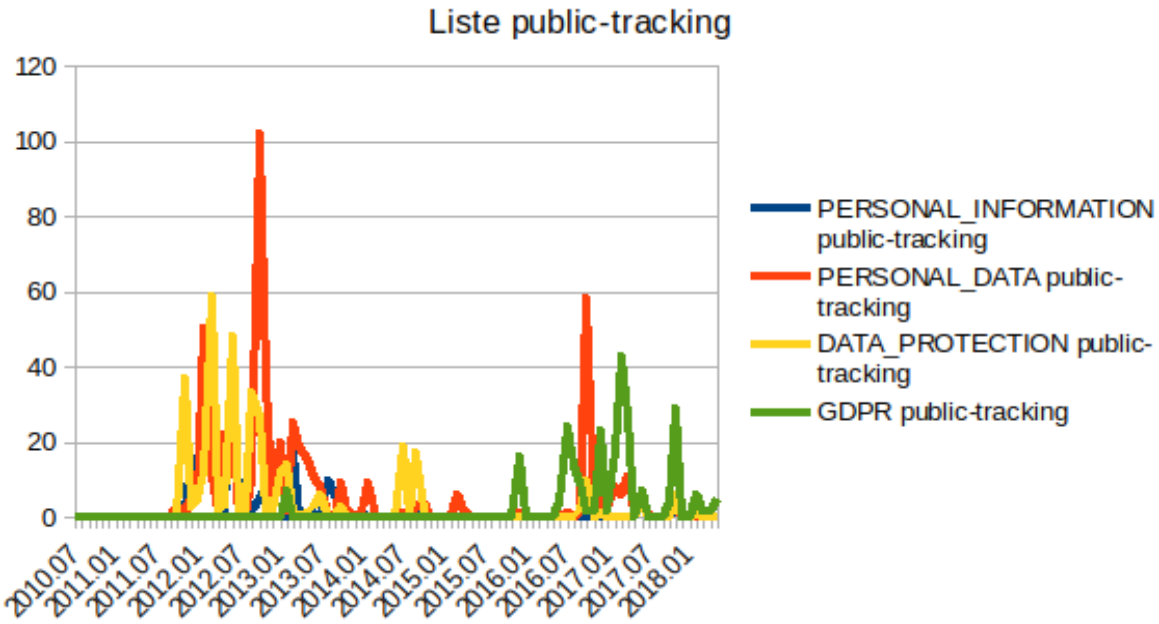


Figure 45 : *Évolution en nombre d'occurrences absolues de l'emploi de certains mots dans la liste de discussion* public-tracking. *Noter que cette liste de discussion n'existe qu'à partir de septembre 2011, ce qui explique le décalage en abscisse.*

Le terme de « *personal data* » ne fait pas son apparition en même temps que les discussions sur le RGPD dans ces deux listes de diffusion. Toutefois, dans *public-privacy*, nous observons assez clairement à la lecture de ces deux graphiques que l'emploi de ce terme se met à dominer très largement celui de « *personal information* » à partir du moment où le RGPD devient un thème de discussion, c'est-à-dire du moment où nous voyons le terme « rgpd » apparaître.

Ces données quantitatives vont dans le même sens que les conclusions tirées de l'analyse des documents produits par le TPWG et le PING. Nous constatons en effet que de la même façon que les connaissances juridiques produites par le réseau transgouvernemental européen des autorités de protection des données ont contribué à l'export des normes européennes dans le monde (Newman, 2008), les arènes de standardisation techno-politiques vont y puiser des concepts et des définitions. Cela s'observe entre autres par l'adoption d'une définition de la notion de « donnée à caractère personnel » qui reprend, dans le fond, et très largement, dans la forme, la définition de la directive de 1995, qui a été reprise dans le RGPD[119].

La première version du brouillon de la recommandation *Tracking Preference Expression* (TPE) du TPWG, en date du 14 novembre 2011 (W3C TPE, version du 14 novembre 2011), ne contenait ni le terme « *personal data* », ni celui de « *controller* » (mot anglais pour désigner un « responsable du traitement »). Il contenait par contre le terme « *personal information* ». La version suivante (du 13 mars 2012) a introduit le terme de « *data controller* » (W3C TPE, version du 13 mars 2012), emprunté au vocabulaire de la directive 95/46/CE et, plus anciennement, de la Convention 108. Le terme de « *personal data* » a quant à lui été introduit à partir de la version du 2 octobre 2012 (W3C TPE, version du 2 octobre 2012).

Toujours dans le TPWG, une « *issue* », c'est-à-dire un fil de discussion regroupant les courriels portant sur un même sujet de débat, a été ouverte sur le sujet de l'adoption de définitions sur les données. Cette « *issue* », qui porte le numéro 20, était intitulée « Différents types de données, ce qui compte comme PII, et la définition d'une PII »[120]. Elle n'a toutefois suscité aucune discussion qui lui ait été reliée, nous l'avons donc ignorée[121]. Une autre, la 188, porte en creux sur la définition de la notion de donnée à caractère personnel. Son titre est : « *Definition of de-identified (or previously, unlinkable) data* », soit : « Définition de données dé-identifiées (ou, précédemment, non-reliables) »[122].

119 Cf. sections 4.3.4. et 6.4.

120 Traduction de l'auteur. Texte original : « Different types of data, what counts as PII, and what definition of PII ». PII signifie : « Personally Identifiable Information », ou « information personnellement identifiable »

121 Voir : https://www.w3.org/2011/tracking-protection/track/issues/20 (page consultée le 1er juillet 2019)

122 Voir : https://www.w3.org/2011/tracking-protection/track/issues/188 (page consultée le 1er juillet 2019).

Pour Rob van Eijk, s'exprimant sur ce fil de discussion, la définition d'une donnée dé-identifiée devrait prendre en compte les conclusions des travaux de Paul Ohm. Il a ainsi fait directement référence au titre (en gras ci-dessous) de l'un de ces articles (Ohm, 2010) dans un e-mail du 5 septembre 2014 :

> « Merci David, Roy, pour la persévérance démontrée. Les derniers efforts de David semblent accommoder de nombreux, voire tous les éléments nécessaires pour avancer au-delà de la confusion causée par la « **promesse brisée de l'anonymat** ». Je vais réfléchir à cette proposition au cours des prochains jours[123]. » (*public-tracking*, e-mail de Rob van Eijk, e-mail du 5 septembre 2014)

Par ailleurs, nous avons trouvé la trace d'une discussion sur le point de savoir si une donnée qui permet de distinguer une personne sans l'identifier, par exemple en traçant son équipement, est ou non « *de-identified* », c'est-à-dire, en creux, est ou non une donnée à caractère personnel. Selon Roy Fielding de la société Adobe, par exemple :

> « Cela n'implique pas, de quelque façon que ce soit, que les jeux de données restent liés à l'utilisateur, qui est ce que l'identifiabilité [*linkability*] signifie en protection des données. (Relier à l'appareil d'un utilisateur n'est qu'un lien indirect à l'utilisateur).
>
> Les données désidentifiées peuvent demeurer liées les unes aux autres comme interactions apparentées après que les données identifiantes aient été ôtées de tous les enregistrements, ce qui inclue la suppression d'information dans le jeu de données qui pourraient être unique à un petit nombre d'utilisateurs (requêtes, temps réels, etc.)[124]. » (*public-tracking*, e-mail de Roy Fielding du 18 juillet 2014)

Vincent Toubiana, de la CNIL, lui rétorqua que :

123 Traduction de l'auteur. Texte original : « Thank you David, Roy for the perseverance shown. David's last effort seems to accomodate many, if not all elements needed to get beyond the confusion caused by the 'broken promise of anonymisation'. I will think this proposal through the coming days. »

124 Traduction de l'auteur. Texte original : « That does not, in any way, imply that the data set remains linked to the user, which is what linkability means to data protection. (Linking to the user's device is just an indirect linking to the user).
The de-identified data can remain linked together as related interactions after the identifying data has been removed from all records, which includes removal of information in the dataset that might be unique to a small set of users (queries, real times, etc.). »

> « Si les jeux de données peuvent être croisés alors il existe une change significative que nous ne soyons pas en train de parler de données anonymisées[125]. » (*public-tracking*, e-mail de Vincent Toubiana du 19 juillet 2014)

La définition finalement adoptée en octobre 2014 pour rédiger les documents de standardisation du *Do Not Track*, après un appel à objections[126], fut la suivante :

> « Les données sont *désidentifiées de façon permanente* lorsqu'il existe un haut niveau de confiance [*confidence*] dans le fait qu'aucune personne concernée humaine [*human data subject*] de la donnée ne puisse plus être identifié, directement ou indirectement (par exemple en association avec un identifiant, agent utilisateur [*user agent*] ou appareil [*device*]), par cette donnée seule ou en combinaison avec d'autres données conservées ou informations disponibles[127]. » (*public-tracking*, e-mail de Matthias Schunter du 22 octobre 2014)

Nous voyons ici que le TPWG a adopté une définition de la donnée anonyme (ou « *de-identified* ») comme étant une donnée, peu importe son contenu, qui ne permet ni directement, ni indirectement d'identifier une personne physique « identifiée ou identifiable ». L'inverse de cette définition correspond à la définition du RGPD de la notion de « donnée à caractère personnel ».

Pour ce qui est du PING, le document « *Specification Privacy Assessment* » destiné à fournir un guide pour effectuer des analyses d'impact vie privée préalablement à l'adoption d'une recommandation du W3C, contenait des références aux définitions et doctrines juridiques européennes et états-unienne[128] :

---

125 Traduction de l'auteur. Texte original : « If data records can be linked then there is a significant chance we're not talking about anonymized data. »

126 Cf. section 5.5.4.

127 Traduction de l'auteur. Texte original : « Data is *permanently de-identified* when there exists a high level of confidence that no human subject of the data can be identified, directly or indirectly (e.g., via association with an identifier, user agent, or device), by that data alone or in combination with other retained or available information. »

128 Il y est en particulier fait référence à un article de Paul Schwartz et Daniel Solove (Schwartz et Solove, 2012) intitulé : « *PII 2.0: Privacy and a New Approach to Personal Information* ». Cet article part du constat que l'anonymat robuste est un mythe, et propose de revoir des approches juridiques états-uniennes de la définition de la notion de « *personally identifiable information* » … pour la rapprocher, en pratique, de la définition européenne de la notion de « donnée à caractère personnel ». Contrairement à la doctrine des autorités de protection des données en Europe, ils proposent toutefois une forme d'approche basée sur le risque qui leur fait proposer un régime moins strict pour les données qui sont indirectement identifiantes, que pour les données directement identifiantes.

« Il convient de noter que, au sein de l'UE, la collecte est elle-même considérée comme un acte de traitement de données.

Il existe un certain nombre de schémas de classification qui peuvent être utilisés pour parvenir à cette étape de traitement, mais en général l'analyse devrait déterminer pourquoi les données sont collectées, quelle est la finalité première pour leur traitement, où elles sont transférées ou stockées et pour combien de temps elles sont conservées. De plus, la caractéristique de nonimat [*nimity*] ou le degré avec lequel l'individu associé avec la donnée personnelle peut être identifié, relié ou nommé à travers l'observation du trafic réseau contenant la donnée, doit être classé (c-à-d : est-ce que la donnée est personnelle, en fait, information personnellement identifiante ou PII). Une approche des PII par la classification peut être trouvée dans [Schwartz et Solove, 2012]. Les données personnelles y sont classées comme identifiées, identifiables, ou non-identifiables. De plus, une typologie des données sensibles pourrait être envisagée[129]. » (W3C SPA)

Nous avons vu que les débats destinés à définir la notion de « vie privée » (« *privacy* ») ou de « pistage » (« *tracking* ») étaient perçus par nombre d'acteurs du TPWG et du PING comme étant indésirables[130]. C'est ce que réaffirme, cette fois au sujet de la notion de « donnée à caractère personnel », un guide du PING sur le *fingerprinting* dont la rédaction a été confiée à Nick Doty :

« Le présent document n'essaie pas de fournir une seule et unique définition de la « vie privée » ou de la « donnée à caractère personnel », mais nous soulignons comment le *fingerprinting* du navigateur pourrait avoir un impact sur la vie privée des utilisateurs. Par exemple, le *fingerprinting* du navigateur peut être utilisé pour :

- identifier un utilisateur
- corréler l'activité d'un utilisateur au sein d'une même session et à travers plusieurs sessions
- pister les utilisateurs sans transparence ni contrôle[131] » (W3C Fingerprinting Guidance 2019).

129 Traduction de l'auteur. Texte original : « It should be noted that within the EU, collection, itself is considered to be an act of data processing.

There are a number of classification schemes that can be used to achieve this process step, but in general the analysis step should determine why the data is collected, what primary purpose there is for the processing of it, where it is being transferred or stored and how long it is being retained. In addition, the nymity characteristic or the degree that the individual associated with the personal data can identified, linked to, or named through observing the network traffic containing the data, needs to be classified (IE, is the personal data, in fact, personally identifiable information or PII). A PII classification approach can be found in [(Schwartz et Solove, 2012)]. There, personal data is classified as identified, identifiable and non-identifiable. In addition, a classification of sensitive identifiable should be considered. »

130 Cf. section 5.5.3.

Pourtant, le document « *Privacy Considerations for Web Protocols* » du PING inclut une définition de la notion de « *personal data* » reprise de la RFC6973, qui elle-même est inspirée de la directive 95/46/CE sous une forme plus succincte :

Définition de la directive 95/46/CE en anglais	« 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; » (art. 2 sous a))
RFC 6973	« Personal data: Any information relating to an individual who can be identified, directly or indirectly » (RFC 6973, p. 7)
Privacy Considerations for Web Protocols Unofficial Draft 29 April 2019	« Personal Data: Any information relating to an individual who can be identified, directly or indirectly. » (W3C Privacy Considerations)

Tableau 19 : *Définition de la notion de « donnée à caractère personnel » dans le droit de l'Union européenne et dans des documents de standardisation techno-politique*

La définition de « *personal data* » dans la RFC 6973 laisse, comme la définition de la directive de 1995, une marge d'interprétation sur le point de savoir si elle est relative ou absolue. Toutefois, la définition des termes « *anonymous* » et « *identifiable* » dans la même RFC indiquent un choix en faveur d'une conception absolue de la « donnée à caractère personnel », compatible avec les évolutions jurisprudentielles dans l'UE[132] et les tendances observées au résultat des « discussions » ayant abouti à l'adoption du RGPD[133]. Selon cette RFC, pour déterminer si une personne à laquelle se rattache une donnée est « *identifiable* », il faut en effet prendre en compte la capacité de n'importe quel « observateur » (et pas simplement « responsable du traitement » ou « *controller* ») ou « attaquant » est en mesure de l'identifier :

131 Traduction de l'auteur. Texte original : « This document does not attempt to provide a single unifying definition of "privacy" or "personal data", but we highlight how browser fingerprinting might impact users' privacy. For example, browser fingerprinting can be used to:
- identify a user
- correlate a user's browsing activity within and across sessions
- track users without transparency or control ».

132 Cf. section 6.3.

133 Cf. section 6.4.

« Anonyme : L'état d'un individu lorsqu'un observateur ou un attaquant ne peut identifier l'individu au sein d'un jeu comprenant d'autres individus (le jeu d'anonymat [*the anonimity set*])[134]. » (RFC 6973, p. 8)

« Identifiable : Une propriété dans laquelle l'identité d'un individu peut être connue d'un observateur ou d'un attaquant[135]. » (RFC 6973, p. 8)

Nous voyons donc que dans le PING et dans le TPWG, qui sont des arènes principalement composées d'informaticiens, la définition des « données à caractère personnel » (ou de leur strict inverse, les « *de-identified data* ») sont fortement inspirées des définitions contenues dans la directive 95/46/CE et, désormais, dans le RGPD. En outre, nous avons pu observer que le terme même de « *personal data* » a, dans ces deux arènes, largement supplanté celui de « *personal information* », la différence étant que, contrairement au premier, le second n'est pas utilisé dans le droit de l'UE *de la* protection des données à caractère personnel.

6.6. Discussion de l'hypothèse initiale d'une distinction entre approche juridique et approche informaticienne

Une hypothèse de sens commun, développée également dans une part de la littérature scientifique, décrit une différence d'approche entre droit et informatique en matière de protection des données. Cette différence d'approche se traduirait notamment par des différences de définition de ce qu'est une donnée à caractère personnel (voir notamment : Mascetti et al., 2013 ; Ohm, 2010)[136].

La comparaison entre les discours, structures argumentatives, référentiels en présence et état des controverses définitionnelles sur la notion de « donnée à caractère personnel » à travers l'étude généalogique du droit *à la* protection des données, du terrain sur les « discussions » sur l'adoption du RGPD, puis du *Privacy Internet Group* du W3C, a notamment été menée pour creuser cette hypothèse, que nous avions prise pour hypothèse initiale dans ce travail de thèse. Comme nous venons de le voir, les définitions de la notion de « donnée à caractère personnel » dans les arènes de standardisation techno-politique, qui sont composées essentiellement d'acteurs formés et socialisés à l'informatique, se rapprochent tendanciellement des définitions juridiques

134 Traduction de l'auteur. Texte original : « Anonymous: A state of an individual in which an observer or attacker cannot identify the individual within a set of other individuals (the anonymity set). »

135 Traduction de l'auteur. Texte original : « Identifiable: A property in which an individual's identity is capable of being known to an observer or attacker. »

136 Voir aussi la présentation des hypothèses dans l'introduction générale.

du droit de l'UE *de la* protection des données à caractère personnel. Ces travaux sont eux-mêmes le fruit de la ré-orientation du travail de recherche initial suite à une première phase exploratoire, qui nous avait déjà amené à nuancer l'hypothèse d'une différence fondamentale et épistémique entre approches juridiques (ou juridico-politiques) et informaticiennes de la protection des données à caractère personnel.

Avant de conclure ce chapitre de discussion transversale des trois principaux terrains d'enquête de cette thèse exposés dans les chapitres précédents, il est donc utile de rediscuter l'hypothèse initiale et d'évoquer la démarche exploratoire qui a précédé la ré-orientation du travail de recherche.

L'idée que juristes et informaticiens aient une vision différente de la protection des données est présente dans divers travaux de la littérature académique, dont les deux articles que nous venons de citer. Une autre idée présente dans cette littérature est que la protection des données, perçue dans ces circonstances plutôt comme quelque chose de juridique, entrerait en conflit avec des considérations de sécurité des systèmes d'information. Pour Martin Meints, par exemple : « la protection des données et la sécurité informatique sont deux domaines tout à fait différents lorsque l'on tient compte de leurs objectifs et acteurs respectifs[137] » (Meints, 2009, p. 255). Il évoque à titre d'exemple la journalisation des connexions à un serveur, incluant des adresses IP des requêtes entrantes, qui peut s'avérer utile à des fins de sécurité.

Comme nous avons pu le constater à diverses reprises en étudiant les arguments sur la définition de la notion de « donnée à caractère personnel » pendant les négociations sur le RGPD, la « réalité technique » a souvent été évoquée – en particulier par des acteurs de la coalition industrielle – pour défendre une définition contre des propositions présentées comme ne tenant pas compte de l'état de l'art en informatique[138].

Dans la même veine, une étude récente de l'Agence pour la formation professionnelle des adultes française (AFPA) a, en collaboration avec la CNIL et l'AFCDP, réalisé une étude auprès des délégués à la protection des données un an après l'entrée en application du RPGD (AFPA, 2019). Cette étude porte sur une population de 1265 délégués désignés auprès de la CNIL, dont 31,1 % identifiaient le droit comme leur « domaine d'expertise principal », et 34 % l'informatique. Une des questions qui leur a été posées était d'estimer le « niveau de maîtrise » requis dans différents domaines pour exercer la fonction de délégué à la protection des données. Pour les informaticiens, l'importance du droit était évaluée à 3,51/5 et l'informatique à 3,77/5, alors que pour les juristes, l'importance de l'informatique était évaluée à 2,81/5 et celle du droit à 4,22/5. Ceci montre des différences de priorité dans les savoirs et compétences à acquérir en fonction de la socialisation disciplinaire et professionnelle.

137 Traduction de l'auteur. Texte original : « data protection and information security are two quite different domains when looking at targets and stakeholders ».

138 Cf. sections 6.4.3 et 4.4.

Plusieurs informaticiens parmi les enquêtés de l'enquête exploratoire sur les représentations comparées d'informaticiens et de juristes en matière de protection des données ont exprimé le sentiment d'un droit « en retard » sur la technique ou bien de différences épistémiques dans les approches de la protection des données personnelles entre droit et informatique. Selon M.S. : « […] faut pas se leurrer, [le big data] est déjà utilisé, donc les politiques ont trois ans de retard [...] ». Plusieurs autres informaticiens interrogés l'ont rejoint sur cette idée, alors qu'à l'inverse, les juristes semblaient globalement plus confiants en la capacité du droit à la réguler les usages de l'informatique, y compris de l'Internet : « […] j'ai plus confiance dans la loi et tout ce qui va être l'appareil normatif » (entretien avec Mathilde Robert).

Nous ne pouvons toutefois généraliser ces résultats à partir d'un échantillon aussi faible, d'autant que dans l'enquête en ligne de la phase exploratoire, deux juristes ont aussi exprimé des doutes quant à la capacité du droit à garantir le droit *à la* protection des données à caractère personnel, tandis que quatre informaticiens sur cinq ont répondu faire confiance au droit pour cela.

Les rares réponses – toutes retranscrites ci-dessous – à la question du questionnaire en ligne portant sur le contenu de la différence d'approche entre juristes et informaticiens sont cependant peu précises :

> « L'approche du juriste est l'encadrement de l'opération de traitement afin d'assurer la protection des droits des individus sur leurs données personnelles, celle de l'informaticien est d'aboutir au résultat escompté par le traitement avec le plus de fiabilité »
>
> « Le juriste pense que la protection passe par des contrats. L'informaticien pense que la protection place par des outils »
>
> « Un juriste n'a aucune idée des limitations techniques et de ce qu'est réellement une donnée. Tout au plus il se représente ça comme un objet que l'on peut mettre dans un coffre fort. Un code-monkey fera au moins pire tant que la spec est respectée. […] En clair les juristes ont une vision extérieure très pure, et les informaticiens très terre-à-terre « j'obéis au management » [...] »
>
> « Les experts juridiques ont tendance à étudier les voies de recours lorsque la protection des données d'un individu ont été enfreints. Perspective descendante.
>
> Les experts techniques tendent à regarder comment sécuriser les données personnelles et les protéger de fuites. Perspective ascendante[139] »

139 Traduction de l'auteur. Texte original : « Legal experts tend to look at what remedies to apply when one's right to data protection was breached. Downstream perspective. Technical expert tend to look on how to safeguard personal data and to protect it from leaks. - Upstream perspective ».

Les descriptions ci-dessus sont assez générales, et lorsqu'elles arrivent effectivement à évoquer une différence, ne semblent converger que sur un point : la description d'une différence dans les outils propres à chaque profession, les juristes utilisant les « contrats » et les « recours » là où les informaticiens utilisent des « outils » qui « sécurisent ». Cela peut renvoyer à la différence de valorisation, au sein de chaque profession, des savoirs et compétences professionnelles de l'autre, qui a été montrée dans l'étude de l'AFPA sur les délégués à la protection des données (AFPA, 2019). Mais au-delà d'une forme de séparation et de spécialisation des tâches résultant de savoirs différents, existe-t-il une différence d'approche de nature épistémique, comme nous en avions initialement fait l'hypothèse à l'entame de cette première enquête exploratoire ?

L'article de Sergio Mascetti *et al.* (2013) a étudié la question sous l'angle de l'étude de différences définitionnelles de la notion de « donnée à caractère personnel » (ou de (quasi-)synonymes, comme « *personally identifying information* » ou PII). Or, nous avons vu qu'étudier les controverses définitionnelles autour de cette notion était une façon d'étudier des controverses sur l'objet de protection du droit *à la* protection des données à caractère personnel et du droit *à la* vie privée. Par conséquent, si, comme l'affirment Sergio Mascetti *et al*. (2013), il y a une différence de fond dans la compréhension de la notion de « donnée à caractère personnel » qu'ont d'une part les juristes, d'autre part les informaticiens, alors il y aurait effectivement lieu de parler de différence d'approche, au-delà de simples différences de savoirs et de savoir-faire professionnels.

Nous n'avons toutefois pas trouvé de telles différences dans nos entretiens et questionnaire exploratoires.

Par exemple, un informaticien a d'abord défini la « donnée anonyme » comme l'inverse de la « donnée à caractère personnel », laissant d'abord supposer une adhésion à l'idée qu'une anonymisation robuste était possible et une solution pour concilier garanties des droits fondamentaux avec possibilité d'exploiter les jeux de données à des fins économiquement utiles. Mais un peu plus tard au cours de l'entretien, la même personne a bien précisé qu'il adoptait une perspective relative de l'anonymat, et donc – par effet de miroir – une perspective absolue de la notion de « donnée à caractère personnel » :

> « […] moi je pense qu'à partir du moment où la donnée peut permettre par un biais quelconque d'identifier la personne […] physique […] c'est une donnée suffisante d'identification. […] à partir du moment où on stocke des données, qui sont associées à un utilisateur, que l'utilisateur doit pouvoir lui-même les retrouver […] y a toujours […] un

moyen plus ou moins détourné […] de retrouver les données. » (Entretien avec Mathieu Ghaleb)

Un autre informaticien, Pierre Colle, a expliqué en entretien :

« […] on pourra toujours te dire que tous les mecs qui habitent Marly-le-Roy et qui ont quatorze ans, ils fonctionnent de la même manière. Et qu'ils sont déjà allés sur un site de jeux vidéo, et au final, y en a qu'un seul de gars, qui a quatorze ans, qui est déjà allé sur un site de jeux vidéo […] » (Entretien avec Pierre Colle)

Une même perspective absolue a été adoptée par Stéphane Bracq, un juriste enseignant à l'Institut d'études politiques de Lille dont la spécialité n'est pas le droit *de la* protection des données et à qui il était demandé de définir, à chaud, en entretien, la notion de « donnée à caractère personnel » :

« […] je dirais deux choses. Des données qui sont […] liées à […] notre identité […]. D'autre part des éléments qui peuvent être rattachés à des éléments biométriques […] qui permettent de dire : c'est nous et pas un autre. […] Données personnelles, je dirais que c'est ce qui fait de nous une personne individuelle, indépendante des autres. C'est-à-dire qui permette de nous distinguer. » (Entretien avec Stéphane Bracq)

À l'inverse, selon informaticien que nous n'avons pas encore cité :

« J'ai un fichier Excel avec des informations. Si je supprime le nom et le prénom des colonnes et que je suis plus capable de les retrouver, mon fichier il devient anonyme » (Entretien avec Mathieu S.)

Sur le point de savoir quelles sont les données couvertes par le droit *de la* protection des données, certains informaticiens ont répondu qu'il s'agissait avant tout ou seulement de données portant sur la vie privée des personnes. Pour S. M., développeur dans une start-up parisienne :

« Alors déjà on est sur un service […] qui va demander plus que nom, prénom, date de naissance, mot de passe. On va probablement chercher à avoir autre chose […]. Du service qui te demande, par exemple, sur le mobile, à accéder à une partie de ton téléphone. C'est-à-dire tes photos, à te géolocaliser... » (Entretien avec S. M.)

Si cette réponse n'est pas celle retenue dans le droit européen *de la* protection des données[140], il serait toutefois faux d'affirmer que seuls des informaticiens se « trompent » à l'égard du droit à ce sujet. Ainsi, selon E. Q., enseignant-chercheur en droit :

> « Donnée à caractère personnel […] je dirais que c'est des données qui touchent à la vie privée des individus, donc […] à leur identité, leur sexe, leur orientation sexuelle, leurs pensées, enfin leur liberté de pensée, leurs opinions religieuses, politiques, mais éventuellement aussi des données qui touchent des éléments médicaux, donc de santé, et de vie familiale, de mode de vie familial […] » (Entretien avec E. Q.)

À l'inverse, pour une autre juriste non-spécialiste des données personnelles et travaillant dans une ONG au moment de l'entretien, le fait qu'une information soit publiquement accessible ne veut pas dire pour autant qu'il ne s'agit pas d'une donnée à caractère personnel :

> « [Il] y a des informations qui sont publiques, par exemple […] je peux faire une demande de ton état civil. Et si je récupère toutes les informations sur plein de gens ça reste un fichier … ça reste des données personnelles […]. Et donc c'est des trucs qui sont personnels, qui sont évidemment publics » (Entretien avec Mathile Robert)

Dans l'enquête en ligne, le fait que le répondant soit informaticien ou juriste n'a pas forcément déterminé fortement sa réponse à la question lui demandant de définir dans ses mots la notion de « protection des données » :

Réponse d'un juriste	**Réponse d'un informaticien**
« On pourrait définir la 'protection des données' comme l'ensemble des phénomènes légaux, réglementaires et techniques permettant de protéger et garantir **la propriété**[141] et la sécurité des données d'un individu au sein des espaces numériques, en particulier contre toute utilisation frauduleuse ou non expressément **consentie** par le sujet »	« La protection des données est une idée avant tout, qui veut que les sujets de données […] aient **le contrôle** sur les données qui les concernent. […] En somme, il s'agit d'admettre, ne serait-ce que partiellement, que **la propriété** des données revient à celui ou celle qu'elles concernent. […] »
« Toute méthode permettant **d'exclure l'intrusion** dans les informations concernant	« **Ne pas donner l'accès** à des données à des personnes **qui n'y aurait [sic] pas droit** »

140 Cf. sections 6.2.2., 6.3.2. et 6.4.

141 La mise en forme a été rajoutée pour souligner les éléments de convergence entre deux réponses sur une même ligne.

une personne »	
« Un système permettant de collecter, modifier et surtout de **sécuriser** les données transmises par informatique »	« Relatif à **la sécurité des données** et à la protection de la vie privée entre autres. C'est tout ce qui permet d'empêcher l'accès, le vol, la copie, la modification, l'altération ou la suppression de données dans le particulier/l'entreprise dépend/est responsable »

Tableau 20 : *Exemples de réponses données à la question : « pouvez-vous décrire brièvement, dans vos propres mots, ce que signifie le terme de « protection des données » ? »*

Sans pouvoir faire de conclusions définitives en raison de l'absence d'échantillon représentatif ou à défaut, massifié, nous voyons que les entretiens et le questionnaire exploratoires n'encouragent pas à poursuivre la piste d'une différence d'approche entre droit et informatique se traduisant par des acceptions différentes de la notion de « donnée à caractère personnel ». La comparaison entre le terrain sur l'adoption du RGPD et celui sur le W3C ont quant à eux montré une convergence forte dans les définitions qui ont été adoptées de la notion de « donnée à caractère personnel »[142]. Elle révèle aussi de fortes similarités dans le contenu des discours en circulation dans le rôle de l'argument de la « confiance »[143], dans l'importance de l'idée d'un droit *à l'*auto-détermination informationnelle (ou de « *user control* »)[144], ou encore dans la structure d'une opposition entre défenseurs de la vie privée à coalition industrielle[145]. Nous pouvons donc au moins conclure que, dans le cas de publics experts comme les acteurs de nos trois terrains, il n'existe pas de différence d'approches entre juristes et informaticiens en matière de protection des données ou de vie privée. S'il y existe pourtant bien une controverse définitionnelle sur la notion de « donnée à caractère personnel », elle ne s'explique pas par une opposition entre savoirs disciplinaires, mais par une opposition entre acteurs ayant des convictions et des objectifs politiques opposés.

L'opposition entre informatique et droit fondée sur l'hypothèse d'une tension entre cybersécurité d'une part et droit *à la* protection des données à caractère personnel (voir : Meints, 2009) ne se vérifie pas non plus. Il est vrai que l'accent n'est pas forcément mis sur les mêmes compétences par les juristes et les informaticiens, et comme le rappelle l'étude de l'AFPA de 2019, ce ne sont pas forcément les mêmes savoirs qui sont mis en œuvre et valorisés par chacun de ces groupes (AFPA, 2019). Toutefois, la cybersécurité est *aussi* une exigence fondamentale du droit *de la* protection des données à caractère personnel (art. 17 de la directive 95/46/CE, art. 32

142 Cf. section 6.5.
143 Cf. sections 3.8., 4.5. et 5.6.3.
144 Cf. sections 4.3.3., 4.6. et 5.6.1.
145 Cf. sections 4.2. et 5.5.

du RGPD). Le traitement de données à caractère personnel pour assurer la confidentialité des données à caractère personnel peut donc logiquement être fondé sur l'article 6 paragraphe 1 sous c) du RGPD, qui couvre les cas où « le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ». Certains « opérateurs de service essentiels » sont soumis à des obligations particulières de sécurité des systèmes d'information en vertu de la directive NIS[146] qui permettent là aussi, pour ces opérateurs, de collecter des données à caractère personnel dans la mesure de leur stricte nécessité pour remplir ces obligations légales. Un grand nombre de secteurs, comme la santé ou le paiement, disposent de leurs propres exigences de sécurité. Et même dans les cas résiduels ou un système d'information ne contient pas de données à caractère personnel, et n'est pas soumis à des obligations particulières en matière de cybersécurité, il n'en demeure pas moins qu'il peut y avoir là un intérêt légitime du responsable du traitement à assurer cette sécurité. La CJUE a eu l'occasion de le confirmer en faisant référence à l'article 7 sous f) de la directive de 1995, instaurant le critère de l'intérêt légitime :

> « L'article 7, sous f), de la directive 95/46 doit être interprété en ce sens qu'il s'oppose à une réglementation d'un État membre en vertu de laquelle un fournisseur de services de médias en ligne ne peut collecter et utiliser des données à caractère personnel afférentes à un utilisateur de ces services, en l'absence du consentement de celui-ci, que dans la mesure où cette collecte et cette utilisation sont nécessaires pour permettre et facturer l'utilisation concrète desdits services par cet utilisateur, sans que l'objectif visant à garantir la capacité générale de fonctionnement des mêmes services puisse justifier l'utilisation desdites données après une session de consultation de ceux-ci. »[147]

La CJUE confirma à l'occasion de ce jugement la position que le G29 avait adoptée dans son avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (G29, 2014a, p. 28 et 73). Quant aux principes *de la* protection des données, certains, comme le principe de minimisation des données et de limitation des finalités, contribuent à une stratégie de sécurité efficace des systèmes d'information en réduisant la surface d'attaque des adversaires potentiels. Il n'y a donc pas de conflit ou même de tension entre droit *de la* protection des données et sécurité informatique. Au contraire, ces deux aspects sont complémentaires. Nous pouvons rappeler à ce titre que dans les années 1960, pour au moins certains des premiers informaticiens à s'être intéressés à ces questions, « sécurité » (« *security* ») et « vie privée » (« *privacy* ») étaient abordés conjointement (Ware, 1967) et qu'en entretien, selon l'un de nos enquêtés, le champ de la cybersécurité ne se serait séparé en France du champ « Informatique et Libertés » qu'à partir des années 1980[148]. Enfin, et nous reviendrons sur ce point, les principes de la protection des données trouvent leur

146 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (dite directive « NIS » pour « *Network Information Systems* »)

147 CJUE 19 octobre 2016 « Patrick Breyer contre Allemagne », Aff. C-582/14, dispositif

148 Entretien avec Henri Delahaie

origine dans des recommandations faites par la *British Computer Society* au Comité Younger en 1971.

Notons pour l'instant que l'étude de l'AFPA de 2019 sur les délégués à la protection des données (DPD) (AFPA, 2019) montre bel et bien que les informaticiens et les avocats DPD accordent une importance moindre aux savoirs de l'autre discipline dans l'exercice de ce métier. Mais si les savoirs opérationnels sont différents – paramétrer un pare-feu ou un système de gestion des accès sur un système d'information ne met pas en œuvre les mêmes compétences que la rédaction d'un contrat de sous-traitance conformément à l'article 28 paragraphe 3 du RGPD ou que la rédaction d'une notice d'information aux personnes concernées – cela ne veut pas dire pour autant qu'il y ait des divergences fondamentales d'approche dans les définitions, les valeurs ou les objectifs qui soient fonction de la socialisation disciplinaire des acteurs. Cybersécurité et protection des données (ou de la vie privée) sont des domaines d'activité distincts mais complémentaires. Cette idée d'une complémentarité se retrouve dans le discours de Sid Stamm, un informaticien ayant contribué aux travaux du TPWG au W3C :

> « La façon dont je le vois est la suivante : la vie privée et la sécurité sont des attributs du système. Et la sécurité est une tendance d'un système à faire ce pour quoi il a été conçu. Donc si ça marche de la façon dont ça a été prévu par les gens qui l'ont créé, ça a un haut niveau de sécurité. La vie privée est un peu différente parce qu'elle est centrée sur l'utilisateur. Donc peu importe la personne qui a créé le système, la question est : le système fait-il ce que les utilisateurs s'attendent à ce qu'il fasse[149] ? » (Entretien avec Sid Stamm)

Enfin, le terrain sur la généalogie du droit à la protection des données à caractère personnel a permis d'observer les rôles respectifs que les juristes et les informaticiens ont joué dans la mise à l'agenda de la notion de « protection des données ». Ce même terrain nous a également permis d'observé, à partir de documents d'archives, que les principes de la protection des données n'ont pas été inventés par des juristes mais que ce sont des informaticiens britanniques qui les ont formulés pour la première fois. Il est utile de revenir sur leur origine pour démontrer cette origine interdisciplinaire, qui bat en brèche l'idée reçue que ces principes auraient été des inventions imposées par des juristes sans aucun égard donné à la « réalité technique ». Revenons donc sur l'histoire du Comité Younger, et de sa relation avec la *British Computer Society*.

149 Traduit de l'anglais. Texte original : « The way that I see it is : privacy and security are both attributes of the system. And security is a tendency for a system to do what it's designed to do. So if it works the way it's designed by the people who created this, it has high level of security. Privacy is a little different because this one is user-centric. So regardless of whoever created the system, the question is : does the system do what its users expect with their data ? »

Ce comité a été mis en place en 1970 par le gouvernement britannique pour étudier le droit *de la* protection de la vie privée et dire si le au Royaume-Uni était adéquatement équipé pour répondre aux problèmes d'intrusion dans la vie privée par des personnes privées[150], physiques ou morales (Younger, 1972, p. 1). Il était composé de juristes et dirigé par Kenneth Younger, un ancien parlementaire travailliste. Un sous-groupe se forma en son sein pour étudier le rôle de l'informatique dans les intrusions commises par des personnes privées dans la vie privée des individus.

La *British Computer Society* (BCS) a fait partie des organisations avec lesquelles ce sous-groupe est entré en contact dans le cadre de ses travaux. Les idées de limitation des finalités, de confidentialité et de sécurité, de minimisation, d'information des personnes concernées, de droit d'accès et de rectification, de responsabilité, de création d'une autorité de supervision, figurent toutes dans le rapport soumis en 1971 par la BCS au comité Younger (British Computer Society, 1971). Le rapport final de ce comité, dans lequel nous retrouvons l'inspiration du paradigme libéral de la vie privée à travers notamment des citations d'Alan Westin (Younger, 1972, p. 18), a repris ces idées en les écrivant sous la forme de « principes » (« *principles* ») (Younger, 1972, p. 182). Puis, G.P. Pratt, secrétaire au *Home Office* britannique et qui faisait partie du groupe ayant étudié l'informatique dans le Comité Younger, a été envoyé à Strasbourg pour la première réunion du groupe d'experts du Conseil de l'Europe sur la protection de la vie privée vis-à-vis des banques de données électroniques (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 5 Rev, annexe 1). Cette réunion fut l'occasion pour lui de présenter ces fameux « principes » proposés dans le rapport du comité. Ces derniers ont ensuite été reformulés puis adoptés par les membres du groupe d'experts, comme en atteste le rapport de la première réunion (Conseil de l'Europe, EXP/Prot.Priv./EDB (72) 5 Rev, pp. 12-16).

À nouveau retravaillés, ces principes ont été inscrits dans la Résolution 22 de 1973 du Comité des ministres du Conseil de l'Europe relative à la protection de la vie privée vis-à-vis des banques de données électroniques dans le secteur privé[151]. De nouveau réécrits, ces principes se retrouvent dans les Lignes directrices de l'OCDE, la Convention 108, et aujourd'hui, le RGPD.

Les groupes d'experts à l'OCDE et au Conseil de l'Europe ne comptaient pas d'informaticiens dans leurs rangs, et étaient contraints de faire appel à des consultants extérieurs et de s'informer sur ce sujet nouveau. Mais par l'intermédiaire du rapport Younger et celui du rapport HEW qui, aux États-Unis, avait été confié à Willis Ware (un informaticien de la Rand Corporation) il est clair que des informaticiens ont, à l'époque, considérablement influencé le droit naissant *de la* protection des données à caractère personnel. Ce droit n'est donc pas une pure invention de juristes imposée à des informaticiens ayant une autre conception du problème que la « protection des données » vise à résoudre.

150 Le comité Younger n'a pas reçu d'autorisation de la part du gouvernement de s'intéresser aux problèmes d'intrusion dans la vie privée par des personnes morales de droit public, malgré ses demandes.

151 Cf. annexes 1 et 13

Tous les éléments discutés dans ce sous-chapitre tendent donc à invalider l'hypothèse initiale d'une différence épistémique entre juristes et informaticiens dans leurs conceptions du droit *à la* protection des données à caractère personnel.

6.7. Conclusion du chapitre : une définition stable sur le temps long de la notion de donnée à caractère personnel, qui correspond aux représentations du paradigme libéral de la vie privée

La phase exploratoire du travail de recherche sur lequel se base cette thèse, même si elle n'a pas généré de données quantitativement représentatives, nous a rapidement amené à nuancer l'hypothèse de recherche initiale et à ré-orienter la recherche. Sur la base des travaux issus de cette ré-orientation, nous avons pu conclure que la définition contenue dans les normes de droit de l'UE de la notion de « donnée à caractère personnel », a été reprise telle qu'elle y est définie et telle qu'elle a été précisée par la jurisprudence de la CJUE dans les arènes de standardisation techno-politique et dans des documents du W3C et de l'IETF. En outre, la plus ancienne trace de formulation des principes de la protection des données, comme celui de limitation des finalités, que nous ayons trouvée en archives, a été rédigée par des informaticiens. Si informatique et droit ont généré des savoirs et des compétences différents en matière de protection *de la* vie privée et des données à caractère personnel, et qu'informaticiens et juristes ne semblent pas accorder la même valeur aux compétences de la profession qu'ils n'exercent pas les explications aux controverses définitionnelles autour de la notion de « donnée à caractère personnel » sont donc à chercher ailleurs.

Les terrains étudiés ont montré que cette controverse est le fruit la confrontation de deux coalitions. Une première coalition est favorable à l'exploitation des données à caractère personnel pour l'utilité perçue de celle-ci pour la croissance économique. Une seconde coalition, celle des défenseurs de la vie privée, s'est structurée autour d'un paradigme libéral de la vie privée, favorable à ce que les juristes ont appelé le « droit à l'auto-détermination informationnelle » et les ingénieurs du W3C PING et du TPWG le principe du « *user control* ». Le but de la coalition industrielle était de limiter les cas concrets *qualifiables* de « données à caractère personnel », pour que le droit *de la* protection des données s'applique moins souvent, le tout dans l'espoir qu'il soit moins coûteux financièrement de s'y conformer. Cela favoriserait l'innovation, et ainsi, une croissance économique qui est pour elle un objectif prioritaire. Ce faisant, cette coalition aux convictions néolibérales ne fut en réalité pas en mesure de remettre en cause le cadrage du débat sur la protection des données proposé par le paradigme libéral de la vie privée[152].

152 Cf. section 4.6.

La rédaction retenue pour la définition de la notion de « donnée à caractère personnel » a donc largement été inspirée par ce cadrage libéral qui la centre sur l'individu comme personne physique, et la distingue de celle de « donnée relative à la vie privée »[153]. En effet, même les données qui ne relèvent pas de la « vie privée » au sens d'un espace physique et informationnel que des normes sociales ôtent du regard du public, sont des « données à caractère personnel », que l'individu qu'elles concernent doit selon ce paradigme pouvoir « contrôler ». Si elles ne sont pas forcément protégées au titre de la « vie privée » si nous adoptons une définition de cette dernière fondée sur la défense d'une frontière public/privé, elles sont bien protégées au titre de la « protection des données à caractère personnel ». Juridiquement, cette distinction paraît bien tranchée.

Pourtant, le droit *de la* protection des données à caractère personnel, comme le supposaient les troisième et quatrième hypothèses, a bien été inventé afin de protéger la « vie privée » conçue comme un *contrôle individuel* face à l'intrusion de l'ordinateur perçu comme une menace, par des personnes adhérant à un système de conviction accordant de la valeur à cette conception libérale de ce droit. Au W3C, c'est bien le terme de « *privacy* » qui est utilisé pour désigner des efforts visant à limiter la collecte de données à caractère personnel par les opérateurs de sites web et à donner du « *user control* » aux internautes. Ces hypothèses 3 et 4 ne sont donc finalement pas fausses… sauf si, au lieu de considérer la « vie privée » comme un droit au contrôle sur les informations qui nous concernent, nous considérons qu'elle s'incarne dans la protection de la délimitation entre un « espace privé » et un « espace public ».

Nous allons maintenant voir en conclusion, après avoir passé en revue nos quatre hypothèses, comment cette définition et la confusion entretenue dans le rapport entre droit *à la* vie privée et droit *à la* protection des données à caractère personnel est en réalité symptomatique d'une tension entre ces deux conceptions du droit *à la* vie privée, que nous proposerons de désigner sous les termes de vie privées « des Anciens » et des « Modernes ». L'explicitation de cette distinction permet de clarifier la réponse concernant la validité des deux dernières hypothèses à laquelle la réponse se résume pour l'instant à un « cela dépend du point de vue » un peu morne, tout en fournissant – c'est, du moins, la thèse que nous défendons – une clef d'explication supplémentaire au fameux paradoxe de la vie privée, par lequel nous avions commencé notre introduction.

153 Cf. section 6.3.2.

Conclusion générale

Que ce soit dans les Lignes directrices de l'OCDE de 1980, dans la Convention 108 du Conseil de l'Europe de 1981, dans le RGPD adopté en 2016 ou dans les documents de standardisation techno-politique produits par le W3C, la notion de « donnée à caractère personnel » est définie comme étant toute donnée, quel que soit son contenu, qui puisse être reliée à une personne physique « identifiée ou identifiable », « directement ou indirectement ». Elle découle d'une conception libérale de la « vie privée », dans laquelle cette dernière est définie comme un contrôle de l'individu sur les informations qui le concernent, dans le but de sauvegarder son autonomie et sa liberté individuelles.

La stabilité de cette définition dans le temps et à travers les différentes arènes où elle a été débattue a de quoi surprendre.

Pour commencer, nous nous attendions, au début de la thèse, à apercevoir des différences conceptuelles fortes entre juristes et informaticiens dans leurs acceptions respectives des notions de « vie privée » et de « données à caractère personnel ». Or, non seulement les principes de la protection des données ont été imaginés en premier dans les années 1970 par des informaticiens, mais en plus, nous observons une forte convergence, malgré des différences lexicales, entre les discours sur les « données personnelles » qui circulent dans les arènes institutionnelles marquées par la présence du droit (comme l'UE) et les arènes de standardisation technique composées essentiellement d'informaticiens (comme le W3C[1]). Partout, nous avons observé l'efficacité de discours inspirés du paradigme libéral de la vie privée favorable au « contrôle » individuel, sur la formation des définitions normatives de la notion de « donnée à caractère personnel ».

Cela nous a conduit à invalider la première hypothèse, qui affirmait « qu'il existe une différence d'ordre épistémique – voire une confrontation – entre des conceptions juridiques d'un côté et des conceptions informaticiennes de l'autre, du sens des termes « protection des données », « vie privée » et surtout « donnée à caractère personnel », notamment en raison de la formation différenciée des juristes d'une part, et des informaticiens de l'autre » (p. 49 de la thèse).

L'autre raison de cette surprise est que les infrastructures techniques d'information et de communication ont profondément évolué entre le début des années 1970, lorsque des experts du Conseil de l'Europe, suivis par quelques législateurs pionniers ont inventé la définition de la notion de « donnée à caractère personnel », et la seconde moitié des années 2010, au moment de l'adoption du RGPD. Lorsque la Convention 108 a été inventée, Internet n'était encore qu'un projet pour relier entre eux différents réseaux informatiques grâce à une même suite de protocoles les rendant interopérables. Les objets connectés, les réseaux sociaux comme Facebook, la

1 Cf. chapitre 6.

publicité comportementale en ligne, ou encore la reconnaissance faciale automatisée couplée à la vidéosurveillance restaient encore à inventer. Les smartphones et les tablettes étaient quant à eux de purs objets de science-fiction.

Si, entre les années 1970 et aujourd'hui, l'objet de la protection du droit *de la* protection des données, qui met notamment en œuvre le droit *à la* vie privée, n'a pas évolué, et que nous définissons la « vie privée » comme l'objet de ce droit, alors devons-nous conclure que l'évolution du milieu technique, et en particulier des techniques de communication, n'a eu aucune incidence sur l'évolution de la « vie privée » ?

En réalité, contrairement à l'affirmation de Karl Marx selon laquelle l'infrastructure matérielle de la société détermine la superstructure, c'est-à-dire les formes d'organisation sociales et l'idéologie (Marx, 2002 [1859] , discuté par : Castoriadis, 2006 [1975]), les transformations du milieu technique ne suffisent pas à elles seules à expliquer les changements d'ordre social. Nous ne pouvons nier que la diffusion de l'informatique en réseaux a transformé les conditions matérielles d'exercice du contrôle de l'accès à soi et de la circulation d'informations qui nous concernent. Mais cela ne suffit pas à expliquer une transformation dans la façon dont une société – ou au moins son droit écrit et son interprétation – envisage la valeur et le contenu du droit *à la* vie privée.

C'est la *perception* que certains acteurs – juristes, hauts fonctionnaires, hommes et femmes politiques et informaticiens – ont eu de l'informatique comme représentant un danger pour la conception libérale de la vie privée à laquelle ils adhéraient qui a provoqué la mise à l'agenda politique de projets de lois désignées par la formule nouvelle de « lois de protection des données » en Europe au début des années 1970[2]. Ces personnes ont formé une communauté transnationale désignée dans la littérature académique par les termes de « *privacy community* » ou de « défenseurs de la vie privée[3] ».

Leur référentiel libéral utilitariste est devenue, en Europe, le référentiel sectoriel d'un nouveau domaine de l'action publique : les politiques publiques de protection des données à caractère personnel. Mais il existe d'autres discours sur la « vie privée » qui le critiquent, ou qui adoptent un point de vue sur les données à caractère personnel qui part d'une réflexion sur la technique plutôt que d'une réflexion sur les droits humains[4]. Certaines théories conçoivent le droit *à la* vie privée comme quelque chose d'indésirable[5]. D'autres encore voient en la quantification de soi à travers des données personnelles générées et traitées par des ordinateurs une façon d'augmenter l'autonomie de l'individu, et non de la réduire[6]. Mais ce ne sont pas ces discours concurrents au paradigme libéral qui ont guidé la rédaction du droit *de la* protection des données.

2 Cf. chapitres 3 et 6.
3 Voir sections 3.5., 4.1.4., 4.2. et 5.5.5.
4 Cf. chapitre 2.
5 Voir par exemple la critique néolibérale de la vie privée en section 2.3.1.
6 Voir l'exemple du mouvement du *Quantified Self* en section 2.4.1.

Enfin, le traitement informatisé et automatisé de données, qu'elles portent ou non, au demeurant, sur des individus, est présenté par certains acteurs comme un facteur de croissance économique. Dans le contexte de l'ancien référentiel global keynésien, cela devait permettre d'améliorer l'efficacité des politiques économiques d'États planificateurs. Désormais, les données personnelles sont perçues à travers le prisme du référentiel global néolibéral comme une source marchande de richesses et une ressource nécessaire à l'innovation permettant de soutenir une croissance « fondée sur les connaissances ». Durant les « discussions » sur le RGPD, la coalition de cause industrielle a ainsi largement insisté sur la nécessité, selon elle, de ménager un équilibre entre droit fondamentaux – dont celui *à la* vie privée et/ou *à la* protection des données – et objectifs de croissance économique. Dans son discours, les possibilités de traitement informatisé de données personnelles n'étaient pas présentées comme une menace pour l'intérêt public, mais au contraire comme une opportunité. Cela prouve bien qu'il n'y a pas de lien de causalité nécessaire unique entre l'évolution du milieu technique, sa perception et ses conséquences sociales, au moins en matière de « vie privée ».

Les défenseurs de la vie privée ont adopté une stratégie argumentative qui leur a permis d'articuler leurs idéaux libéraux à ces référentiels globaux successifs. En d'autres termes, ils ont dû démontrer que leur projet de droit *de la* protection des données ne remettrait pas en cause les objectifs du référentiel global auquel sont soumis l'ensemble des sous-systèmes de politiques publiques à un moment historique donné. Leur argument principal a été que le droit *de la* protection des données serait indispensable pour garantir la confiance des citoyens – et donc des consommateurs – dans l'informatique, dans les réseaux de communication numériques, et dans les services de la société de l'information. Cette stratégie leur a permis de rendre leurs revendications compatibles avec les objectifs des référentiels globaux qui se sont succédé entre les années 1970 et aujourd'hui. Nous avons trouvé cet argument de la confiance employé à l'OCDE, au Conseil de l'Europe[7], dans les « discussions » sur le RGPD[8] et dans les débats sur la « vie privée » au W3C[9].

Ce succès stable de la stratégie argumentative des défenseurs de la vie privée dans les controverses que nous avons étudiées contribue à expliquer la stabilité des mesures concrètes adoptées dans les textes normatifs étudiés, et en particulier la stabilité de la définition de la notion de « donnée à caractère personnel » qui découle du paradigme libéral, malgré les transformations en profondeur du milieu technique en général et des techniques d'information et de communication en particulier. Dans le même temps, c'est bien la perception de ces évolutions, au prisme d'un imaginaire social situé, qui a généré dans les années 1960 et 1970 le retour à l'agenda politique du droit *à la* vie privée et a abouti à l'invention du droit *de la* (puis *à la*) protection des données.

7 Cf. section 3.8.
8 Cf. section 4.5.
9 Cf. section 5.6.3.

Nous pouvons donc valider notre seconde hypothèse, née d'observations de terrain que nous avions reformulées en hypothèse en cours de thèse, selon laquelle « les formules de « protection des données », « droit à la protection des données à caractère personnel », et la définition de la notion juridique de « donnée à caractère personnel » n'ont pas émergé comme conséquence mécanique des évolutions de l'infrastructure technique de la société, mais en conséquence de *perceptions* de l'informatique, des ordinateurs qui s'insèrent dans cette infrastructure, comme étant des dangers pour un droit à la « vie privée » pré-existant » (p. 51 de la thèse).

Les premiers instruments juridiques désignés comme étant des instruments de « protection des données » sont nés de la volonté de protéger une conception libérale de la vie privée, qui insiste sur le droit de l'individu de contrôler l'accès à soi, et en particulier les informations qui le concernent. C'est ce que le Tribunal constitutionnel fédéral de la RFA a appelé le « droit à l'auto-détermination informationnelle ». Ce droit a une valeur intrinsèque – fondée par exemple selon les juges de ce même tribunal sur le principe de dignité de la personne humaine – mais aussi une valeur instrumentale : il est vu comme nécessaire à l'exercice d'autres droits fondamentaux, comme le droit à la non-discrimination ou à la liberté de conscience. Certains théoriciens libéraux ont aussi vu en ce droit un prérequis pour des droits collectifs, comme celui de participer à des élections libres ou de limiter le pouvoir des bureaucraties étatiques.

Les textes juridiques ont progressivement opéré une distinction (au moins formelle) entre le droit *à la* vie privée et le droit *à la* protection des données. Comme nous l'avions exposé dans l'introduction, le rapport concret entre ces deux catégories de droits fondamentaux n'est pas clair, mais nous savons que le droit *de la* protection des données – par exemple le RGPD – vise à garantir les deux. Pour compléter ce tableau conceptuel complexe, en droit de l'UE, « donnée à caractère personnel » et « donnée relative à la vie privée » n'ont pas la même signification, mais il existe au sein de la catégorie générale de « donnée à caractère personnel » du RGPD une catégorie spéciale, définie à son article 9, de données personnelles considérées *a priori* comme étant particulièrement sensibles.

Cette confusion conceptuelle, qui ne peut être levée sans déformer ce que nous avons observé sur le terrain, ne nous permet pas de formuler de conclusions claires sur nos troisième et quatrième hypothèses sans préciser d'abord le point de vue selon lequel nous nous exprimons.

Si, conformément au paradigme libéral de la vie privée, la « vie privée » est un droit à l'auto-détermination informationnelle, où l'individu définit lui-même, librement, les frontières spatiales et informationnelles de son espace privé, alors le droit *à la* protection des données, qui porte sur *toute* donnée relative à une personne physique quel que soit son contenu, vise bien à protéger le même objet que le droit *à la* vie privée. Dans ce cas, la troisième hypothèse, selon laquelle « le droit *à la* et *de la* protection des données à caractère personnel ont été imaginés pour

conserver l'efficacité de la protection du même objet qu'un droit pré-existant : le droit *à la* vie privée » (p. 52 de la thèse), se vérifie effectivement.

Quant à la quatrième hypothèse, qui supposait « l'existence d'une continuité dans les idées, idéologies, systèmes de convictions, imaginaires sociaux et arguments qui […] motivent la défense [de ces droits], ou au moins […] du partage d'une même généalogie intellectuelle et politique » (p. 53 de la thèse), elle se vérifie alors aussi dans la mesure où le paradigme libéral de la vie privée s'inscrit dans la continuité intellectuelle des réflexions qui, avant l'informatique, et avant l'invention de la protection des données en Europe, avaient inspirées à Louis Brandeis et Samuel Warren l'invention d'un droit cohérent *à la* vie privée, proposé dans un article académique publié en 1890[10].

Mais il est aussi possible d'adopter le point de vue selon lequel la « vie privée » se définit avant tout par opposition à la « vie publique » ou à « l'espace public ». Dans cette conception, le droit *à la* vie privée et *de la* vie privée doivent protéger un espace privé dont les frontières sont définies collectivement, et pas par des individus. Ce droit peut aussi être conçu comme une protection contre l'intrusion dans l'espace public de certains sujets, jugés trop triviaux, intimes, ne devant pas relever d'une discussion collective. Typiquement, cette conception a pu compliquer la formulation dans l'espace public des discriminations de genre, ou encore justifier auprès d'un juge qu'un tribunal n'aurait pas à connaître, au nom du droit *à la* vie privée, d'affaires de violences conjugales[11]. Ces exemples illustrent les raisons de l'existence de toute une littérature féministe critique envers ce droit *à la* vie privée, au moins lorsqu'il est conçu comme une défense d'une frontière rigide et collectivement définie entre ce qui doit rester privé et ce qui mérite d'accéder à la notoriété de l'espace public.

Bien que de telles tentatives aient finalement été assez rares, nous avons vu que la théorie contextuelle de la vie privée d'Helen Nissenbaum, défavorable au droit à l'auto-détermination informationnelle et s'inscrivant dans la tradition intellectuelle de la recherche des frontières de l'espace privé[12], a été utilisée pour tenter de remettre en cause la définition juridique de la notion de « consentement » au traitement de données à caractère personnel, qui est l'une des principales mesures concrètes inspirées du paradigme libéral[13], ou pour avancer une définition de la notion du « *tracking* » qui contrevienne aux projets des défenseurs de la vie privée qui ont porté le projet *Do Not Track* au sein du W3C[14].

Donc si nous adoptons cette autre façon de concevoir la « vie privée », comme une protection de « l'intime » du regard du « public », alors le droit *de la* protection des données, qui donne aux individus des droits sur les données qui les concernent quel que soit leur contenu (intime ou non), s'applique à de nombreuses situations qui ne relèvent *pas* du droit *à la* vie

10 Cf. sections 2.2. et 3.2.1.
11 Cf. p. 37 en introduction générale.
12 Cf. section 2.3.5.
13 Cf. sections 4.3.3. et 4.6.
14 Cf. sections 5.5. et 5.6.2.

privée. Dans ce cas, seules les dispositions relatives aux données dites sensibles relèvent du droit *à la* vie privée, et le reste relèverait uniquement du droit *à la* protection des données à caractère personnel.

En poursuivant ce raisonnement, notre troisième hypothèse devient fausse : le droit *à la* protection des données est alors un droit nouveau, nettement distinct du droit *à la* vie privée. La quatrième hypothèse est alors également invalidée, puisque le droit *à la* comme celui *de la* protection des données est inspiré de théories libérales qui ont défendu un droit à l'auto-détermination informationnelle *individuel*, et non la protection d'une frontière *collectivement définie* entre public et privé.

Quel que soit le point de vue adopté, une certitude demeure : la perception, découlant d'imaginaires sociaux véhiculés entre autres par la science-fiction dans les années 1960 et 1970, du développement de l'informatique comme un danger pour la conception libérale de la « vie privée » définie comme une possibilité de contrôle par l'individu sur l'espace physique et informationnel qu'il choisit d'ôter du regard du public pour protéger son droit à une liberté individuelle héritée des traditions libérales classiques utilitaristes, a abouti à remettre à l'agenda la question du droit *à la* vie privée dans les années 1960. Le débat sur ce sujet, né aux États-Unis au moment de la liquidation de l'ère du McCarthysme, s'est exporté en Europe à la fin des années 1960, où des acteurs institutionnels qui se sont rapidement constitués en réseau transgouvernemental ont cherché, conformément à des traditions de droit continental, à légiférer pour protéger cette conception libérale de la vie privée fondée sur l'idée de l'autonomie de l'individu qui doit pouvoir manifester son consentement au traitement de « toute donnée » le concernant.

Juridiquement, cela a consacré une rupture par rapport à des conceptions du droit *de la* vie privée qui protégeaient la barrière érigée collectivement entre l'espace privé et le public, par exemple au travers de réglementations protégeant l'inviolabilité du domicile ou le secret des correspondances, ou encore à travers une jurisprudence consacrant l'incompétence du juge pour connaître des affaires de violences dans l'espace privé domestique. Le fait que cette évolution juridique ait eu pour élément déclencheur l'irruption d'une informatique perçue comme un danger pour les droits fondamentaux est certes contingent, mais c'est ce qui de fait, historiquement, a conduit à cette évolution. Nous pouvons de la sorte dire que la transformation du milieu technique par l'informatique, qui transforme notre capacité d'agir notamment en matière d'information et de communication, a, en raison de la façon dont elle a été perçue à un moment particulier de l'Histoire, bel et bien transformé ce qu'est la « vie privée » en tant qu'objet du droit *à la* vie privée, en consacrant les notions de consentement et de donnée à caractère personnel inspirées par le paradigme libéral de la vie privée.

En 1819, Benjamin Contant remarquait que la Liberté des Modernes, qu'il définissait comme la capacité des individus à agir de façon autonome tout en déléguant le pouvoir de prendre des décisions collectives à des représentants, gagnait en popularité face à une Liberté des Anciens qui consistait à prendre part aux décisions collectives et à s'y soumettre :

> « [La liberté des Anciens] consistait à exercer collectivement, mais directement, plusieurs parties de la souveraineté toute entière, à délibérer, sur la place publique, de la guerre et de la paix, à conclure avec les étrangers des traités d'alliance, à voter les lois, à prononcer les jugements, à examiner les comptes, les actes, la gestion des magistrats, à les faire comparaître devant tout le peuple, à les mettre en accusation, à les condamner ou à les absoudre ; mais en même temps que c'était là ce que les Anciens nommaient liberté, ils admettaient comme compatible avec cette liberté collective l'assujettissement complet de l'individu à l'autorité de l'ensemble. » (Constant, 1989 [1819], p. 495)

Au contraire, la Liberté des Modernes se rapproche du principe de la liberté individuelle de John Stuart Mill et suppose :

> « […] le droit de n'être soumis qu'aux lois, de ne pouvoir être ni arrêté, ni détenu, ni mis à mort, ni maltraité d'aucune manière, par l'effet de la volonté arbitraire d'un ou de plusieurs individus : c'est pour chacun le droit de dire son opinion, de choisir son industrie, et de l'exercer, de disposer de sa propriété, d'en abuser même ; d'aller, de venir sans en obtenir la permission, et sans rendre compte de ses motifs ou de ses démarches. C'est, pour chacun, le droit de se réunir à d'autres individus, soit pour conférer sur ses intérêts, soit pour professer le culte que lui et ses associés préfèrent, soit simplement pour remplir ses jours ou ses heures d'une manière plus conforme à ses inclinations, à ses fantaisies. » (Constant, 1980 [1819], p. 494-495)

Il nous semble qu'un parallèle peut être tracé entre la Liberté des Anciens et des Modernes et les deux formes de vie privée dont nous venons de discuter des différences. Celle qui repose sur une distinction collectivement élaborée et défendue entre espaces public et privé protégeant ce dernier du regard extérieur nous semble correspondre à cette Liberté des Anciens. Elle se traduit notamment par l'interdiction pour la puissance publique d'intervenir dans l'espace protégé du domicile ou de la correspondance privée, mais peut empêcher certains sujets d'accéder à la notoriété de l'espace public contre la volonté de la personne concernée. À l'inverse, une vie privée désignant un contrôle de l'individu sur son espace physique et informationnel, en fonction de ses propres préférences, pour défendre son autonomie, et qui se traduit par un droit à l'auto-détermination et des mécanismes de consentement, nous paraît relever de la Liberté des Modernes.

Nous avions vu dans l'introduction que de nombreux travaux de recherche ont démontré l'existence d'un paradoxe de la vie privée : les internautes, même s'ils déclarent accorder beaucoup d'importance à leur « vie privée », ont des comportements qui la mettent en péril, puisqu'ils acceptent (ou accepteraient) en pratique facilement de partager des informations qui relèvent de cette même « vie privée ». La distinction entre une « Vie privée des Anciens » et une « Vie privée des Modernes » pourrait fournir un élément d'explication supplémentaire à ce paradoxe (Rossi, 2019) .

En effet, ce paradoxe, tel que décrit dans une large part de la littérature, existe surtout si nous considérons que la « vie privée » implique une frontière public/privé définie collectivement par des normes sociales, par exemple de pudeur, s'imposant à tous : tant les personnes que le droit désigne comme les « personnes concernées » que les « responsables du traitement ». Dans ce cas, partager des contenus qui relèvent de la vie privée sur des réseaux sociaux et participer à des pratiques de mise en visibilité de soi, ou accepter de partager des données en échange d'un service nécessitant ces données, paraît en effet impudique et imprudent. Collectivement, ces comportements s'interprètent alors comme un renoncement à se protéger de l'intrusion du regard d'autrui, puisque nous fournissons volontairement aux surveillants les données qui nous concernent.

Mais de telles pratiques sont nettement moins paradoxales si nous adoptons le point de vue selon lequel le droit *à la* vie privée est un droit au contrôle de l'information qui nous concerne. Dans ce cas, il est tout à fait possible de partager avec une audience *choisie* les contenus de son choix – même de nature intime – tout en maintenant une revendication au *contrôle* sur la circulation et l'utilisation de cette information, par exemple en pouvant choisir à tout moment de l'effacer, en pouvant interdire au prestataire du service utilisé pour communiquer cette information de l'utiliser pour ses propres fins, et cela en ayant par ailleurs le droit de consentir librement à des usages que la morale collective pourrait réprouver, par exemple au nom des normes de pudeur. Dans un tel scénario, ce n'est plus à la personne concernée de ne rien partager de « privé » dans des espaces « publics », mais aux personnes (physiques ou morales) à qui *n'importe quelle* information sur cette personne est confiée de s'assurer du respect des ses *choix* communicationnels.

Bien entendu, de la même façon que l'existence du droit de vote montre que des formes de Liberté des Anciens perdurent encore, toute notion de protection d'un espace privé retiré de l'œil du public et de l'État n'a pas disparu, y compris dans le droit. L'article 9 du RGPD maintient une protection renforcée pour des données sensibles comme l'opinion politique, la santé ou l'orientation et la vie sexuelles. Le secret des correspondances et le principe de l'inviolabilité du domicile existent toujours. L'existence d'autorités de contrôle et de procédures d'action collective dans le RGPD relèvent de mécanismes de décision collective. Mais il nous semble que l'invention du droit *à la* protection des données à caractère personnel, fondé sur une définition de la donnée personnelle qui porte sur *toute* information quelle que soit sa nature, ne

peut être comprise qu'à l'aune d'une consécration par le législateur d'une conception Moderne de la vie privée comme droit individuel à l'auto-détermination.

L'évolution du droit *à la* vie privée manifestée par l'adoption du droit *de la* protection des données à caractère personnel nous semble ainsi s'inscrire dans le mouvement historique de la modernité et de ses évolutions (voir : Bauman, 2000). Cela est vrai aussi pour les pratiques de surveillance – horizontales et verticales – que les rédacteurs de ces règles de droit ont voulu encadrer. De nombreux travaux ont déjà montré comment l'informatique, le traitement automatisé de données à caractère personnelle et le profilage des populations (Vitalis et Mattelart, 2014) s'inscrivent dans des processus au temps long de transformation du pouvoir, dans l'histoire du passage de la société de souveraineté à la société de discipline à la société de contrôle (Deleuze, 1990 ; Foucault, 1975 ; Simon, 2002), aboutissant à une gouvernementalité algorithmique (Rouvroy et Berns, 2013) exploitant les techniques de surveillance informatisée pour imposer des formes nouvelles de contrôle social à une société de modernité liquide (voir : Bauman et Lyon, 2013).

La question de savoir si cette évolution des conceptions juridiques exprimées dans les arènes spécialisées dans lesquelles sont produits les textes normatifs de protection des données personnelles s'applique à l'ensemble de la société, et se traduit effectivement par une évolution des pratiques communicationnelles de vie privée, est encore à vérifier. Là où cette thèse s'est concentrée sur sa production, il serait pertinent de poursuivre les recherches par l'étude de la réception de l'action publique en matière de protection des données. Les textes normatifs que nous avons étudiés sont-ils décodés par leur public comme protégeant une vie privée fondée sur le contrôle individuel, ou bien sur la distinction collectivement établie entre le public et le privé ? Est-ce que cela a une incidence sur la mise en pratique de ces règles, et donc sur la matérialité des dispositifs de traitement des données personnelles qu'elles cherchent à encadrer ? L'évolution des normes juridiques (dures ou souples) est-elle la conséquence, la cause ou totalement décorrélée des évolutions dans les normes et les pratiques sociales de communication et de vie privée ? Ces questions sont des pistes de recherche futures que nous formulons au terme de ce travail de recherche sur la production des normes de protection des données.

Pour conclure, la protection de la vie privée comme des données personnelles est une matière *politique* et non *technique* comme notre première hypothèse initiale le suggérait. S'il fallait donc ne retenir qu'une seule conclusion à l'issue de tout ce qui précède, c'est qu'il est vain d'attendre d'un débat entre experts une réponse à des questions comme ce que devrait être la vie privée, sa désirabilité sociale, et les règles qui doivent régir le fonctionnement, la configuration matérielle et l'évolution de notre milieu technique.

Bibliographie

Travaux cités

ACQUISTI A., GROSS R., 2006, « Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook », *Proceedings of the 6th International Conference on Privacy Enhancing Technologies*, p. 36-58.

ACQUISTI A., IDA M.F.MB., ROCHELANDET F., 2011, « Les comportements de vie privée face au commerce électronique », *Réseaux*, 167, p. 105-130.

ADLER E., HAAS P.M., 1992, « Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program », *International Organization*, *46*, 1, p. 367-390.

AGRE P.E., 1994, « Surveillance and capture: Two models of privacy », *The Information Society*, *10*, 2, p. 101-127.

AKRICH M., 1993, « Technique et médiation », *Réseaux. Communication - Technologie - Société*, *11*, 60, p. 87-98.

ALBRECHT J.P., 2015b, « No EU Data Protection Standard Below the Level of 1995 », *European Data Protection Law Review*, *1*, 1, p. 3-4.

ALLEN A., 1999, « Coercing Privacy », *William and Mary Law Review*, volume 40, p. 723 et s.

ALLEN A., 2000, « Gender and Privacy in Cyberspace », *Faculty Scholarship at Penn Law*, 789.

ALLEN A., 1988, *Uneasy Access: Privacy for Women in a Free Society*, Rowman & Littlefield.

ALTMAN I., 1977, « Privacy Regulation: Culturally Universal or Culturally Specific? », *Journal of Social Issues*, *33*, 3, p. 66-84.

ALVESTRAND H.T., WIUM LIE H., 2009, « Development of Core Internet Standards: The Work of IETF and W3C », dans BYGRAVE Lee A. et BING Jon (dir.), *Internet Governance: Infrastructure and Institutions*, Oxford, Oxford University Press, p. 126-146.

ANCIAUX A., FARCHY J., MÉADEL C., 2017, « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », *Revue d'economie industrielle*, *n° 158*, 2, p. 9-41.

ANIĆ I.-D., BUDAK J., RAJH E., RECHER V., ŠKARE V., ŠKRINJARIĆ B., ŽOKALJ M., 2018, *The Extended Model of Online Privacy Concern*, Zagreb, Institute of Economics Zagreb.

ARENDT H., 1998, *The Human Condition*, 2nd edition, Chicago, The University of Chicago Press.

ATTEN M., 2013, « Ce que les bases de données font à la vie privée », *Réseaux*, 178-179, p. 21-53.

AUSTIN J.L., 1970, *Quand dire, c'est faire*, LANE G. (dir.), Paris, Seuil.

BACHIMONT B., 2010, *Le sens de la technique: le numérique et le calcul*, Paris, Belles lettres (Encre marine).

BADOUARD R., 2012, « Faire participer. Un enjeu de légitimité pour l'Union européenne », *Participations*, *3*, 2, p. 207-218.

BADOUARD R., MABI C., MONNOYER-SMITH L., 2016, « Le débat et ses arènes », *Questions de communication*, 30, p. 7-23.

BADOUARD R., MABI C., SIRE G., 2016, « Beyond "Points of Control": logics of digital governmentality », *Internet Policy Review*, *5*, 3.

BALDÉ K., 2015, *The global e-waste monitor 2014 quantities, flows and resources*, Bonn, United Nations Univ., Institute for the advanced study on sustainability.

BAMBERGER K.A., MULLIGAN D.K., 2015, *Privacy on the ground: driving corporate behavior in the United States and Europe*, Cambridge, Massachusetts, The MIT Press (Information policy series).

BARAN P., 1964, *On Distributed Communications: I. Introduction to Distributed Communications Networks*, RAND Corporation.

BARNES S.B., 2006, « A privacy paradox: Social networking in the United States », *First Monday*, *11*, 9.

BARTHES R., 2014, *Mythologies*, Paris, Points.

BARTHES R., 2015, *L'Aventure sémiologique*, Le Seuil.

BAUMAN Z., 2000, *Liquid modernity*, Cambridge, UK : Malden, MA, Polity Press ; Blackwell.

BAUMAN Z., LYON D., 2013, *Liquid surveillance: a conversation*, Cambridge, UK ; Malden, MA, Polity Press (Polity conversations series).

BEAUD S., WEBER F., 2017, *Guide de l'enquête de terrain: produire et analyser des données ethnographiques*, Paris, La Découverte.

BELLI L., 2016, *De la gouvernance à la régulation de l'Internet*, Boulogne-Billancourt, Berger-Levrault.

BELLON A., 2019, « Numérisation des politiques culturelles en France », dans GEORGE É. (dir.), *Numérisation de la société et enjeux sociopolitiques. Tome 1. Numérique, communication et culture*, Londres, ISTE (Systèmes d'information, Web et société), p. 169-176.

BENFORD R.D., SNOW D.A., PLOUCHARD N.M., 2012, « Processus de cadrage et mouvements sociaux : présentation et bilan », *Politix, n° 99*, 3, p. 217-255.

BENNETT C.J., 1991, « What Is Policy Convergence and What Causes It? », *British Journal of Political Science*, *21*, 2, p. 215-233.

BENNETT C.J., 1992, *Regulating privacy: Data protection and public policy in Europe and the United States*, Ithaca, N.Y., Cornell University Press.

BENNETT C.J., 2008, *The privacy advocates: resisting the spread of surveillance*, Cambridge, MA, MIT Press.

BENNETT C.J., RAAB C.D., 2003, *The Governance of Privacy. Policy Instruments in Global Perspective*, Aldershot, Ashgate.

BENOIT A., 2014, « L'« espace public » à l'épreuve de la critique féministe », *Philonsorbonne*, 8, pp. 121-131

BENTHAM J., 1791, *Panopticon Or the Inspection House*, London, T. Payne.

BERGERON H., SUREL Y., VALLUY J., 1998, « L'Advocacy Coalition Framework. Une contribution au renouvellement des études de politiques publiques ? », *Politix, 11*, 41, p. 195-223.

BERLIN I., 1969, « Two concepts of liberty », dans *Four Essays on Liberty*, Oxford, Oxford University Press, p. 118-172.

BERNSTEIN P.L., 1998, *Against the gods: the remarkable story of risk*, New York, NY, Wiley.

BIGOT J.-É., 2018, *Instruments, pratiques et enjeux d'une recherche numériquement équipée en sciences humaines et sociales*, Thèse de doctorat, Compiègne, Université de technologie de Compiègne.

BIJKER W.E., 1995, *Of bicycles, bakelites, and bulbs: toward a theory of sociotechnical change*, Cambridge, Mass., MIT Press (Inside technology).

BING J., 2009, « Building cyberspace: a brief history of Internet », dans *Internet Governance: Infrastructure and Institutions*, Oxford, Oxford University Press, p. 8-47.

BIRD K., 2001, « L'impossible réglementation des propos à caractère raciste aux États-unis », *Revue française de droit constitutionnel*, *46*, 2, p. 265-287.

BLOUSTEIN E.J., 1964, « Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser », *New York University Law Review*, *39*, p. 962 et s.

BODIN J., 1576, *Les Six Livres de la République*, Paris, Jacques du Puy.

BONACCORSI J., JULLIARD V., 2010, « Dispositifs de communication numériques et médiation du politique. Le cas du site web d'Ideal-Eu », dans AGHABABAIE M., BONJOUR A., CLERC A., RAUSCHER G. (dirs.), *Usages et enjeux des dispositifs de médiation*, Nancy, Presses universitaires de Nancy, p. 65-78.

BONENFANT M., MONDOUX A., MÉNARD M., OUELLET M., 2015, « Big Data, médiation symbolique et gouvernementalité », dans *Big Data - Open Data : Quelles valeurs ? Quels enjeux ?*, De Boeck Supérieur, p. 31 et s.

BÖRÖCZ I., 2016, « Risk to the Right to the Protection of Personal Data »:, *European Data Protection Law Review*, *2*, 4, p. 467-480.

BOTTINI T., JULLIARD V., 2017, « Entre informatique et sémiotique », *Réseaux*, *n° 204*, 4, p. 35-69.

BOULLIER D., 2015, « Vie et mort des sciences sociales avec le big data », *Socio. La nouvelle revue des sciences sociales*, 4, p. 19-37.

BOUMAZA M., 2001, « L'expérience d'une jeune chercheuse en "milieu extrême" : Une enquête au Front national », *Regards sociologiques*, *22*, p. 105-121.

BOURDELOIE H., 2014, « Ce que le numérique fait aux sciences humaines et sociales. épistémologie, méthodes et outils en questions », *tic&société*, Vol. 7, N° 2, p. 7-38.

BOURG D., 2007, « Le défi de la dématérialisation », *Entropia*, 3, p. 19-30.

BOUWEN P., 2002, « Corporate lobbying in the European Union: the logic of access », *Journal of European Public Policy*, *9*, 3, p. 365-390.

BOUWEN P., 2009, « The European Commission », dans *Lobbying the European Union: Institutions, Actors, and Issues*, Oxford ; New York, OUP Oxford, p. 19-38.

BOWEN G.A., 2009, « Document Analysis as a Qualitative Research Method », *Qualitative Research Journal*, *9*, 2, p. 27-40.

BOYADJIAN J., 2014, « Twitter, un nouveau « baromètre de l'opinion publique » ? », *Participations*, 8, p. 55-74.

BOYADJIAN J., 2016, « La science politique face aux enjeux du big data et de la protection des données personnelles sur internet », *Revue de Droit public*, 1, p. 7 et s.

BRAUNSTEIN P., 1985, « Approches de l'intimité XIVe-Xve siècle », dans ARIÈS P., DUBY G. (dirs.), *Histoire de la vie privée. Tome 2 : De l'Europe féodale à la Renaissance*, Paris, Seuil, p. 526-619.

BRETON P., 1997, *L' utopie de la communication: le mythe du village planétaire*, Paris, Éd. La Découverte (La découverte poche Essais).

BROCA S., 2013, *Utopie du logiciel libre ; du bricolage informatique à la réinvention sociale*, Neuvy-en-Champagne, Le passager clandestin.

BROUWER R., 2008, *LIBERTICIDE: kritische reflecties op het neoliberalisme*, Utrecht, IJzer Uitgeverij.

BROWN A.E., STEWART J.JR., 1993, « Competing Advocacy Coalitions, Policy Evolution and Airline Deregulation », dans SABATIER P.A., JENKINS-SMITH H.C. (dirs.), *Policy change and learning: an advocacy coalition approach*, Boulder, Colo, Westview Press (Theoretical lenses on public policy), p. 83-103.

BUTLER J., 1997, *Excitable speech: a politics of the performative*, New York, Routledge.

BUTLER J., 2010, « Performative Agency », *Journal of Cultural Economy*, *3*, 2, p. 147-161.

CALLEGATI F., CERRONI W., RAMILLI M., 2009, « Man-in-the-Middle Attack to the HTTPS Protocol », *IEEE Security Privacy*, *7*, 1, p. 78-81.

CALOQUE-BERGÈS C., 2018, « La genèse autonome des réseaux de données en France et en Europe (1978-1992) », *Réseaux*, 210, p. 151-178.

CARANTA, R., ANDENAS, M., FAIRGRIEVE, D. (dirs.), 2004, *Independent Administrative Authorities*, London, British Institute of International and Comparative Law.

CARBONNIER J., 2001, *Flexible droit*, Paris, LGDJ.

CARDON D., 2019, *Culture numérique*, Paris, Presses de Sciences Po (Petites humanités).

CARDON D., CASILLI A.A., 2015, *Qu'est-ce que le digital labor ?*, Bry-sur-Marne, INA.

CARRÉ D., PANICO R., 2012, « L'«affichage de soi» comme «puissance d'agir». Contrôle social et enjeux éthiques à l'heure de l'hyperconnectivité », dans PROULX S., MILLETTE M., HEATON L. (dirs.), *Médias sociaux: enjeux pour la communication*, Québec, Presses de l'université du Québec, p. 61-79.

CASILLI A.A., 2013, « Contre l'hypothèse de la « fin de la vie privée » », *Revue française des sciences de l'information et de la communication*, 3.

CASILLI A.A., 2015, « Digital Labor : Travail, technologies et conflictualités », dans *Qu'est-ce que le digital labor ?*, Bry-sur-Marne, INA, p. 8-40.

CASILLI A.A., 2019, *En attendant les robots: enquête sur le travail du clic*, Paris XIXe, Éditions du Seuil (La Couleur des idées).

CASTELLS M., 1998, *La société en réseaux. Tome 1 : l'ère de l'information*, Paris, Fayard.

CASTETS-RENARD C., 2018, « Personnalité juridique et identification numérique », dans BIOY X. (dir.), *La personnalité juridique*, Toulouse, Presses de l'Université Toulouse 1 Capitole (Travaux de l'IFR), p. 305-317.

CASTEX L., HARBINJA E., ROSSI J., 2018, « Défendre les vivants ou les morts ? », *Réseaux*, 210, p. 117-148.

CASTORIADIS C., 2006, *L'institution imaginaire de la société*, Nachdr., Paris, Éd. du Seuil (Points Essais).

CAVOUKIAN A., 2013, « Privacy by Design: Leadership, Methods and Results », dans GUTWIRTH S., LEENES R., HERT P. DE, POULLET Y. (dirs.), *European Data Protection: Coming of Age*, Dordrecht, Springer Netherlands, p. 175-202.

CAZALA J., 2011, « « Le Soft Law international entre inspiration et aspiration » », *Revue interdisciplinaire d'études juridiques*, *66*, 1, p. 41 et s.

CECERE G., GUEL F.L., ROCHELANDET F., 2015, « Les modèles d'affaires numériques sont-ils trop indiscrets ? », *Réseaux*, 189, p. 77-101.

CECERE G., ROCHELANDET F., 2013, « Privacy Intrusiveness and Web Audiences: Empirical Evidence », *Telecommunication Policy*, *37*, 10, p. 1004–1014.

CEFAÏ D., 1996, « La construction des problèmes publics. Définitions de situations dans des arènes publiques », *Réseaux*, *14*, 75, p. 43-66.

CHEMILLIER-GENDREAU M., 2006, « Faut-il un statut international de réfugié écologique ? », *Revue européenne de droit de l'environnement*, *10*, 4, p. 446-452.

CHEVALLIER J., 2003, « La gouvernance, un nouveau paradigme étatique ? », *Revue française d'administration publique*, n° 105-106, p. 203-217.

CLARKE R., 1988, « Information Technology and Dataveillance », *Commun. ACM*, *31*, 5, p. 498–512.

CLÉMENT-FONTAINE M., 2017, « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *LEGICOM*, *N° 59*, 2, p. 61-68.

COCHET Y., 2017, *Chapitre 1 - Ce que l'effondrement révèle de la nature humaine*, dans : Agnès Sinaï (éd.), *Gouverner la décroissance. Politiques de l'Anthropocène III*, Paris, Presses de Sciences Po, p. 25-46.

COHEN D., POSTEL J.B., 1983, « The ISO Reference Model and Other Protocol Architectures », dans *Information Processing 83: Proc. IFIP 9th World Computer Congress*, North Holland, New York, R.E.A. Mason, p. 29-34.

COLLOMB C., 2016, *Un concept technologique de trace numérique*, Thèse de doctorat, Compiègne, Université de technologie de Compiègne et Université libre de Bruxelles.

CONSTANT B., 1989, *De la liberté chez les modernes: écrits politiques*, GAUCHET M. (dir.), Paris, Hachette (Collection Pluriel).

CONSTANT B., 2010, *De la liberté des anciens comparée à celle des modernes*, Paris, Mille et une nuits.

CONTRERAS J.L., 2016, « Patents and Internet Standards », *Global Commission on Internet Governance - Paper Series*, 29, Waterloo, ON and London, England, Centre for International Governance and Innovation and Chatham House.

COOLEY T., 1879, *Treatise on the Law of Torts*, Chicago, Callagan.

COURNIL C., 2010, « Émergence et faisabilité des protections en discussion sur les « réfugiés environnementaux » », *Revue Tiers Monde*, *n°204*, 4, p. 35-54.

COUTURE S., TOUPIN S., 2017, « What Does the Concept of "Sovereignty" Mean in Digital, Network and Technological Sovereignty? », *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017*.

CRÉAC'H X., 2002, « Les évolutions dans l'interprétation du terme réfugié », *Hommes et Migrations*, *1238*, 1, p. 65-74.

CREMER C., EICHHAMMER W., FRIEDEWALD M., GEORGIEFF P., RIETH-HOERST S., SCHLOMANN B., ZOCHE P., AEBISCHER B., HUSER A., 2003, « Energy Consumption of Information and Communication Technology (ICT) in Germany up to 2010. Summary of the final report to the German Federal Ministry of Economics and Labour », Karlsruhe/Zurich, Centre for Energy Policy and Economics and Fraunhofer Institut Systemtechnik und Innovationsforschung.

CRESPY A., RAVINET P., 2014, « Les avatars du néo-libéralisme dans la fabrique des politiques européennes », *Gouvernement et action publique*, *N° 2*, 2, p. 9-29.

DACHEUX É., 2008, « Nouvelle approche de l'espace public européen. Dépasser le clivage entre sciences de l'information et de la communication et science politique », *Questions de communication*, 14, p. 221-242.

DAGIRAL É., LICOPPE C., MARTIN O., PHARABOD A.-S., 2019, « Le Quantified Self en question(s) », *Réseaux*, *n° 216*, 4, p. 17-54.

DAVID R., JAUFFRET-SPINOSI C., GORÉ M., 2016, *Les grands systèmes de droit contemporains*, 12e édition, Paris, Dalloz (Précis), 539 p.

DECEW J., 2018, « Privacy », dans ZALTA E.N. (dir.), *The Stanford Encyclopedia of Philosophy*, Spring 2018, Metaphysics Research Lab, Stanford University.

DECEW J.W., 2015, « The feminist critique of privacy: past arguments and new social understandings », dans ROESSLER B., MOKROSINSKA D. (dirs.), *Social Dimensions of Privacy*, Cambridge, Cambridge University Press, p. 85-103.

DEHOUSSE R., BENDJABALLAH S., MICHAUD G., ROZENBERG O., DELOCHE-GAUDEZ F., AZZI G.C., COSTA O., LALANDE R., 2017, « L'Observatory of European Institutions », *Politique européenne*, *N° 58*, 4, p. 14-42.

DEHOUSSE R., NOVAK S., BENDJABALLAH S., 2017, « Consensus under pressure », *Politique européenne*, *N° 58*, 4, p. 44-70.

DELEUZE G., 1990, « Post-scriptum sur les sociétés de contrôle », dans *Pourparlers*, Paris, Les éditions de Minuit, p. 240-247.

DELMAS C., 2011, *Sociologie politique de l'expertise*, Paris, La Découverte (Repères).

DENARDIS L., 2014, *The global war for internet governance*, New Haven London, Yale University Press.

DESROSIÈRES A., 2014, *Prouver et gouverner: une analyse politique des statistiques publiques*, Paris, La Découverte.

DIAS M., 2007, « L'illusion technologique », *Entropia*, 3, p. 31-36.

DIJCK J. VAN, 2014, « Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology », *Surveillance & Society*, *12*, 2, p. 197-208.

DODIER N., 1999, « L'espace public de la recherche médicale. Autour de l'affaire de la ciclosporine », *Reseaux*, *n° 95*, 4, p. 107-154.

DOTY N., 2015, « Reviewing for Privacy in Internet and Web Standard-Setting », *2015 IEEE Security and Privacy Workshops*, p. 185-192.

DOTY N., MULLIGAN D.K., 2013, « Internet Multistakeholder Processes and Techno-Policy Standards. », *Journal on Telecommunications and High Technology Law*, *11*, p. 135-184.

DOUEIHI M., 2008, *La grande conversion numérique*, Paris, Éd. du Seuil (La librairie du XXIe siècle).

DOUILLET A.-C., MAILLARD J. DE, 2010, « Les comités d'experts : une ressource institutionnelle pas toujours maîtrisée. », *Politique européenne*, *n° 32*, 3, p. 77-98.

DRAPER H., 1965, *Berkeley: The New Student Revolt*, New York, Grove Press.

DUBOIS V., 1999, *La politique culturelle. Genèse d'une catégorie d'intervention publique*, Paris, Belin (Socio-histoires).

DUBOIS V., 2010, « Les champs de l'action publique », *Papier publié sur HAL-SHS, id : halshs-00498020, version 1*.

DUBOIS V., 2014, « L'Etat, l'action publique et la sociologie des champs », *Swiss Political Science Review*, *20*, 1, p. 25-30.S

DUMONT B., 2011, « La régulation à l'échelle communautaire. Une analyse économique des instruments et institutions de la protection des données au sein de l'UE », *Réseaux*, *167*, 3, p. 49-73.

DUPUY G., 1982, « Téléphone pour la ville: l'enjeu urbain des centraux », *Métropolis*, 52-53, p. 29-37.

DURKHEIM E., 1893, *De la division du travail social*, Paris, Félix Alcan.

EBERLEIN B., NEWMAN A., 2006, « Innovating EU Governance Modes: the rise of incorporated transgovernmental networks », Chicago, Ill., 14th Conference of Europeanists.

ELGIE R., 2002, « The politics of the European Central Bank: principal-agent theory and the democratic deficit », *Journal of European Public Policy*, *9*, 2, p. 186-200.

ELLUL J., 1954, *La technique ou l'enjeu du siècle*, Paris, Armand Colin.

ELLUL J., 1981, « Préface », dans *Informatique, pouvoir et libertés*, 2e édition, Paris, Economica (Politique comparée), p. 11-21.

ELLUL J., 2004, *Le système technicien*, 2e édition, Paris, Cherche Midi.

ENGELS F., 1978, « On Authority », dans *Marx-Engels Reader*, 2nd edition, New York, W. W. Norton and Co, p. 730-733.

EPSTEIN D., KATZENBACH C., MUSIANI F., 2016, « Doing internet governance: practices, controversies, infrastructures, and institutions », *Internet Policy Review*, 5 (3).

ERIKSEN E.O., 2009, *The unfinished democratization of Europe*, New York, NY, Oxford University Press.

ERMOSHINA K., MUSIANI F., 2017, « Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era », *Media and Communication*, *5*, 1, p. 42-53.

ESTIENNE Y., 2011, « Un monde de verre : Facebook ou les paradoxes de la vie privée (sur)exposée », *Terminal. Technologie de l'information, culture & société*, 108-109, p. 65-84.

ETZIONI A., 1999, *The Limits of Privacy*, New York, Basic Books.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (dir.), 2013, *Access to data protection remedies in the EU Member States*, Luxembourg, Publ. Off. of the Europ. Union (Freedoms).

EYNARD J., 2013, *Les données personnelles: quelle définition pour un régime de protection efficace?*, Paris, Michalon (Essai).

FAIVRET J.-P., MISSIKA J.-L., WOLTON D., 1977, *Les dégâts du progrès. Les travailleurs face au changement technique.*, Paris, Seuil.

FALQUE-PIERROTIN I., 2009, « Production et diffusion des données à caractère personnel sur Internet : enjeux nouveaux et questions éthiques », *La Gazette des archives*, *215*, 215, p. 175-178.

FAVRO K., 2017, « La démarche de compliance ou la mise en œuvre d'une approche inversée », *LEGICOM*, *N° 59*, 2, p. 21-28.

FEDERICI S., 2017, *Caliban et la sorcière: femmes, corps et accumulation primitive*, Genève, Ed. Entremonde.

FERRACIOLI L., 2014, « The Appeal and Danger of a New Refugee Convention », *Social Theory and Practice*, *40*, 1, p. 123-144.

FILLIEULE O., PÉCHU C., 1993, *Lutter ensemble. Les théories de l'action collective*, Paris, L'Harmattan.

FLAHERTY D.H., 1989, *Protecting Privacy in Surveillance Societies*, Chapel Hill and London, The University of North Carolina Press.

FLICHY P., 2001, *L'imaginaire d'Internet*, Paris, Découverte (Sciences et société).

FLIPO F., 2007, « L'infrastructure numérique en question », *Entropia*, 3, p. 67-85.

FLIPO F., DOBRÉ M., MICHOT M., 2013, *La face cachée du numérique: l'impact environnemental des nouvelles technologies*, Montreuil, Éditions L'Échappée (Collection Pour en finir avec).

FONTAN C., 2013, « Frankenstein en Europe. L'impact de la Banque centrale européenne sur la gestion de la crise de la zone euro », *Politique européenne*, *42*, 4, p. 22-45.

FONTAN C., 2014, « La BCE dans la crise : Qui décide quoi ? », *Pouvoirs*, *149*, 2, p. 91-100.

FONTANA A., FREY J.H., 2005, « The Interview: From Neutral Stance to Political Involvement », dans DENZIN N.K., LINCOLN Y.S. (dirs.), *The Sage handbook of qualitative research*, Thousand Oaks, CA, Sage, p. 695-727.

FOUCAULT M., 1975, *Surveiller et punir. Naissance de la prison*, Paris, Gallimard.

FOUCAULT M., 1976, *Histoire de la sexualité. Tome 1 : la volonté de savoir*, Paris, Gallimard.

FOUCAULT M., 1988, « Technologies of the Self », dans MARTIN L.H., GUTMAN H., HUTTON P.H. (dirs.), *Technologies of the Self. A Seminar with Michel Foucault*, Amherst, Massachussets, University of Massachusetts Press, p. 16-49.

FOUCAULT M., 2008, *L'archéologie du savoir*, Paris, Gallimard.

FRANÇOIS L., 2014, « Les droits nationaux de la liberté d'expression et le principe européen de proportionnalité », *LEGICOM*, *52*, 1, p. 101-107.

FRASER N., 1990, « Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy », *Social Text*, 25/26, p. 56-80.

FRASER N., 2007, « Special Section: Transnational Public Sphere: Transnationalizing the Public Sphere: On the Legitimacy and Efficacy of Public Opinion in a Post-Westphalian World », *Theory, Culture & Society*, *24*, 4, p. 7-30.

FREEMAN C., 1988, « Part I - Introduction », dans DOSI G., FREEMAN C., NELSON R., SILVERBERG G., SOETE L. (dirs.), *Technical Change and Economic Theory*, Londres, Pinter, p. 1-8.

FRIEDMAN M., 1960, *A program for monetary stability.*, New York, Fordham University Press.

FRIEDMAN M., 1962, *Capitalism and freedom*, Chicago, University of Chicago Press.

FRISON-ROCHE M.-A., 2016, « Le droit de la compliance », *Recueil Dalloz*, 32, p. 1871-1874.

FUCHS C., 2011, « Towards an alternative concept of privacy », *Journal of Information, Communication and Ethics in Society*, vol. 9 n° 4, p. 220-237

FUCHS, C. (dir.), 2012, *Internet and surveillance: the challenges of Web 2.0 and social media*, New York, Routledge (Routledge studies in science, technology and society).

GALINON-MÉLÉNEC B., 2011, « L'Homme trace, arguments », dans GALINON-MÉLÉNEC B. (dir.), *L'homme-trace : perspectives anthropologiques des traces contemporaines*, Paris, CNRS-éditions, p. 13-14.

GALLOUEDEC GENUYS F., MAISL H., 1976, *Le secret des fichiers*, Paris, Cujas (Cahier - Institut français des sciences administratives).

GANDY O., 1993, *The panoptic sort: A political economy of personal information*, Boulder, Col., Westview Press.

GELLERT R., 2016, « We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection », *European Data Protection Law Review (EDPL)*, *2*, p. 481 et s.

GEORGE É. (dir.), 2019, *Numérisation de la société et enjeux sociopolitiques*, Londres, ISTE.

GERBER N., GERBER P., VOLKAMER M., 2018, « Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior », *Computers & Security*, *77*, p. 226-261.

GILLIOM J., 2001, *Overseers of the poor: surveillance, resistance, and the limits of privacy*, Chicago, University of Chicago Press (The Chicago series in law and society).

GILL-PETERSON J., 2015, « Sexting girls: technological sovereignty and the digital », *Women & Performance: a journal of feminist theory*, *25*, 2, p. 143-156.

GLANCY D., 1979, « The Invention of the RIght to Privacy », *Arizona Law Review*, *21*, 1, p. 1-39.

GODIN B., 2016, « Making sense of innovation: from weapon to instrument to buzzword », *Quaderni. Communication, technologies, pouvoir*, 90, p. 21-40.

GOFFMAN E., 1974, *Frame Analysis: An Essay on the Organization of the Experience*, New York, Harper Colophon.

GOLDSTEIN R.J., 2006, « Prelude to McCarthyism: The Making of a Blacklist », *Prologue*, *38*, 3.

GONZÁLEZ FUSTER G., 2014a, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, Springer.

GONZÁLEZ FUSTER G., 2014b, « Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection », *Birkbeck Law Review*, *2*, 2, p. 263-278.

GOODY J., 1979, *La raison graphique, la domestication de la pensée sauvage*, Paris, Les éditions de minuit.

GOUGEON P., 1995, « «Nul n'est censé ignorer la loi». La publication au Journal officiel : genèse d'un mode d'universalisation de la «puissance publique» », *Politix. Revue des sciences sociales du politique*, *8*, 32, p. 66-88.

GOUPY M., 2014, « La bienveillante neutralité des technologies d'espionnage des communications : le cas tunisien », *Cultures & Conflits*, 93, p. 109-124.

GRAMSCI A., 2018, *Lettres de prison*, République des Lettres.

GRANT P., 1983, « Technological Sovereignty: Forgotten Factor in the "Hi-Tech" Razzamatazz », *Prometheus*, *1*, 2, p. 239-270.

GRAY C.M., KOU Y., BATTLES B., HOGGATT J., TOOMBS A.L., 2018, « The Dark (Patterns) Side of UX Design », *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, p. 1-14.

GREENLEAF G., 2008, « Privacy in Australia », dans : RULE J.B., GREENLEAF G., *Global Privacy Protection – The First Generation*, Cheltenham, Edward Elgar, p. 141-173

GROSSMAN E., SAURUGGER S., 2012, *Les groupes d'intérêt action collective et stratégies de représentation*, Paris, A. Colin.

GRUDIN J., 2001, « Desituating Action: Digital Representation of Context », *Human–Computer Interaction*, *16*, 2-4, p. 269-286.

GUERRAND R.-H., 1987, « Espaces privés », dans ARIÈS P., DUBY G. (dirs.), *Histoire de la vie privée. Tome 4 : De la Révolution à la Grande Guerre*, Paris, Seuil, p. 325-411.

GUSFIELD J.R., 1994, *The culture of public problems: drinking-driving and the Symbolic order*, Chicago, Univ. of Chicago Press.

HAAS E.B., 1958, *The Uniting of Europe: Political, Social, and Economic Forces, 1950-1957*, Stanford University Press.

HAAS P.M., 1989, « Do Regimes Matter? Epistemic Communities and Mediterranean Pollution Control », *International Organization*, *43*, 3, p. 377-403.

HABERMAS J., 1987, *Théorie de l'agir communicationnel*, Paris, Fayard.

HABERMAS J., 1988, *L'espace public: archéologie de la publicité comme dimension constitutive de la société bourgeoise*, Paris, Payot (Critique de la politique Payot).

HABERMAS J., 2000, *Après l'Etat-nation: Une nouvelle constellation politique*, Fayard.

HALL P.A., 1986, *Governing the economy: the politics of state intervention in Britain and France*, New York, Oxford University Press (Europe and the international order).

HALL P.A., 1993, « Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain », *Comparative Politics*, *25*, 3, p. 275 et s.

HALL S., 1994, « Codage/décodage », *Réseaux*, *12*, 68, p. 27-39.

HALPÉRIN J.-L., 2005, « L'essor de la « privacy » et l'usage des concepts juridiques », *Droit et societe*, 3, p. 765-782.

HAYEK F., 1944, *The Road to Serfdom*, Abingdon, Routledge Press.

HÉMONT F., GOUT M., à paraître, « Consentement résigné : en finir avec le Privacy Paradox », dans *Le profilage en ligne : entre libéralisme et régulation*, Paris, Mare et Martin.

HIRSHLEIFER J., 1971, « The Private and Social Value of Information and the Reward to Inventive Activity », *American Economic Review*, *61*, 4, p. 561-574.

HIRSHLEIFER J., 1980, « Privacy: Its Origin, Function, and Future », *Journal of Legal Studies*, *9*, 4.

HOBBES T., 2000, *Léviathan*, Paris, Folio.

HOLVAST J., 2013, *De volkstelling van 1971: verslag van de eerste brede maatschappelijke discussie over aantasting van privacy*, Zutphen, Paris.

HONDIUS F.W., 1975, *Emerging data protection in Europe*, Amsterdam, Elsevier.

HORIBE M., 1984, « Allgemeiner Zugang zu Daten und Schutz der Privatsphäre in Japan », dans BULL H.P., KITAGAWA Z. (dirs.), *Computer im Dienst der Gesellschaft?*, Carl Heymanns Verlag, Köln, p. 99 et s.

HUET R., SARROUY O., 2015, « Le fleuve et ses berges : la sociologie des controverses, ou la négation de l'existence », *Hermes*, *73*, 3, p. 101-108.

HUME D., 2000, *An enquiry concerning human understanding: a critical edition*, Oxford : New York, Clarendon Press ; Oxford University Press (The Clarendon edition of the works of David Hume).

HUSTINX P., 2013, « EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation ». Article basé sur un cours donné à l'Académie de droit européen de l'Institut université européen, 24th Session on European Union Law, 1 à 12 juillet 2013.

HYNDMAN P., 1987, « The 1951 Convention Definition of Refugee: An Appraisal with Particular Reference to the Case of Sri Lankan Tamil Applicants », *Human Rights Quarterly*, *9*, 1, p. 49-73.

IBEKWE-SANJUAN F., PAQUIENSÉGUY F., 2015, « Open, Big, Collaboration : trois utopies de l'innovation au xxie siècle », dans BROUDOUX É., CHARTRON G. (dirs.), *Big Data - Open Data : Quelles valeurs ? Quels enjeux ? Actes du colloque « Document numérique et société*, Louvain-la-Neuve, De Boeck Supérieur, p. 15-29.

ILLICH I., 2014, *La convivialité*, Paris, Seuil.

ILSHAMMAR L., 2007, « When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s », *Human IT*, *9*, 1, p. 6–37.

ISIDRO M.R., 2017, « La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679 », *La Ley mercantil*, 42, p. 1 et s.

JACQUE J.P., 2011, « Accession of the European Union to the European Convention on Human Rights and Fundamental Freedoms, The », *Common Market Law Review*, *48*, p. 995 et s.

JACQUÉ J.P., 2018, *Droit institutionnel de l'Union européenne*, Paris, DALLOZ.

JAKOBSON R., 1963, *Essais de linguistique générale*, traduit par RUWET N., Paris, France, Éd. de Minuit.

JAULIN A., 2014, « L'espace public dans l'Athènes classique », *Philonsorbonne*, 8, p. 155-165.

JAURÉGUIBERRY F., PROULX S., 2011, *Usages et enjeux des technologies de communication*, Toulouse, érès.

JEANNERET Y., 2011, « Complexité de la notion de trace », dans GALINON-MÉLÉNEC B. (dir.), *L'homme-trace : perspectives anthropologiques des traces contemporaines*, Paris, CNRS-éditions, p. 59-86.

JOBERT B., 1994, *Le tournant néo-libéral en Europe: idées et recettes dans les pratiques gouvernementales*, Paris, Harmattan.

JOBERT M., MÜLLER P., 1987, *L'État en action*, Paris, Presses Universitaires de France.

JONAS H., 1982, « Technology as a Subject for Ethics », *Social Research*, *49*, 4, p. 891-898.

JONES C.O., 1970, *An introduction to the study of public policy.*, Belmont, Ca., Duxbury Press.

JONES R., RAAB C., SZÉKELY I., 2018, « Surveillance and resilience: Relationships, dynamics, and consequences », *Democracy and Security*, p. 1-38.

JULLIARD V., 2004, « Une "femme machine" au travail : la "demoiselle du téléphone" », *Quaderni*, *56*, 1, p. 23-32.

KARABOGA M., 2018, « The emergence and analysis of European data protection regulation », dans *Managing Democracy in the Digital Age*, p. 29-52.

KATZ E., LAZARSFELD P.F., 2008, *Influence personnelle: Ce que les gens font des médias*, Paris; Paris, A. Colin ; INA.

KATZ J.E., RICE R.E., 2002, *Social consequences of Internet use: Access, involvement and interaction*, Cambirdge, Mass., MIT Press.

KELSEN H., 1962, *Théorie pure du droit*, Paris, Dalloz.

KEOHANE R.O., HOFFMANN S., 1994, « Institutional Change in Europe in the 1980s », dans *The European Union*, Palgrave, London, p. 237-255.

KEOHANE R.O., NYE J.S., 1974, « Transgovernmental Relations and International Organizations », *World Politics*, *27*, 1, p. 39-62.

KEYNES J.M., 1977, *Théorie générale de l'emploi, de l'intérêt et de la monnaie*, Paris, Payot.

KHATCHATOUROV A., 2018, « La confiance dans le numérique. Des signes extérieurs vers la régulation de soi. », dans LEVALLOIS-BARTH C. (dir.), *Signes de confiance, l'impact des labels sur la gestion des données personnelles*, Paris, Telecom ParisTech (Chaire et Valeurs des Politiques des Informations Personnelles), p. 5-20.

KILIAN W., 2010, « Germany », dans RULE J.B., GREENLEAF G. (dirs.), *Global privacy protection: the first generation*, Cheltenham, Edward Elgar, p. 80-106.

KIRBY M., 1980, « Transborder Data Flows and the "Basic Rules" of Data Privacy », *Stanford Journal of International Law*, *16*, p. 27 et s.

KIRBY M., 2017, « Privacy Today Something Old, Something New, Something Borrowed, Something Blue », *Journal of Law, Information & Science*, *25*.

KLEIN A., 2012, « Facebook, quand tu nous tiens », dans PROULX S., MILLETTE M., HEATON L. (dirs.), *Médias sociaux. Enjeux pour la communication*, Québec, Presses de l'Université du Québec, p. 105-116.

KLEINWÄCHTER W., 2012, « Internet, sociétés civiles et gouvernements : cohabitation ou choc des cultures ? », *Politique étrangère*, 2, p. 263-275.

KLIMAS T., VAIČIUKAITĖ J., 2008, « The Law of Recitals In European Community Legislation », *ILSA Journal of International & Comparative Law*, *15*, 1, p. 61-93.

KNIGHT F.H., 1921, *Risk, Uncertainty and Profit*, Boston, MA, Hart, Schaffner & Marx; Houghton Mifflin Co.

KOOPMAN C., 2013, *Genealogy as Critique: Foucault and the Problems of Modernity*, Bloomington, Indiana University Press.

KOOPS B.-J., NEWELL B.C., TIMAN T., ŠKORVÁNEK I., CHOKREVSKI T., GALIČ M., 2016, « A Typology of Privacy », SSRN Scholarly Paper, ID 2754043, Rochester, NY, Social Science Research Network.

KRANZBERG M., 1985, « The Information Age: Evolution of Revolution? », dans *Information Technologies and Social Transformation*, Washington, D.C., National Academies Press, p. 35-54.

KRAUS R., 2013, « Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants », *Journal of Privacy and Confidentiality*, *5*, 1.

KRIEG-PLANQUE A., 2009, *La notion de formule en analyse du discours: cadre théorique et méthodologique*, Besançon, Presses universitaires de Franche-Comté (Annales littéraires de l'Université de Franche-Comté).

KRIEG-PLANQUE A., 2010, « La formule "développement durable" : un opérateur de neutralisation de la conflictualité, The formula 'sustainable development' : an conflict-neutralizing operator », *Langage et société*, 134, p. 5-29.

KÜBLER D., 2002, « Les acteurs associatifs dans l'advocacy coalition framework : application aux politiques publiques de lutte contre la drogue en suisse », *Pyramides. Revue du Centre d'études et de recherches en administration publique*, 6, p. 83-102.

KUHN T.S., 1972, *La structure des révolutions scientifiques*, Paris, Flammarion.

KURZWEIL R., 2010, *The singularity is near: when humans transcend biology.*, London, Penguin.

LACROIX G., 1984, « Informatique et contrôle social », *Terminal*, 9, p. 26-27.

LANDES J.B., 1988, *Women and the Public Sphere in the Age of the French Revolution*, Cornell University Press.

LANDES J.B., 2003, « Further Thoughts on the Public/Private Distinction », *Journal of Women's History*, *15*, 2, p. 28-39.

LANEY D., 2001, « 3D Data Management: Controlling Data Volume, Velocity, and Variety », *META Group*, File 949, 6 févier 2001.

LANZING M., 2016, « The transparent self », *Ethics and Information Technology*, *18*, 1, p. 9-16.

LASCOUMES P., 2004, « La Gouvernementalité : de la critique de l'État aux technologies du pouvoir », *Le Portique*, 13-14, p. 1-15.

LASCOUMES P., LE GALÈS P., 2005, *Gouverner par les instruments*, Paris, Presses de Sciences Po.

LATOUCHE S., 2012, *L'Âge des limites*, Paris, Fayard/Mille et une nuits.

LATOUR B., 2004, *La fabrique du droit. Une ethnographie du Conseil d'Etat*, Nachdr., Paris, La Découverte.

LATZKO-TOTH G., PASTINELLI M., 2014, « Par-delà la dichotomie public/privé : la mise en visibilité des pratiques numériques et ses enjeux éthiques », *tic&société*, *7*, 2.

LAUGIER S., 2004, « Performativité, normativité et droit », *Archives de Philosophie*, *67*, 4, p. 607-627.

LAVELLE S., 2009, « Politiques des artefacts.: Ce que les choses font et ne font pas », *Cités*, *39*, 3, p. 39-51.

LE BRETON D., 2017, *La sociologie du risque*, Paris, PUF (Que sais-je ?).

LE GUERN P., 2007, « L'enquête par observation : méthode et enjeux », dans OLIVESI S. (dir.), *La recherche en SIC*, Grenoble, Presses universitaires de Grenoble, p. 13-33.

LENERT E., 2004, « A social shaping perspective on the development of the world wide web: The case of iCraveTV », *New Media & Society*, *6*, 2, p. 235-258.

LESSIG L., 1999, *Code and Other Laws of Cyberspace*, New York, Basic Books.

LESSIG L., 2000, « Code is Law. On Liberty in Cyberspace », *Harvard Magazine*. 1er janvier 2020.

LEVALLOIS-BARTH, C. (dir.), 2018, *Signes de confiance: l'impact des labels sur la gestion des données personnelles*, Paris, Telecom ParisTech.

LÉVY P., 2000, « La montée vers la noosphère », *Sociologie et sociétés*, *32*, 2, p. 19-30.

LINDBERG L.N., 1963, *The Political Dynamics of European Economic Integration*, Stanford University Press.

LOCKE J., 1999, *Traité du gouvernement civil*, traduit par MAZEL D., 2e éd. corr, Paris, Flammarion.

LOVELUCK B., 2015, « Internet, une société contre l'État ? », *Réseaux*, 192, p. 235-270.

LYON D., 1994, *The Electronic Eye: The Rise of Surveillance Society*, University of Minnesota Press.

LYON D., 2015, *Surveillance After Snowden*, Cambridge, Mass., Polity Press.

MABI C., 2013, « Inclusion des publics et matérialité des dispositifs participatifs », *Participations*, *7*, 3, p. 201-213.

MACHIAVEL N., 2007, *Le Prince*, Folio.

MACKINNON C.A., 1989, *Toward a Feminist Theory of the State*, Harvard University Press.

MAGNETTE P., 2009, *Le régime politique de l'Union européenne*, Presses de Sciences Po.

MAGNON X., 2008, *Théorie(s) du droit*, Paris, Ellipses (Manuel universités droit).

MANGENOT M., 2011, « La présidence du Conseil : sociologie d'une institution de l'Union européenne », *Politique europeenne*, *n° 35*, 3, p. 7-28.

MANNHEIM K., 2006, *Idéologie et utopie*, Paris, Éditions de la Maison des Sciences de l'Homme.

MANYIKA J., CHUI M., BROWN B., BUGHIN J., DOBBS R., ROXBURGH C., HUNG BYERS A., 2011, « Big data: The next frontier for innovation, competition and productivity », McKinsey Global Institute.

MARTIN-JUCHAT F., PIERRE J., 2011, « Facebook et les sites de socialisation : une surveillance consentie », dans GALINON-MÉLÉNEC B. (dir.), *L'homme trace: perspectives anthropologiques des traces contemporaines*, Paris, CNRS éditions, p. 105-123.

MARTY F., KIRAT T., 2018, « Les mutations du néolibéralisme américain quant à l'articulation des libertés économiques et de la démocratie », *Revue internationale de droit économique*, *t.XXXII*, 4, p. 471-498.

MARX K., 1872, *Le Capital*, Paris, Maurice Lachâtre.

MARX K., 2002, *Contribution à la critique de l'économie politique*, Chicoutimi, Université du Québec à Chicoutimi (Classiques des sciences sociales).

MASCETTI S., MONREALE A., RICCI A., GERINO A., 2013, « Anonimity : A Comparison Between the Legal and Computer Science Perspectives », dans *European Data Protection: Coming of Age*, Dordrecht, Springer, p. 85-115.

MASSIT-FOLLÉA F., 2014, « La régulation de l'internet : fictions et frictions », dans CARMES M., NOYER J.-M. (dirs.), *Les débats du numérique*, Paris, Presses des Mines (Territoires numériques), p. 17-45.

MATTELART A., 2007, *La globalisation de la surveillance: aux origines de l'ordre sécuritaire*, Paris, Découverte (Cahiers libres).

MAWHINNEY H.B., 1993, « An Advocacy Coalition Approach to Change in Canadian Education », dans SABATIER P.A., JENKINS-SMITH H.C. (dirs.), *Policy change and learning: an advocacy coalition approach*, Boulder, Colo, Westview Press (Theoretical lenses on public policy), p. 59-82.

MEARSHEIMER J.J., 1990, « Back to the Future: Instability in Europe after the Cold War », *International Security*, *15*, 1, p. 5-56.

MEINTS M., 2009, « The Relationship between Data Protection Legislation and Information Security Related Standards », dans MATYÁŠ V., FISCHER-HÜBNER S., CVRČEK D., ŠVENDA P. (dirs.), *The Future of Identity in the Information Society*, Berlin, Springer, p. 254-267.

MÉNY Y., THOENIG J.-C., 1989, *Politiques publiques*, Paris, PUF.

MESSERLIN P., 2009, « La politique commerciale », dans DEHOUSSE R. (dir.), *Politiques européennes*, Paris, Presses de Sciences Po, p. 149-170.

MEUNIER S., MCNAMARA K.R., 2007, *Making History: European Integration and Institutional Change at Fifty*, Oxford, Oxford University Press.

MIDDELAAR L. VAN, 2009, *De passage naar Europa: geschiedenis van een begin*, Groningen, Netherlands, Historische Uitgeverij.

MILL J.S., 1861, *Principes d'économie politique avec quelques unes de leurs applications à l'économie sociale*, 2nde édition, Paris, Guillaumin et Compagnie.

MILL J.S., 1882, *A System of Logic, Ratiocinative and Inductive, Being a Connected View of the Principles of Evidence, and the Scientific Methods of Scientific Investigation*, New York, Harper & Brothers.

MILL J.S., 1965, *Principles of Political Economy*, London, University of Toronto Press.

MILL J.S., 1989, *On liberty ; with The subjection of women ; and chapters on socialism*, COLLINI S. (dir.), Cambridge etNew York, Cambridge University Press (Cambridge texts in the history of political thought).

MILLER A.R., 1971, *The assault on privacy: computers, data banks, and dossiers*, Ann Arbor, University of Michigan Press.

MILLER D.E., 2019, « Harriet Taylor Mill », *Stanford Encyclopedia of Philosophy Archive*.

MILTGEN C.L., SMITH H.J., 2015, « Exploring information privacy regulation, risks, trust, and behavior », *Information & Management*, *52*, 6, p. 741-759.

MITRANY D., 1944, *A Working Peace System: An Argument for the Functional Development of International Organization*, Oxford University Press.

MONDOUX A., 2011, « Identité numérique et surveillance », *Les cahiers du numérique*, *7*, 1, p. 49-59.

MONTJOYE Y.-A. DE, RADAELLI L., SINGH V.K., PENTLAND A.S., 2015, « Unique in the shopping mall: On the reidentifiability of credit card metadata », *Science*, *347*, 6221, p. 536-539.

MOORE A.D., 2003, « Privacy: Its Meaning and Value », *American Philosophical Quarterly*, *40*, 3, p. 215-227.

MORAVCSIK A., 1991, « Negotiating the Single European Act: national interests and conventional statecraft in the European Community », *International Organization*, *45*, 01, p. 19-56.

MOROZOV E., 2015, *Le mirage numérique*, Paris, Les pairies ordinaires.

MOULIER BOUTANG Y., 2007, *Le capitalisme cognitif. La nouvelle grande transformation.*, Paris, Editions Amsterdam.

MOULIER BOUTANG Y., 1998, *De l'esclavage au salariat : économie historique du salariat bridé*, Paris, PUF.

MOURON P., 2018, « Pour ou contre la patrimonialité des données personnelles », *Papier publié sur HAL-SHS, id : hal-01823901, version 1*.

MUELLER M., 2010, *Networks and states: the global politics of Internet governance*, Cambridge, Mass, MIT Press (Information revolution and global politics).

MÜLLER P., 1984, *Le Technocrate et le Paysan*, Paris, Ouvrière.

MÜLLER P., 1997, « L'européanisation des politiques publiques », *Politiques et management public*, *15*, 1, p. 3-9.

MÜLLER P., 2000, « L'analyse cognitive des politiques publiques : vers une sociologie politique de l'action publique », *Revue française de science politique*, *50*, 50, p. 189-208.

MÜLLER P., 2011, *Les politiques publiques*, Paris, Presses universitaires de France.

MULLIGAN D.K., KOOPMAN C., DOTY N., 2016, « Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy », *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*.

MUMFORD L., 1938, *The culture of cities*, New York, Harcourt, Brace and Company.

MUMFORD L., 1964, « Authoritarian and Democratic Technics », *Technology and Culture*, *5*, 1, p. 1-8.

MUNRO J.F., 1993, « California Water Politics: Explaining Policy Change in a Cognitively Polarized Subsystem », dans SABATIER P.A., JENKINS-SMITH H.C. (dirs.), *Policy change and learning: an advocacy coalition approach*, Boulder, Colo, Westview Press (Theoretical lenses on public policy), p. 105-127.

MUSIANI F., 2015, « Edward Snowden, l'« homme-controverse » de la vie privée sur les réseaux », *Hermes, La Revue*, *n° 73*, 3, p. 209-215.

MUSIANI F., COGBURN D.L., DENARDIS L., LEVINSON N.S., 2016, *The Turn to Infrastructure in Internet Governance*, New York, Palgrave Macmillan US :Imprint: Palgrave Macmillan.

NELSON T.H., 1983, *Computer Lib*, South Bend, Ind, The Distributors.

NEWMAN A., 2008, *Protectors of Privacy. Regulating Personal Data in the Global Economy*, Ithaca, Cornell University Press.

NISSENBAUM H., 1998, « Protecting Privacy in an Information Age: The Problem of Privacy in Public », *Law and Philosophy*, *17*, 5/6, p. 559-596.

NISSENBAUM H., 2004, « Privacy as Contextual Integrity », *Washington Law Review*, *79*, 1, p. 119-158.

NISSENBAUM H.F., 2010, *Privacy in context: technology, policy, and the integrity of social life*, Stanford, Calif, Stanford Law Books.

NORBERG P.A., HOME D.R., HOME D.A., 2007, « The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors », *Journal of Consumer Affairs*, 41, p. 100-126.

NYE J.S., 2004, *Soft power: the means to success in world politics*, 1st ed, New York; N.Y, Public Affairs.

OHM P., 2010, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », *UCLA Law Review*, 57, p. 1701-1777.

OLEJNIK L., ACAR G., CASTELLUCCIA C., DÍAZ C., 2015, « The leaking battery: A privacy analysis of the HTML5 Battery Status API », *IACR Cryptology ePrint Archive, 2015*, p. 616 et s.

OLEJNIK L., ENGLEHARDT S., NARAYANAN A., 2017, « Battery Status Not Included: Assessing Privacy in Web Standards », *3rd International Workshop on Privacy Engineering (IWPE'17). San Jose, United States*.

OLIVIER DE SARDAN J.-P., 1993, « Le développement comme champ politique local », *Bulletin de l'APAD*, 6, p. 1-9.

OLLIVIER-YANIV C., 2018, « Présentation du dossier », *Politiques de communication*, *11*, 2, p. 5-14.

OLLIVIER-YANIV C., 2019, « Les publics institutionnels: réception et appropriation des informations et des recommandations », *Politiques de communication*, 2018/2, n° 11, p. 5-14.

OLLIVIER-YANIV C., à paraître. « La carrière des controverses de santé publique : dispersion des arènes et politisation. Le cas de la vaccination en France dans les années 2010 ». Dans : Pailliart I. (dir.), *Les nouveaux territoires de santé*, Londres, ISTE.

OLSEN J.P., 2002, « The Many Faces of Europeanization », *Journal of Common Market Studies*, *40*, 5, p. 921-952.

OPHIR S., 2016, « Big data for the humanities using Google Ngrams: Discovering hidden patterns of conceptual trends », *First Monday*, *21*, 7.

O'REILLY T., 2007, « What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software », *International Journal of Digital Economics*, 65, p. 17-37.

ORGOAN A., 2016, « L'appréciation du principe d'autonomie institutionnelle à l'aune des exigences d'indepéndance des Agences de réglementation nationales », *Journal d'actualité des droits européens*, 23.

ORIGGI G., 2004, « Is Trust an Epistemological Notion? », *Episteme*, *1*, 1, p. 61–72.

ORIGGI G., 2013, « Democracy and Trust in the Age of the Social Web », dans BOVERO M. (dir.), *Teoria Politica - Nuova Serie - Annali III*, Madrid, Marcial Pons, p. 23-38.

PACKARD V., 1965, *The Naked Society*, New York, Pocket Books Inc.

PARKER D.B., 1968, « Rules of Ethics in Information Processing », *Communications of the ACM*, *11*, 3, p. 198-201.

PAUGAM S., 2012, « S'affranchir des prénotions », dans PAUGAM S. (dir.), *L'enquête sociologique*, Paris, Presses Universitaires de France (Quadrige), p. 5-26.

PHARABOD A.-S., 2019, « « Faire ses 10 000 pas », vraiment ? », *Reseaux*, *n° 216*, 4, p. 157-187.

PHILIP C., 1975, « La Cour de Justice des Communautés et la protection des droits fondamentaux dans l'ordre juridique communautaire », *Annuaire Français de Droit International*, *21*, 1, p. 383-407.

PIERSON P., 2000, « Increasing Returns, Path Dependence, and the Study of Politics », *American Political Science Review*, *94*, 02, p. 251-267.

POINSOT E., 2005, « L'engagement communautaire d'Amnesty International », dans *Lobbyistes et lobbying de l'Union européenne. Trajectoires, formations et pratiques des représentants d'intérêts*, Strasbourg, PUS, p. 197-223.

POLÁNYI K., 2009, *La grande transformation: aux origines politiques et économiques de notre temps*, traduit par ANGENO M., MALAMOUD C., DUMONT L. (dir.), Paris, Gallimard.

POSNER R.A., 1977, « The Right of Privacy », *Georgia Law Review*, *12*, 3, p. 393-422.

POSNER R.A., 1978, « An economic theory of privacy », *Regulation*, p. 16-26.

POSNER R.A., 1981, « The Economics of Privacy », *The American Economic Review*, *71*, 2, p. 405-409.

POSTER M., 1995, « Databases as Discourse », dans *The second media age*, Cambridge, Polity Press, p. 78-94.

POULLET Y., 2010, « About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? », dans GUTWIRTH S., POULLET Y., DE HERT P. (dirs.), *Data Protection in a Profiled World*, Dordrecht, Springer Netherlands, p. 3-30.

PROSSER W., 1960, « Privacy », *California Law Review*, *48*, 3, p. 383 et s.

PROST A., 1987, « Frontières et espaces du privé », dans ARIÈS P., DUBY G. (dirs.), *Histoire de la vie privée. Tome 5 : De la Première Guerre mondiale à nos jours*, Paris, Seuil, p. 13-154.

QUELLE C., 2017, « The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too », dans LEENES R., BRAKEL R. VAN, GUTWIRTH S., HERT P. DE (dirs.), *Data Protection and Privacy: The Age of Intelligent Machines*, Oxford and Portland, Oregon, Hart Publishing, p. 33-62.

RAAB C.D., JONES R., SZÉKELY I., 2015, « Surveillance and Resilience in Theory and Practice », *Media and Communication*, *3*, 2, p. 21-41.

RAAB C., SZÉKELY I., 2017, « Data protection authorities and information technology », *Computer Law & Security Review*, *33*, 4, p. 421-433.

RÁNKI S., 2011, « A kriminalisztikai szövegnyelvészet hazai kutatástörténete 1960-tól 1990-ig », *E-Nyelv Magazin*, 2011/3.

RAVINET P., 2014, « La Commission européenne et l'enseignement supérieur », *Gouvernement et action publique*, *2*, 2, p. 81-102.

REGAN P.M., 1995, *Legislating Privacy: Technology, Social Values, and Public Policy*, Univ of North Carolina Press.

REIDENBERG J., 1997, « Lex Informatica: The Formulation of Information Policy Rules through Technology », *Texas Law Review*, p. 553-593.

REINACH A., 2004, *Les fondements a priori du Droit Civil*, traduit par CALAN R. DE, Paris, Librairie Philosophique Vrin.

REVILLARD A., 2018, « Saisir les conséquences d'une politique à partir de ses ressortissants. La réception de l'action publique », *Revue française de science politique*, *68*, 3, p. 469-491.

REY B., 2009, *La privacy à l'ère du numérique : une gestion par les tensions*, Thèse soutenue en 2009 à l'Université Paris 5.

REY B., 2012, « La privacy à l'ère du numérique », *Terminal. Technologie de l'information, culture & société*, 110, p. 91-103.

RICHARDS N.M., SOLOVE D.J., 2010, « Prosser's Privacy Law: A Mixed Legacy », *California Law Review*, *98*, 6, p. 1887-1924.

RICŒUR P., 1984, « L'idéologie et l'utopie : deux expressions de l'imaginaire social », *Autres Temps*, *2*, 1, p. 53-64.

RIEHL W.H., 1889, *Die Familie*, Stuttgart, Cotta'sche Buchhandlung.

RIOS-BORDES A., 2018, *Les savoirs de l'ombre : La surveillance militaire des populations aux États-Unis*, Paris, Éditions de l'École des Hautes Études en Sciences Sociales.

ROBERT C., 2003, « L'expertise comme mode d'administration communautaire : entre logiques technocratiques et stratégies d'alliance », *Politique européenne*, *11*, 3, p. 57-78.

ROCHELANDET F., 2010, *Économie des données personnelles et de la vie privée*, Paris, Découverte.

ROSANVALLON P., 1989, « The Development of Keynesianism in France », dans HALL P.A. (dir.), *The Political Power of Economic Ideas: Keynesianism across Nations*, Princeton, NJ, Princeton University Press, p. 171-194.

ROSENAU J.N., CZEMPIEL E.-O., 2009, *Governance Without Government.*, Cambridge, Cambridge University Press.

ROSSI J., 2013, *Les autorités nationales de protection des données personnelles dans l'Union européenne. Etude des causes des manquements constatés par la Cour de justice de l'Union européenne*, Mémoire soutenu à Lille, IEP de Lille.

ROSSI J., 2015a, « Données de recherche et vie privée : l'anonymat règle-t-il le problème ? », dans RASLE B. (dir.), *Correspondant informatique et libertés : bien plus qu'un métier*, Paris, AFCDP, p. 319-332.

ROSSI J., 2015b, « Les quatre modèles de Data Protection Officers en Europe », dans RASLE B. (dir.), *Correspondant informatique et libertés : bien plus qu'un métier*, Paris, AFCDP, p. 27-42.

ROSSI J., 2016, « Framing the Privacy Debate and Big Data Governmentality in Degrowth Theory », Degrowth Conference Budapest, Budapest - Corvinus Egyetem, 31 août 2016.

ROSSI J., 2017a, « Les enjeux de l'infrastructure numérique dans les politiques de développement », dans *Stabilité, intégration, coopération et développement*, Szeged, Centre universitaire francophone (Cahiers du Centre universitaire francophone), p. 141-166.

ROSSI J., 2017b, « Nemzeti konzultáció és adatvédelem », *Acta Humana*, *5*, 2, p. 43-60.

ROSSI J., 2017c, « Guide de la jurisprudence européenne en matière de protection des données à caractère personnel. Cour Européenne des Droits de l'Homme et Cour de Justice de l'Union Européenne », *Cahiers du COSTECH*, 1.

ROSSI J., 2019, « L'hypothèse de la vie privée des Anciens et des Modernes », dans GEORGE É. (dir.), *Numérisation de la société et enjeux sociopolitiques. Tome 1. Numérique, communication et culture*, Londres, ISTE (Systèmes d'information, Web et société), p. 77-88.

ROSSI J., BIGOT J.-É., 2018, « Traces numériques et recherche scientifique au prisme du droit des données personnelles », *Les Enjeux de l'information et de la communication, 19/2*, 2, p. 161-177.

ROUVROY A., BERNS T., 2013, « Gouvernementalité algorithmique et perspectives d'émancipation: Le disparate comme condition d'individuation par la relation ? », *Réseaux*, *177*, 1, p. 163-196.

ROUVROY A., POULLET Y., 2009, « The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy » GUTWIRTH S., POULLET Y., DE HERT P., TERWANGNE C. DE, NOUWT S. (dirs.), *Reinventing Data Protection?*, p. 45-76.

RUCKENSTEIN M., PANTZAR M., 2019, « Par-delà le Quantified Self », *Réseaux*, n° 216, p. 55-81.

RULE, J.B., GREENLEAF, G. (dirs.), 2010, *Global privacy protection: the first generation*, Cheltenham, Edward Elgar.

RUSSELL A.L., 2006, « "Rough Consensus and Running Code" and the Internet-OSI Standards War », *IEEE Annals of the History of Computing*, *28*, 3, p. 48-61.

RUSSELL A.L., 2003, « The W3C and Its Patent Policy Controversy: A Case Study of Authority and Legitimacy in Internet Governance », SSRN Scholarly Paper, ID 2056900, Rochester, NY, Social Science Research Network.

RUSSELL A.L., SCHAFER V., 2014, « In the Shadow of ARPANET and Internet: Louis Pouzin and the Cyclades Network in the 1970s », *Technology and Culture*, *55*, 4, p. 880-907.

SABATIER P., 1993, « Policy Change over a Decade or More », dans SABATIER P.A., JENKINS-SMITH H.C. (dirs.), *Policy change and learning: an advocacy coalition approach*, Boulder, Colo., Westview Press (Theoretical lenses on public policy), p. 13-39.

SABATIER P.A., 1998, « The Advocacy Coalition Framework: revisions and relevance for Europe », *Journal of European Public Policy*, *5*, 1, p. 98-130.

SABATIER, P.A., JENKINS-SMITH, H.C. (dirs.), 1993, *Policy change and learning: an advocacy coalition approach*, Boulder, Colo, Westview Press (Theoretical lenses on public policy), 290 p.

SAURON J.-L., RÉGUER-PETIT L., 2018, *Procédures européennes devant la CJUE (CJ et Tribunal), devant la CEDH: avec index thématique et de nombreux schémas explicatifs*, Paris, Gualino.

SAURUGGER S., 2012, « The Professionalization of EU's Civil Society. A conceptual framework », dans *New Participatory Dimensions in Civil Society: Professionalization and Individualized Collective Action*, London, Routledge, p. 69-83.

SAURUGGER S., HEIKE K., 2013, « Opening the Black Box : The professionalization of Interest Groups in the EU », *Interests Groups and Advocacy*, *2*, 2, p. 185-202.

SAURUGGER S., SUREL Y., 2006, « L'européanisation comme processus de transfert de politique publique », *Revue internationale de politique comparée*, *13*, 2, p. 179-211.

SCHARPF F.W., 2000, *Gouverner l'Europe*, Paris, Presses de Sciences Po.

SCHICK A., 2002, « Les agences à la recherche de principes », *Revue de l'OCDE sur la gestion budgétaire*, *2*, 1, p. 7-30.

SCHLIMMER S., 2018, « Accaparement des terres ou investissements agricoles bénéfiques ? », *Gouvernement et action publique*, *N° 2*, 2, p. 31-52.

SCHMELZER M., 2016, *The hegemony of growth: the OECD and the making of the economic growth paradigm*, Cambridge, Cambridge University Press.

SCHMITT E., 2015, « L'ambiguïté épistémologique des big data : le cas de la donnée web en sciences sociales », dans BROUDOUX É., CHARTRON G. (dirs.), *Big Data - Open Data : Quelles valeurs ? Quels enjeux ?Actes du colloque « Document numérique et société*, Louvain-la-Neuve, De Boeck Supérieur, p. 43-53.

SCHOLZ T., 2012, *Digital Labor: The Internet as Playground and Factory*, London, Routledge.

SCHWARTZ P.M., SOLOVE D., 2012, « PII 2.0: Privacy and a New Approach to Personal Information », *Privacy & Security Law Report*, 11.

SCOTT J.C., 2009, *The Art of Not Being Governed – An Anarchist History of Upland Southeast Asia*, New Haven, Yale University Press.

SÉNAC-SLAWINSKI R., 2008, « Du gender mainstreaming au paritarisme : genèse d'un concept controversé », *Cahiers du Genre*, 44, p. 27-47.

SHILS E., 1956, *The Torment of Secrecy: The Background and Consequences of American Security Policies*, Free Press.

SHILS E., 1966, « Privacy: Its Constitution and Vicissitudes », *Law and Contemporary Problems*, *31*, 2, p. 281-306.

SIEGHART P., 1976, *Privacy and computers*, London, Latimer New Dimensions.

SIMON B., 2002, « The Return of Panopticism: Supervision, Subjection and the New Surveillance », *Surveillance & Society*, *3*, 1, p. 1-20.

SIMONDON G., 1958, *Du mode d'existence des objets techniques*, Paris, Aubier-Montaigne.

SIRE G., 2017, « Gouverner le HTML », *Réseaux*, 206, p. 37-60.

SKOWRONSKA K., 2014, « Europeanization through daily practices – public administrations, third sector actors and the creation of a migration regime in Poland », papier présenté à la conférence du Réseau de sociologie de la migration de l'European Sociological Association à Francfort sur le Main le 13 novembre 2014.

SLOAN L., MORGAN J., BURNAP P., WILLIAMS M., 2015, « Who Tweets? Deriving the Demographic Characteristics of Age, Occupation and Social Class from Twitter User Meta-Data », *PLoS ONE*, *10*, 3.

SMITH A., 1996, *L'Europe politique au miroir du local: les fonds structurels et les zones rurales en France, en Espagne et au Royaume-Uni*, Paris, L'Harmattan (Collection Logiques politiques).

SÓLYOM L., 1988a, « Egy új szabadságjog: az információszabadság », *Valóság*, 31, p. 14-34.

SÓLYOM L., 1988b, « Adatvédelem és személyiségi jog », *Világosság*, *29*, 1, p. 53-60.

SOUCHIER E., JEANNERET Y., 2001, « Écriture numérique ou médias informatisés ? », *Pour la science*, 33, p. 100-105.

STEINER P., 2010, « Philosophie, technologie et cognition. États des lieux et perspectives », *Intellectica*, *53*, 1, p. 7-40.

STEUCKARDT A., 2015, « Histoire de quelques correctifs formés sur dire », *Langue française*, 186, p. 13-30.

STIGLER G.J., 1961, « The Economics of Information », *The Journal of Political Economy*, *69*, 3, p. 213-225.

STIGLER G.J., 1980, « An Introduction to Privacy in Economics and Politics », *The Journal of Legal Studies*, *9*, 4, p. 623-644.

SUSSER D., ROESSLER B., NISSENBAUM H.F., 2018, « Online Manipulation: Hidden Influences in a Digital World », *Georgetown Law Technology Review*, 1, p. 1-45.

SWEENEY L., 2000, « Uniquement of Simple Demographics in the U.S. Population », *Laboratory for International Data Privacy, Working Paper LIDAP-WP4*.

SZIKLAY J., 2011, *Az információs jogok kialakulása, fejlődése és társadalmi hatása*, Thèse de doctorat, Pécs, Pécsi Tudományegyetem Állam - és Jogtudományi Kar.

SZIKLAY, J. (dir.), 2016, *KULCS A NET VILÁGÁHOZ! A gyermekek biztonságos és jogtudatos internethasználatáról (a gyermekek (jog)tudatos internethasználatának elősegítése az alapjogi jogvédelem eszközeivel)*, 2nde édition, Budapest, NAIH.

SZUBA M., 2017, « Chapitre 4 - Le rationnement, outil convivial », dans : SINAÏ A., SZUBA M. (dirs), *Gouverner la décroissance. Politiques de l'Anthropocène III*, Paris, Presses de Sciences Po, p. 95-118.

TALBOT C., 2003, *Unbundled Government: A Critical Analysis of the Global Trend to Agencies, Quangos and Contractualisation*, POLLITT C. (dir.), 1 edition, London ; New York, Routledge.

TAVANI H., 2008, « Informational privacy: concepts, theories, and controversies », dans HIMMA K., TAVANI H. (dirs.), *The Handbook of Information and Computer Ethics*, Hoboken, New Jersey, Wiley, p. 131-164.

THOMSON J.J., 1975, « The right to privacy », *Philosophy and Public Affairs*, *4*, 4, p. 295-314.

THURNER P.W., BINDER M., 2009, « European Union transgovernmental networks: The emergence of a new political space beyond the nation-state? », *European Journal of Political Research*, *48*, 1, p. 80-106.

TISSOT S., 2013, *L'Etat et les quartiers. Genèse d'une catégorie de l'action publique: Genèse d'une catégorie de l'action publique*, Le Seuil.

TRÉGUER F., 2019, *L'utopie déchue: une contre-histoire d'Internet, XVe-XXIe siècle*, Paris, Fayard (A venir).

TULMETS E., 2014, « Analyser l'exportation des normes au-delà de l'Union européenne », *Politique europeenne*, 46, p. 8-32.

TÜRK A., 2011, *La vie privée en péril: des citoyens sous contrôle*, Paris, Odile Jacob.

TURNER F., 2008, *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*, Chicago, Ill., University of Chicago Press.

UTZ C., DEGELING M., FAHL S., SCHAUB F., HOLZ T., 2019, « (Un)informed Consent: Studying GDPR Consent Notices in the Field », *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, 2019.

VAN HEDDEGHEM W., LAMBERT S., LANNOO B., COLLE D., PICKAVET M., DEMEESTER P., 2014, « Trends in worldwide ICT electricity consumption from 2007 to 2012 », *Computer Communications*, 50, p. 64-76.

VERGARA F., 2002, *Les fondements philosophiques du libéralisme. Libéralisme et éthique.*, Paris, La Découverte.

VITALIS A., 1988, *Informatique, pouvoir et libertés*, 2e édition, Paris, Economica.

VITALIS A., 2009, « « Informatique et libertés » : une histoire de trente ans », *Hermès, La Revue*, 53, p. 137-143.

VITALIS A., 2010, « France », dans RULE J.B., GREENLEAF G. (dirs.), *Global privacy protection: the first generation*, Cheltenham, Edward Elgar, p. 107-140.

VITALIS A., MATTELART A., 2014, *Le profilage des populations: Du livret ouvrier au cybercontrôle*, Paris, La Découverte.

WAELBROECK P., DUBUS A., 2018, « Analyse économique des marques de confiance », dans LEVALLOIS-BARTH C. (dir.), *Signes de confiance, l'impact des labels sur la gestion des données personnelles*, Paris, Telecom ParisTech (Chaire et Valeurs des Politiques des Informations Personnelles), p. 153-166.

WALCZAK N., 2014, *La protection des données personnelles sur l'internet.- Analyse des discours et des enjeux sociopolitiques.*, Thèse de doctorat soutenue à l'Université Lyon 2.

WALLERSTEIN I., 2009, *Comprendre le monde: introduction à l'analyse des systèmes-monde*, Paris, La Découverte.

WALREE T., 2017, « De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens », *Weekblad voor Privaatrecht, Notariaat en Registratie*, 7172, p. 921-930.

WARE W.H., 1966, « Future Computer Technology and Its Impact », Santa Monica, Rand Corporation.

WARE W.H., 1967, « Security and Privacy in Computer Systems. », Santa Monica, Californie, Rand Corporation.

WARREN S.D., BRANDEIS L.D., 1890, « The Right to Privacy », *Harvard Law Review*, *4*, 5, p. 193-220.

WEBER M., 2003, *Economie et société, tome 1 : Les Catégories de la sociologie*, Nouvelle, Paris, Pocket.

WEBER M., 2011, *Le Savant et le Politique*, Paris, Belles Lettres.

WEISS M.-A., 2014, « Liberté d'expression sur les réseaux sociaux. Regards croisés États-Unis/Europe », *Documentaliste-Sciences de l'Information*, *51*, 3, p. 20-22.

WESTIN A.F., 1967a, « Legal Safeguards to Insure Privacy in a Computer Society », *Communications of the ACM*, *10*, 9, p. 533-537.

WESTIN A.F., 1967b, *Privacy and Freedom*, New York, Atheneum.

WESTIN A.F., 1970, *Privacy and Freedom*, Bodley Head.

WESTIN A.F., 2015, *Privacy and Freedom*, New York, IG Publishing.

WIENER N., 1962, *Cybernétique et société: l'usage humain des êtres humains*, traduit par MISTOULON P.-Y., Paris, France, Union générale d'éditions.

WIENER N., 2014, *La cybernétique information et régulation dans le vivant et la machine*, traduit par LE ROUX R., VALLÉE R., VALLÉE N., Paris, Editions du Seuil.

WINDRUM P., 2004, « Leveraging technological externalities in complex technologies: Microsoft's exploitation of standards in the browser wars », *Research Policy*, *33*, 3, p. 385-394.

WINNER L., 1980, « Do Artifacts Have Politics? », *Daedalus*, *109*, 1, p. 121-136.

WOLL C., 2009, « La politique de concurrence », dans DEHOUSSE R. (dir.), *Politiques européennes*, Paris, Presses de Sciences Po, p. 171-188.

ZAFONTE M., SABATIER P., 1998, « Shared Beliefs and Imposed Interdependencies as Determinants of Ally Networks in Overlapping Subsystems », *Journal of Theoretical Politics*, *10*, 4, p. 473-505.

ZIELONKA J., 2008, « Europe as a global actor: empire by example? », *International Affairs*, *84*, 3, p. 471-484.

ZITTRAIN J., 2003, « Internet Points of Control », *Boston College Law Review*, *44*, 2, p. 653-688.

ZOUINAR M., 2019, « Théories et principes de conception des systèmes d'automesure numériques », *Réseaux*, 216, p. 83-117.

ZUBOFF S., 1989, *In The Age Of The Smart Machine: The Future Of Work And Power*, New York, Basic Books.

ZUBOFF S., 2018, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, Première édition, New York, PublicAffairs.

ZUIDERVEEN BORGESIUS F., 2017, « The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition », *European Data Protection Law Review*, *3*, 1, p. 130-137.

ZUIDERVEEN BORGESIUS F.J., 2016, « Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation », *Computer Law & Security Review*, *32*, 2, p. 256-271.

Articles de presse

AFP, 2017, « Russie : la loi sur la dépénalisation des violences domestiques promulguée par Vladimir Poutine », *Le Monde.fr*, 7 février 2017.

ANDERSON C., 2008, « The End of Theory: The Data Deluge Makes the Scientific Method Obsolete », *Wired*, 23 juin 2008.

ANGWIN J., 2012, « Microsoft's "Do Not Track" Move Angers Advertising Industry », *Wall Street Journal*, 31 mai 2012.

ARTHUR C., 2012, « The end of online privacy? », *The Guardian*, 28 février 2012.

ASHLEY M., 2019, « It's Time to Fight Back for Data Sovereignty », *Forbes*.

AUFFRAY C., 2019, « Les données personnelles, un patrimoine comme les autres ? », *ZDNet.fr*.

AUFRÈRE L., MAUREL L., 2018b, « Données personnelles : « Un enjeu de dignité collective, face aux manipulations des Gafam » », *Le Monde*, 25 mai 2018.

AUTEUR INCONNU, 1980a, « Boycottons la carte d'identité électronique », *Terminal*, 2, p. 24.

AUTEUR INCONNU, 1980b, « Le CLODO contre le CII », *Le Monde*, 13 août 1980.

AUTEUR INCONNU, 1983, « Éditorial. La CNIL et les données du pouvoir. », *Terminal*, 19, p. 2.

BAKER J., 2013, « Google, Microsoft, and Yahoo are secret backers behind European Privacy Association », *PCWorld*, 20 mai 2013.

BALL J., BORGER J., GREENWALD G., 2013, « Revealed: how US and UK spy agencies defeat internet privacy and security », *The Guardian*, 6 septembre 2013.

BANCAUD D., 2011, « Les réseaux sociaux, un vrai danger pour les plus jeunes », *20 Minutes.fr*, 5 juillet 2011.

BARBARO M., ZELLER T.JR., 2006, « A Face Is Exposed for AOL Searcher No. 4417749 », *The New York Times*, 9 août 2006.

BARNETT E., 2010, « Facebook's Mark Zuckerberg says privacy is no longer a "social norm" », *The Guardian*, 11 janvier 2010.

BENHAMOU P., 2019, « L'Europe officiellement à court d'adresses IPV4 », *ZDNet France*, 26 novembre 2019.

BERINATO S., NISSENBAUM H., 2018, « Why Data Privacy Based on Consent Is Impossible », *Harvard Business Review*, 24 septembre 2018.

BERRETTA E., 2016, « La souveraineté numérique : ce dossier qui effraie Hollande et Valls », *Le Point*, 13 janvier 2016.

BOUCHER P., 1974, « SAFARI ou la chasse aux Français », *Le Monde*, p. 9.

BUSH V., 1965, « As We May Think », *The Atlantic Monthly*, 176, p. 101-108.

CALORE M., 2007, « Microsoft Allegedly Bullies and Bribes to Make Office an International Standard », *Wired*, 31 août 2007.

CENTRE ASSOCIATIF POUR UNE INFORMATIQUE DIFFÉRENTE (CAID), 1984, « Naissance du C.A.I.D. », *Terminal*, 9, p. 30.

CHERIF A., 2018, « Être propriétaire de ses données personnelles, une dangereuse illusion », *La Tribune*, 29 mars 2018.

CIMPANU C., 2019, « Russia to disconnect from the internet as part of a planned test », *ZDNet*, 11 février 2019.

CLIFFORD C., 2018, « Zuckerberg on Facebook and privacy before Cambridge Analytica scandal », *CNBC*, 3 avril 2018.

ESPINER T., 2012, « ICO to enforce cookie law from this weekend », *ZDNet.com*, 25 mai 2012.

FERRAN B., 2019, « Les dangers d'une «balkanisation du Web» », *Le Figaro.fr*, 14 avril 2019.

GREENWALD G., 2013, « NSA collecting phone records of millions of Verizon customers daily », *The Guardian*, 6 juin 2013.

GUITON A., 2019, « Internet : des Etats entre «souveraineté numérique» et «autonomie stratégique» », *Libération.fr*, 13 février 2019.

HERN A., 2016, « Firefox disables loophole that allows sites to track users via battery status », *The Guardian*, 1 novembre 2016.

HOLPUCH A., 2013, « Brazil's controversial plan to extricate the internet from US control », *The Guardian*, 20 septembre 2013.

ICDP, 2013, « Digital ecosystem comes under threat », *POLITICO*, 30 janvier 2013.

JOHNSON B., 2010, « Privacy no longer a social norm, says Facebook founder », *The Guardian*, 11 janvier 2010.

LAMONICA M., 2008, « Office Open XML is an ISO standard: Now what? », *CNET*, 1er avril 2008.

LATOUCHE S., 2003, « Pour une société de décroissance », *Le Monde diplomatique*, novembre 2003, p. 18-19.

MANDRAUD I., 2017, « La Russie dépénalise les violences domestiques pour éviter la « destruction de la famille » », *Le Monde.fr*, 26 janvier 2017.

MCCULLOUGH M., 1984, « Informatique alternative aux États-Unis : une brassée d'expériences », *Terminal*, 9, p. 19-20.

O'NEIL M., 1998, « Internet, ou la fin de la vie privée », *Le Monde diplomatique*, 1 septembre 1998.

SCHMITT F., MADELAINE N., 2018, « Gaspard Koenig : « Chaque citoyen doit pouvoir vendre ses données personnelles » », *Les Echos*, 7 janvier 2018.

SMITH O., 2018, « The GDPR Racket: Who's Making Money From This $9bn Business Shakedown », *Forbes*, 2 mai 2018.

STIEGLER B., DURAND J.-M., 2016, « Bernard Stiegler : "Être entièrement calculable par des algorithmes nous réduit à rien" », *Les Inrocks*, 14 juin 2016.

VANHESTE T., MARTIJN M., 2013, « Hoe een machtige lobby onze privacy onder druk zet », *De Correspondent*, 10 octobre 2013.

WANG P., 2019, « Pas de révolution technologique sans souveraineté numérique », *Jeune Afrique*, 20 juin 2019.

WHITNEY L., 2012, « Microsoft ticks off advertisers with IE10 "Do Not Track" policy », CNet. 1er juin 2012.

WOLF G., 2009, « Know Thyself: Tracking Every Facet of Life, from Sleep to Mood to Pain, 24/7/365 », *Wired*, 22 juin 2009.

Normes juridiques citées

Accords internationaux

- Déclaration universelle des droits de l'Homme du 10 décembre 1948
- Statut du Conseil de l'Europe signé à Londres le 5 mai 1949
- Convention de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950 (Convention EDH)
- Traité de Paris du 18 avril 1951 instituant la Communauté européenne du charbon et de l'acier (CECA)
- Traité de Rome du 25 mars 1957 instituant la Communauté économique européenne (CEE)
- Traité de Rome du 25 mars 1957 instituant la Communauté européenne de l'énergie atomique (Euratom)
- Traité de fusion des exécutifs des trois Communautés signé à Bruxelles le 8 avril 1965
- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (Convention 108 du Conseil de l'Europe)
- Traité de Maastricht sur l'Union européenne du 7 février 1992
- Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000

- Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne du 13 décembre 2007
- Convention modernisée pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel du 18 mai 2018 (Convention 108+ du Conseil de l’Europe)

Droit dérivé des Communautés européennes puis de l’Union européenne

- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Directive 97/66/CE du 15 décembre 1997 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications »
- Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques
- Règlement 343/2003/CE du Conseil du 18 février 2003 établissant les critères et mécanismes de détermination de l’État membre responsable de l’examen d’une demande d’asile présentée dans l’un des États membres par un ressortissant d’un pays tiers, puis Règlement 604/2013/UE du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l’État membre responsable de l’examen d’une demande de protection internationale introduite dans l’un des États membres par un ressortissant de pays tiers ou un apatride
- Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) n° 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE
- Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE

- Règlement 1907/2006/CE du Parlement européen et du Conseil du 18 décembre 2006 concernant l'enregistrement, l'évaluation et l'autorisation des substances chimiques, ainsi que les restrictions applicables à ces substances (règlement REACH)
- Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale
- Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

Droit dérivé de la Communauté économique des États de l'Afrique de l'Ouest

- Acte additionnel de la CEDEAO A/SA 1/01/10 du 16 février 2010 relatif à la protection des données personnelles

Lois et règlements

Autriche

- Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2013)

Californie (État des États-Unis d'Amérique)

- California Consumer Privacy Act 2018

États-Unis d'Amérique

- Executive Order 9835 Prescribing Procedures for the Administration of an Employees Loyalty Program by the Executive Branch of the Governement, du 21 mars 1947
- Subversive Activities Control Act of 1950
- Civil Rights Act 1964
- Voting Rights Act 1965
- Privacy Act 1974

France

- Décret n° 46-2 du 3 janvier 1946 portant création à la présidence du Gouvernement d'un conseil du plan de modernisation et d'équipement et fixant les attributions du commissaire général du plan
- Loi n° 46-854 du 27 avril 1946 portant ouverture et annulation de crédits sur l'exercice 1946
- Loi n° 73-1227 du 31 décembre 1973 autorisant la ratification de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et de ses protocoles additionnels n°^{s} 1, 3, 4 et 5
- Décret n° 74-360 du 3 mai 1974 portant publication de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée le 4 novembre 1950, de ses protocoles additionnels n°^{s} 1, 3, 4 et 5, signés les 20 mars 1952, 6 mai 1963, 16 septembre 1963 et 20 janvier 1966, ainsi que des déclarations et réserves qui ont été formulées par le Gouvernement de la République française lors de la ratification
- Décret n° 74-938 du 8 novembre 1974 portant création de la commission informatique et libertés

- Loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés (dite : loi Informatique et Libertés)
- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

Hesse (Land allemand)

- Hessische Datenschutzgesetz (loi de protection des données du Land de Hesse), 7 octobre 1970 (GVBl. I S. 625)

Hongrie

- Loi IV de 1977 amendant la loi IV de 1959 sur le Code civil de la République populaire de Hongrie (*1977. évi IV. törvény a Magyar Népköztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény módosításáról és egységes szövegéről*)

New York (État des États-Unis d’Amérique)

- New York Civil Rights Act de 1903 (N.Y. Civ. Rights Act 1903, § 51)

Pays-Bas

- Décret royal (*Koninklijk Besluit*) n° 70 du 21 février 1972
- Wet persoonsregistraties (loi sur l’enregistrement des personnes) de 1988

Rhénanie-Palatinat (Land allemand)

- Landesgesetz gegen mißbräuchliche Datennutzung vom 24. Januar 1974, GVBl. S. 31 (loi contre l’usage abusif de données du 24 janvier 1974)

Royaume-Uni

- Data Protection Act 1984

Russie

- О внесении изменения в статью 116 Уголовного кодекса Российской Федерации: Федеральный Закон от 7 февраля 2017г (Loi fédérale du 7 février 2017 modifiant l'article 116 du Code pénal de la Fédération de Russie (dépénalisation des violences conjugales))

Saint-Marin

- Legge 21 dicembre 2018 n° 171 - Protezione delle persone fisiche con riguardo al trattamento di dati personali (loi n° 171 du 21 décembre 2018 sur la protection des personnes physiques à l'égard du traitement de données personnelles)

Schleswig-Holstein (Land allemand)

- Gesetz über die Datenzentrale Schleswig-Holstein vom 2. April 1968 (loi sur le centre de données du Schleswig-Holstein du 2 avril 1968)

Suède

- Tryckfrihetsförordning som utfärdades den 2 december 1766 (Édit sur la liberté de la presse du 2 décembre 1766)
- Datalag (1973:289) (loi n° 289 de 1973 sur les données)

Jurisprudence citée

Allemagne

- BVerfG, 16 juillet 1969 – 1 BvL 19/63, « Mikrozensus »
- BVerfGE, 29 mai 1974, 37, 271 - « Solange I »

- Décision du Tribunal constitutionnel fédéral allemand BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil)

Communautés européennes puis Union européenne

Voir dans l'annexe 12 la liste des décisions de la CJCE/CJUE qui portent sur le droit de la protection des données à caractère personnel. Les autres décisions citées sont les suivantes :

- CJCE 6 avril 1962, « De Geus contre Bosch e.a. », aff. 13-61
- CJCE 5 février 1963 « Van Gend en Loos », Aff. 26/62
- CJCE 15 juillet 1964 « Costa contre ENEL », Aff. 6/64
- CJCE 17 décembre 1970 « Internationale Handelsgesellschaft », Aff. 11/70
- CJCE 14 décembre 1971 « Politi », Aff. 43-71
- CJCE 4 décembre 1974 « Van Duyn contre Home Office » Aff. 41/74
- CJCE 5 avril 1979 « Ministère public contre Tullio Ratti », Aff. 148/78

Cour européenne des droits de l'Homme

Voir dans l'annexe 12 la liste des décisions de la CEDH qui portent sur le droit de la protection des données à caractère personnel

États-Unis d'Amérique

- Cour suprême, 4 juin 1928, *Olmstead contre Etats-Unis*, 277 U.S. 438
- Cour suprême, 3 mars 1952, *Adler v. Board of Education of the City of New York*, 342 U.S. 485
- Cour suprême, 9 avril 1956, *Slochower v. Board of Education*, 350 U.S. 551
- Cour suprême, 16 juin 1958, *Kent v. Dulles*, 357 U.S. 116
- Cour suprême, 7 juin 1965, *Griswold contre Connecticut*, 318 U.S. 479
- Cour suprême, 18 décembre 1967, *Katz contre Etats-Unis*, 389 U.S. 347
- Cour suprême, 22 février 1977, *Whalen contre Roe*, 429 U.S. 589

France

- Conseil constitutionnel, n° 71-44 DC du 16 juillet 1971
- C. Cass. Ch. Crim. 17 juillet 1984, pourvoi 84-91.288
- Conseil d'État, Ass., 28 février 1992, « Société Philipp Morris », publié au Recueil
- C. Cass. 11 juin 1992, pourvoi 91-86.346
- Conseil d'État, Ass., 30 octobre 2009, « Madame A. », publié au Recueil
- Tribunal de grande instance de Paris 9 avril 2019 « UFC-Que Choisir contre Facebook », 14/07298
- Cour d'appel de Paris, pôle 6, 2e chambre, arrêt du 10 janvier 2019, « M. X contre Uber »

Hongrie

- Cour constitutionnelle de la République hongroise, décision 15/1991. (IV. 13.) AB

Minnesota (État)

- Cour Suprême du Minnesota, Lake v. Wall-Mart Stores, Inc. 582 N.W. 2d. 231 (Minn 1998)

Pays-Bas

- Gerechtshof Den Haag (Pays-Bas) 27 juin 2017 « Mothers of Srebrenica », affaires 200.158.313/01 et 200.160.317/01

Rhénanie-du-Nord–Westphalie (Land allemand)

- Oberlandesgericht Köln. 3 septembre 2018. « ICANN gegen EPAG ». Aff. 19W 32/18

Décisions d’autorités administratives indépendantes

Agencia Española de Protectión de Datos (AEPD – Espagne)

- Procedimiento PS/0034/2013 18 Diciembre 2013

Commission nationale de l’informatique et des libertés (CNIL – France)

- Délibération 89-78 du 11 juillet 1989 relative à la transmission d'informations relatives aux cadres supérieurs de la société Fiat France à la société Fiat à Turin
- Délibération 2013-420 du 3 janvier 2014 de la CNIL prononçant une sanction pécuniaire à l’encontre de Google Inc
- Délibération n° SAN – 2019 – 001 du 21 janvier 2019 prononçant une sanction pécuniaire à l’encontre de la société Google Inc.

Garante Privacy (Italie)

- Ordinanza di ingiunzione nei confronti di Google Inc., 18 décembre 2013

Avis et autres résolutions non-contraignantes

Communautés européennes puis Union européenne

- Résolution du 21 février 1975 de l’Assemblée parlementaire des Communautés européennes sur la protection des droits de la personne face au développement des progrès techniques dans le domaine de l’informatique. (voir : Journal officiel des Communautés européennes 1975 n° C 60 p. 48)
- Résolution de l’Assemblée parlementaire des Communautés européennes du 8 avril 1976 relative à la protection des droits de la personne face au développement des progrès techniques dans le domaine de l’informatique (voir : Journal officiel des Communautés européennes 1976 n° C 100 p. 27)

- Résolution du Parlement européen du 8 mai 1979 sur la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique (voir : Journal officiel des Communautés européennes 1979 n° C 140 p. 34-38)
- Recommandation de la Commission européenne du 29 juillet 1981 concernant une convention du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (voir : Journal officiel des Communautés européennes, 1981, n° L 246, p. 31)
- Résolution du Parlement européen du 12 avril 1989 portant adoption de la Déclaration des droits fondamentaux (voir : Journal officiel des Communautés européennes, n° C 120, p. 54)

Conseil de l'Europe

- Recommandation 509 (1968) de l'Assemblée parlementaire du Conseil de l'Europe : « Droits de l'Homme et réalisations scientifiques et technologiques modernes » du 31 janvier 1968
- Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé du 26 septembre 1973
- Résolution (74) 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public du 20 septembre 1974

Groupe de travail de l'Article 29

- G29, 2007. *Avis 4/2007 sur le concept de données à caractère personnel*. 20 juin. Document WP 136. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_fr.pdf (document consulté le 20 décembre 2019)
- G29, 2010. *Avis 02/2010 sur la publicité comportementale en ligne.* 22 juin. Document WP 171. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_fr.pdf
- G29, 2011. *Avis 16/2011 sur le code de bonnes pratiques de l'AEEP et de l'IAB en matière de publicité comportementale en ligne*. 8 décembre. Document WP 188. Disponible en ligne à l'URL :

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_fr.pdf (document consulté le 20 décembre 2019)

- G29, 2012a. *Avis 1/2012 sur les propositions de réforme de la protection des données.* Document WP 191. 23 mars. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_fr.pdf (document consulté le 20 décembre 2019)

- G29, 2012b. *Avis 8/2012 apportant des contributions au débat sur la réforme de la protection des données.* Document WP 199. 5 octobre. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp199_fr.pdf (document consulté le 20 décembre 2019)

- G29, 2014a. *Avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement au sens de l'article 7 de la directive 95/46/CE*. 9 avril. Document WP 217. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf (document consulté le 20 décembre 2019)

OCDE

- Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel du 23 septembre 1980

Documents de corpus cités

Documents d'archives

Archives du Conseil de l'Europe

Cote du document	Date	Titre
CM (68) 53	27 mars 1968	Right to Privacy. Memorandum submitted by the Secretariat
CCJ/Prot.Priv. (71) 1	21 septembre 1971	Information document. Draft International Convention for the Protection of Personal

		and Industrial Privacy prepared by the Permanent Commission "Law and Technology" of the International Association of Lawyers for the Council of Europe
CCJ/Prot.Priv. (71) 6	21 septembre 1971	Information document
CCJ (71) 66	18 octobre 1971	Report on meeting held at Strasbourg from 11 – 13 October 1971
CCJ/SC.Prot.Priv. (73) 2	28 février 1973	Observations by the French authorities on the draft Resolutions
CCJ/SC.Prot.Priv. (73) 7	10 avril 1973	Observations by the United Kingdom
CCJ/SC.Prot.Priv. (73) 9	14 mai 1973	Summary analysis of the observations made by the governments of the member States
EXP/Prot.Priv./EDB (72) 5 REV	16 juin 1972	Report of the first meeting held in Strasbourg from 13 to 15 March 1972
EXP/Prot.Priv./EDB (72) 14	29 septembre 1972	Draft resolution relating to the protection of privacy vis-à-vis electronic data banks in the private sector and Preliminary draft explanatory report
EXP/Prot.Priv./EDB (72) 15	6 octobre 1972	Principes concernant la protection de la vie privée vis-à-vis des banques de données électroniques dans le secteur privé. Proposition présentée par l'expert suisse.
EXP/Prot.Priv./EDB (72) 17	22 novembre 1972	Report of the Third Meeting held in Strasbourg, from 25 to 27 March 1972
EXP/Prot.Priv./EDB (73) 2	26 janvier 1973	Preliminary Draft (Referentenentwurf) Bill on protection against the misuse of personal data in data processing (Data Protection Act). Information document

EXP/Prot.Priv. (73) 11	20 septembre 1973	Preliminary Draft Explanatory Report to the Resolution on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector
EXP/Prot.Priv. (74) 3	25 janvier 1974	Draft Explanatory Report to the Resolution on the protection of privacy of invididuals vis-à-vis electronic data banks in the public sector
EXP/Prot.Priv. (75) 6	20 juillet 1975	Austrian Government Bill of 18 December 1974
CJ-PD-GTI (79) 1	25 janvier 1979	Projet de convention pour la protection des personnes à l'égard des fichiers automatisés

Archives de l'OCDE

Cote du document	**Date**	**Titre**
DAS/SPR/68.1	9 janvier 1968	Gaps in Technology Between Member Countries. Group of Experts on Electronic Components. Draft Report.
DAS/SPR/68.8	7 févier 1968	Écarts technologiques entre pays membres. Groupe d'experts sur les instruments scientifiques. Compte-rendu succinct de la réunion du 22 janvier 1968
DAS/SPR/68.10	12 février 1968	Sujets proposés par le Comité de politique scientifique à la discussion de la troisième Conférence ministérielle de la science
CMS (68) 18	11 et 12 mars 1968	Troisième Conférence ministérielle sur la science des pays de l'OCDE. Point VII de l'ordre du jour. Politiques en matière de systèmes d'information scientifique et technique. Rapport général.

DSTI/ICCP/77.47	12 décembre 1977	Colloque sur les flux de de données transfrontières et la protection des libertés individuelles. Effets et tendance. Rapport de synthèse.
DSTI/ICCP/78.6	17 mars 1978	Mandat du nouveau groupe sur les obstacles au mouvement transfrontières des données et la protection des libertés individuelles
DSTI/ICCP/79.40	22 juin 1979	Projet de lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel
SPT/M(79)3	31 décembre 1979	Committee for Scientific and Technological Policy – Summary Record of the 24th Session held at the Château de la Muette, Paris, on 20th, 21st and 22nd November, 1979

Documents versés à la Consultation de 2009 de la Commission européenne

Le tableau ci-dessous donne des précisions sur les documents listés en annexe 4 qui sont directement cités dans la thèse.

Identifiant du document	Organisme	Auteur(s) (si identifiables)	Date (si identifiable)	Nom du document	Titre du document
AMCHAMEU 1	AmCham EU	Roger Coelho	19 janvier 2010	american_chamber_commerce_to_eu_en.pdf	AmCham EU response to the Commission consultation on protection of personal data
DIGITALEUROPE1	Digitaleurope	Hara Klasina (sur la base des	20 novembre 2009	digital_europe_en.pdf	Response to European Commission

		métadonnées du document PDF)			Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data
DMA1	Digital Marketing Association	James Milligan	23 décembre 2009	the_direct_marketing_association_UK_en.pdf	Response of The Direct Marketing Association (UK) Limited (ID Number 43161482922-05) to the consultation on the legal framework for the fundamental right to protection of personal data.
FEDMA1	FEDMA	Goetz Brandau	16 décembre 2009	fedma_en.pdf	FEDMA submission to the Public Consultation of the European Commission (DG JLS) on the legal framework for the fundamental right to protection of personal data

Documents versés à la Consultation de 2010 de la Commission européenne

Le tableau ci-dessous donne des précisions sur les documents listés en annexe 4 qui sont directement cités dans la thèse.

Identifiant du document	Organisme	Auteur(s) (si identifiables)	Date (si identifiable)	Nom du document	Titre du document
AMCHAM1	AmCham EU		14 janvier 2011	amcham_en.pdf	AmCham EU's response to the Commission communication on a comprehensive approach on data protection in the European Union
BEUC1	BEUC		24 janvier 2011	beuc_en.pdf	A Comprehensive Approach on Personal Data Protection in the European Union. European Commission's Consultation. BEUC, The European Consumers' Organisation's response
BSA1	BSA	Thomas Boué	14 janvier 2011	bsa_en.pdf	Views of the Business Software Alliance on the Commission's Data Protection Strategy
EK1	Confederation of Finnish Industries		14 janvier 2011	finnish_industries_en.pdf	Response to the Commission

	(EK)				Consultation on a Comprehensive Approach on Personal Data Protection in the European Union

Corpus de documents récupérés du collectif Lobbyplag

Le tableau ci-dessous donne des précisions sur les documents listés en annexe 4 qui sont directement cités dans la thèse.

Identifiant du document	Organisme	Auteur(s) (si identifiables)	Date (si identifiable)	Nom du document	Titre du document
ACCIS1	ACCIS		Avril 2012	ACCIS_Position Paper on Proposed Data Protection Regulation May 2012.pdf	Proposal for amendments to the proposed review of the EU's Data Protection Legal Framework
AMCHAMEU1	AmCham EU	Roger Coelho (sur la base des métadonnées du document)	5 février 2013 (sur la base des métadonnées du document)	AmCham_EU_Proposed_Amendments_on_Data_Protection.pdf	AmCham EU Proposed Amendments on the General Data Protection Regulation
BEUC1	BEUC		28 novembre 2012 (sur la base des métadonnées du document)	Data-Protection-Regulation-Proposal-BEUC-analyse-of-Administrative-burden.pdf	Proposal for a Data Protection Regulation. BEUC analysis of consumer benefits versus administrative burden of key provisions

BITKOM1	Bitkom		12 octobre 2012	bmi_auskunft.pdf	Amendments to the General Data Protection Regulation
BITSOFFREEDOM1	Bits of Freedom	Ot Daalen (sur la base des métadonnées du document)	11 février 2013 (sur la base des métadonnées du document)	Amendments DP Regulation Bits of Freedom.pdf	Amendments to the Draft Data Protection Regulation Proposed by Bits of Freedom
BUSINESSEUROPE1	Business Europe	Konteas Ilias (sur la base des métadonnées du document PDF)	17 octobre 2012	1017-BUSINESSEUROPE-pp-data-protection-regulation.pdf	Position Paper. Commission Proposal on a General Data Protection Regulation
DIGITALEUROPE1	Digitaleurope	Anna-Verena Naether (sur la base des métadonnées du document PDF)	12 mars 2012	DIGITALEUROPE-priorities-of-Data-Protection-Regulation_March-2012.pdf	Digitaleurope Comments on Proposed European Commission's Regulation on Data Protection
DIGITALEUROPE2	Digitaleurope	Anna-Verena Naether (sur la base des métadonnées du document PDF)	1er novembre 2012	DIGITALEUROPE_Amendments-to-Data-Protection-Regulation_final.pdf	Draft DIGITALEUROPE amendments
EDRI1	EDRi		22 octobre 2012 (sur la base des métadonnées du document PDF)	EDRis-comments-on-draft-imco-opinion-on-general-data-protection-regulation.pdf	Comments on IMCO draft opinion on the General Data Protection Regulation
EDRI2	EDRi	Konteas Ilias (sur la base des métadonnées du document	12 décembre 2012	EDRi Amendments.pdf	EDRi's suggested amendments to the Commission's

		PDF)			Proposal for a Regulation on the Protection of Individuals with regard to the processing of personal data, and the free movement of such data (General Data Protection Regulation)
FACEBOOK1	Facebook	Abtin Kronold (sur la base des métadonnées du document PDF)	29 janvier 2013 (sur la base des métadonnées du document PDF)	facebook_imco.pdf	Facebook recommendations on the Internal Market and Consumer Affairs draft opinion on the European Commission's proposal for a General Data Protection Regulation "on the protection of individuals with regard to the processing of personal data and on the free movement of such data"
FBF1	Fédération bancaire française		Août 2012	FBF_position_protection_donnees_personnelles_EN1.pdf	Proposal for a Regulation of the European Union and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on

					the Free Movement of such Data (General Data Protection Regulation)
FEDIL1	Fedil	Romain Lanners (sur la base des métadonnées du document PDF)	17 juillet 2012	Fedil_ppdataprotection-final_17July2012.pdf	Comments on the Commission Proposal for a Regulation on the Protection of Personal Data in the EU and on the free Movement of such Data
FPF1	Future of Privacy Forum	Omer Tene et Christopher Wolf	Janvier 2013	Future of Privacy Forum White Paper on Consent.pdf	White Paper. The Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent
ICDP1	ICDP		28 novembre 2011 (sur la base des métadonnées du document PDF)	eudataprotect.pdf	Industry Coalition for Data Protection Paper on proposals for a “New EU legal framework on data protection”
MICROSOFT1	Microsoft	David Fink (sur la base des métadonnées du document PDF)	15 février 2013 (sur la base des métadonnées du document PDF)	Microsoft_final DP amendments.pdf	Microsoft positions and suggestions for the draft General Data Protection Regulation
NOKIA1	Nokia	Mikko Niva	19 novembre	nokia_engströ	Lettre de

			2012	m.pdf	Mikko Niva à Christian Engström
TELEFONIC A1	Telefónica	Fernando Herrera González (sur la base des métadonnées du document PDF)	21 janvier 2013 (sur la base des métadonnées du document)	Telefonica-Amendments-on-GDPR-Proposal.pdf	Telefónica's proposed amendments to the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

E-mails des listes de discussion publiques du W3C

Liste public-privacy

Expéditeur	Date	Sujet	URL
Thomas Roessler <tlr@w3.org>	19 juillet 2010	Thanks for joining the W3C privacy workshop last week!	https://lists.w3.org/Archives/Public/public-privacy/2010JulSep/0000.html
David Singer <singer@apple.com>	2 août 2010	'do not track' list?	https://lists.w3.org/Archives/Public/public-privacy/2010JulSep/0042.html
Thomas Roessler <tlr@w3.org>	24 février 2011	Do Not Track and W3C	https://lists.w3.org/Archives/Public/public-privacy/

			2011JanMar/0005.html
Rigo Wenning <rigo@w3.org>	19 avril 2011	Re: do we have a right to be forgotten?	https://lists.w3.org/Archives/Public/public-privacy/2011AprJun/0047.html
Christine Runnegar <runnegar@isoc.org>	13 avril 2012	PING Kick-off call - Thursday 19 April - UTC 14	https://lists.w3.org/Archives/Public/public-privacy/2012AprJun/0018.html
Dan Brickley <danbri@danbri.org>	18 avril 2012	Re: Lightning talk at W3C camp	https://lists.w3.org/Archives/Public/public-privacy/2012AprJun/0030.html
Christine Runnegar <runnegar@isoc.org>	21 octobre 2012	TPAC breakout session - Is user agent Fingerprinting a lost cause?	https://lists.w3.org/Archives/Public/public-privacy/2012OctDec/0098.html
David Singer <singer@apple.com>	24 octobre 2012	Re: TPAC breakout session - Is user agent Fingerprinting a lost cause?	https://lists.w3.org/Archives/Public/public-privacy/2012OctDec/0159.html
Charles McCathie Neville <chaals@yandex-team.ru>	30 janvier 2015	Re: indicating 'private browsing mode' over the net (was Re: Super Cookies in Privacy Browsing mode)	https://lists.w3.org/Archives/Public/public-privacy/2015JanMar/0069.html
Léonie Watson <tink@tink.uk>	26 avril 2018	Request Privacy review of HTML5.3	https://lists.w3.org/Archives/Public/public-privacy/2018AprJun/0026.html

Liste public-tracking

Expéditeur	Date	Sujet	URL
Roy T. Fielding <fielding@gbiv.com>	12 octobre 2011	Re: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/Archives/Public/public-tracking/2011Oct/0066.html
Aleecia M. McDonald	12 octobre 2011	Re: ISSUE-5: What is	https://lists.w3.org/

<aleecia@aleecia.com>		the definition of tracking?	Archives/Public/ public-tracking/ 2011Oct/0068.html
Brett Error <brett@adobe.com>	12 octobre 2011	RE: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0072.html
Brett Error <brett@adobe.com>	13 octobre 2011	RE: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0081.html
Jonathan Mayer <jmayer@stanford.edu>	13 octobre 2011 (1)	RE: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0085.html
David Wainberg <dwainberg@appnexus.com>	13 octobre 2011	Re: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0092.html
Justin Brookman <justin@cdt.org>	13 octobre 2011	Re: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0094.html
Jonathan Mayer <jmayer@stanford.edu>	13 octobre 2011 (2)	Re: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0096.html
Aleecia M. McDonald <aleecia@aleecia.com>	13 octobre 2011	Re: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0099.html
David Singer <singer@apple.com>	22 octobre 2011	Re: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0183.html
JC Cannon <jccannon@microsoft.com>	23 octobre 2011	RE: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0186.html
Sean Harvey <sharvey@google.com>	24 octobre 2011	RE: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/ Archives/Public/ public-tracking/ 2011Oct/0191.html

Jonathan Mayer <jmayer@stanford.edu>	25 octobre 2011	RE: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/Archives/Public/public-tracking/2011Oct/0192.html
David Wainberg <dwainberg@appnexus.com>	25 octobre 2011	RE: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/Archives/Public/public-tracking/2011Oct/0197.html
Sean Harvey <sharvey@google.com>	27 octobre 2011	RE: ISSUE-5: What is the definition of tracking?	https://lists.w3.org/Archives/Public/public-tracking/2011Oct/0277.html
John Simpson <john@consumerwatchdog.org>	29 novembre 2011	Re: Issue-17, Issue-51 First party obligations; Issue-5 Definition of Tracking	https://lists.w3.org/Archives/Public/public-tracking/2011Nov/0276.html
Ninja Marnau <nmarnau@datenschutzzentrum.de>	30 novembre 2011	Re: Issue-17, Issue-51 First party obligations; Issue-5 Definition of Tracking	https://lists.w3.org/Archives/Public/public-tracking/2011Nov/0288.html
Shane Wiley <wileys@yahoo-inc.com>	30 novembre 2011	RE: Issue-17, Issue-51 First party obligations; Issue-5 Definition of Tracking	https://lists.w3.org/Archives/Public/public-tracking/2011Nov/0290.html
David Wainberg <dwainberg@appnexus.com>	30 novembre 2011	Re: Issue-17, Issue-51 First party obligations	https://lists.w3.org/Archives/Public/public-tracking/2011Nov/0291.html
Chris Pedigo <CPedigo@online-publishers.org	30 novembre 2011	RE: Issue-17, Issue-51 First party obligations; Issue-5 Definition of Tracking	https://lists.w3.org/Archives/Public/public-tracking/2011Nov/0312.html
Jeffrey Chester <jeff@democraticmedia.org>	1er décembre 2011	Re: Issue-17, Issue-51 First party obligations; Issue-5 Definition of Tracking	https://lists.w3.org/Archives/Public/public-tracking/2011Dec/0002.html
Kevin Smith <kevsmith@adobe.com>	9 décembre 2011	[ISSUE-5] What is the definition of tracking?	https://lists.w3.org/Archives/Public/public-tracking/2011Dec/0051.html
Jonathan Mayer <jmayer@stanford.edu>	10 décembre 2011	Re: [ISSUE-5] What is the definition of tracking?	https://lists.w3.org/Archives/Public/public-tracking/

			2011Dec/0056.html
Aleecia M. McDonald <aleecia@aleecia.com>	12 décembre 2012	Re: [ISSUE-5] What is the definition of tracking?	https://lists.w3.org/Archives/Public/public-tracking/2011Dec/0058.html
Rigo Wenning <rigo@w3.org>	12 janvier 2012	Re: diff of TPE editing since the FPWD	https://lists.w3.org/Archives/Public/public-tracking/2012Jan/0107.html
Roy T. Fielding <fielding@gbiv.com>	16 janvier 2012	Re: meaning of DNT 1 and DNT 0 when sent by user agents [ISSUE-78]	https://lists.w3.org/Archives/Public/public-tracking/2012Jan/0157.html
Roy T. Fielding <fielding@gbiv.com>	4 mars 2012	Re: [ISSUE-5] What is the definition of tracking?	https://lists.w3.org/Archives/Public/public-tracking/2012Mar/0044.html
Rigo Wenning <rigo@w3.org>	7 mars 2012	Re: [ISSUE-5] What is the definition of tracking?	https://lists.w3.org/Archives/Public/public-tracking/2012Mar/0123.html
Roy T. Fielding <fielding@gbiv.com>	4 septembre 2012	ISSUE-5: definition of tracking	https://lists.w3.org/Archives/Public/public-tracking/2012Sep/0009.html
Rob van Eijk <rob@blaeu.com>	5 septembre 2012	Re: ISSUE-5: definition of tracking	https://lists.w3.org/Archives/Public/public-tracking/2012Sep/0015.html
Mike O'Neill <michael.oneill@baycloud.com>	11 octobre 2012	RE: Third-Party Web Tracking: Policy and Technology Paper outlining harms of tracking	https://lists.w3.org/Archives/Public/public-tracking/2012Oct/0228.html
Rigo Wenning <rigo@w3.org>	16 octobre 2012	Re: Third-Party Web Tracking: Policy and Technology Paper outlining harms of tracking	https://lists.w3.org/Archives/Public/public-tracking/2012Oct/0279.html
Alan Chapell <achapell@chapellassociates.com>	18 juillet 2013	Re: Explanatory Memorandum	https://lists.w3.org/Archives/Public/public-tracking/2013Jul/0435.html

Thomas Roessler <tlr@w3.org>	18 juillet 2013	Re: Explanatory Memorandum	https://lists.w3.org/Archives/Public/public-tracking/2013Jul/0436.html
Matthias Schunter (Intel Corporation) <mts-std@schunter.org>	9 octobre 2013	ISSUE-5: Consensus definition of "tracking" for the intro?	https://lists.w3.org/Archives/Public/public-tracking/2013Oct/0206.html
Rob van Eijk <rob@blaeu.com>	5 septembre 2014	Re: Deidentification (ISSUE-188)	https://lists.w3.org/Archives/Public/public-tracking/2014Sep/0003.html
Xueyuan <xueyuan@w3.org>	10 avril 2018	Tracking Protection Working Group Charter Extended	https://lists.w3.org/Archives/Public/public-tracking/2018Apr/0002.html
xueyuan <xueyuan@w3.org>	17 janvier 2019	Tracking Protection Working Group now closed	https://lists.w3.org/Archives/Public/public-tracking/2019Jan/0000.html
Mike O'Neill <michael.oneill@baycloud.com>	21 mai 2019	FW: Yet another DNT Act	https://lists.w3.org/Archives/Public/public-tracking/2019May/0007.html

Autres listes de discussion

Liste de discussion	Expéditeur	Date	Sujet	URL
www-style	Liam Quinn <liam@htmlhelp.com>	1er juillet 1997	Re: CSS1 Support on the Macintosh site	https://lists.w3.org/Archives/Public/www-style/1997Jul/0000.html
public-geolocation	Alec Berntson <alecb@windows.microsoft.com>	6 juin 2008	Geolocation: Security and Privacy	https://lists.w3.org/Archives/Public/public-geolocation/2008Jun/0020.html

public-geolocation	Doug Schepers <schepers@w3.org>	8 juin 2008	Re: Geolocation: Security and Privacy	https://lists.w3.org/Archives/Public/public-geolocation/2008Jun/0025.html
public-geolocation	John Morris <jmorris@cdt.org>	23 octobre 2008	Location privacy concerns	https://lists.w3.org/Archives/Public/public-geolocation/2008Oct/0055.html
public-geolocation	Nick Doty <npdoty@ischool.berkeley.edu>	8 avril 2009	Re: Intended usage notification	https://lists.w3.org/Archives/Public/public-geolocation/2009Apr/0043.html
public-p3p-spec	Lorrie Cranor <lorrie+@cs.cmu.edu>	27 octobre 2006	RESPONSE NEEDED: P3P 1.1 note publication and working group close	https://lists.w3.org/Archives/Public/public-p3p-spec/2006Oct/0001.html
public-p3p-spec	Susan Lesch <lesch@w3.org>	22 novembre 2006	P3P Specification Working Group now closed	https://lists.w3.org/Archives/Public/public-p3p-spec/2006Nov/0010.html

Documents de standardisation technique

Identifiant	Organisation	Éditeur(s)	Date	Titre
HTTP 0.9	CERN	Tim BL	1991	HTTP 0.9
IEEE754:2008	IEEE C/MSC - Microprocessor Standards Committee		29 août 2008	IEEE Standard for Floating-Point Arithmetic

IEEE P802E	IEEE 802 EC Privacy Recommendation Study Group		3 septembre 2015	IEEE Draft Recommended Practice for Privacy Considerations for IEEE 802 Technologies
IEEEP7006	WG-PDAI – Personal Data AI Agent Working Group		23 mars 2017	Standard for Personal Data Artificial Intelligence (AI) Agent
IEEE EADv1	IEEE Global Initiative on Ethics and Autonomous and Intelligent Systems		2019	IEEE Ethically Aligned Design v1
IETF draft-mayer-do-not-track-00	IETF	J. Mayer, A. Narayanan et S. Stamm[1]	7 mars 2011	Do Not Track: A Universal Third-Party Web Tracking Opt Out
IETF draft-ietf-ttpbis-client-hints-06	IETF	I. Grigorik	16 juillet 2018	HTTP Client Hints
ISO/IEC 7498-1:1994	ISO/IEC JTC 1		Novembre 1994	Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Modèle de référence de base: Le modèle de base
ISO/IEC 27018:2014	ISO/IEC JTC 1/SC 27		Août 2014	Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII
ISO/IEC 29190:2015	ISO/IEC JTC 1/SC 27		Août 2015	Technologies de l'information — Techniques de sécurité — Modèle d'évaluation de l'aptitude à la confidentialité
ISO/IEC 29134:2017	ISO/IEC JTC 1/SC 27		Juin 2017	Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'évaluation d'impacts sur la vie

1 Les noms des éditeurs de la norme sont repris ici exactement comme ils sont rédigés dans le document cité.

				privée
OASIS PbD-SE 1.0	OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC	Ann Cavoukian, Fred Carter, Dawn Jutla, John Sabo, Frank Dawson, Jonathan Fox, Tom Finneran, Sander Fieten	25 juin 2014	OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC, Privacy by Design Documentation for Software Engineers Version 1.0
OASIS PMRM 1.0	OASIS Privacy Management Reference Model (PMRM) TC	Michele Drgon, Gail Magnuson et John Sabo	17 mai 2016	OASIS Privacy Management Reference Model and Methodology (PMRM) Version 1.0
MIT CTSS PROGRAMMING STAFF NOTE 39	Compatible Time-Sharing System (CTSS), MIT	Crisman, Schroeder et Pouzin	1964	Proposed Minimum System Documentation
RFC 1	IETF[2]	Steve Crocker	7 avril 1969	Host Software
RFC 20	IETF	Vint Cerf	16 octobre 1969	ASCII format for Network Interchange
RFC 675	IETF	Vinton Cerf, Yogen Dalal et Carl Sunshine	Décembre 1974	Specification of Internet Transmission Control Program
RFC 768	IETF	Jon Postel	28 août 1980	User Datagram Protocol
RFC 791	IETF	Jon Postel	Septembre 1981	Internet Protocol
RFC 793	IETF	Jon Postel	Septembre 1981	Transmission Control Protocol
RFC 937	IETF	M. Butler, J. Postel, D. Chase, J. Goldberger et J. K. Reynolds	Février 1985	Post Office Protocol version 2
RFC 959	IETF	J. Postel et J. Reynolds	Octobre 1985	File Transfer Protocol

2 Par souci de simplicité, désigne l'IETF et ses précédecesseurs (NWG, INWG…)

RFC 1034	IETF	P. Mockapetris	Novembre 1987	Domain names – concepts and facilities
RFC 1035	IETF	P. Mockapetris	Novembre 1987	Domain names – implementation and specification
RFC 1087	IETF	Internet Activities Board	Janvier 1989	Ethics and the Internet
RFC 1160	IETF	V. Cerf	Mai 1990	The Internet Activities Board
RFC 1436	IETF	F. Anklesaria, M. McCahill, P. Lindner, D. Johnson, D. Torrey et B. Alberti	Mars 1993	The Internet Gopher Protocol
RFC 1459	IETF	J. Oikarinen et D. Reed	Mai 1993	Internet Relay Chat Protocol
RFC 1543	IETF	J. Postel	Octobre 1993	Instructions to RFC Authors
RFC 1866	IETF	T. Berners-Lee et D. Connolly	Novembre 1995	Hypertext Markup Language - 2.0
RFC 1945	IETF	T. Berners-Lee, R. Fielding, H. Frystyk	Mai 1996	Hypertext Transfer Protocol -- HTTP/1.0
RFC 2026	IETF	S. Bradner	Octobre 1996	The Internet Standards Process -- Revision 3
RFC 2027	IETF	J. Galvin	Octobre 1996	IAB and IESG Selection, Confirmation, and Recall Process: Operation of the Nominating and Recall Committees
RFC 2031	IETF	E. Huizer	Octobre 1996	IETF-ISOC relationship
RFC 2119	IETF	S. Bradner	Mars 1997	Key words for use in RFCs to Indicate Requirement Levels
RFC 2460	IETF	S. Deering et R. Hinden	Décembre 1998	Internet Protocol, Version 6 (IPv6) – Specification
RFC 2616	IETF	R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter,	Juin 1999	Hypertext Transfer Protocol -- HTTP/1.1

		P. Leach, T. Berners-Lee		
RFC 2818	IETF	E. Rescorla	Mai 2000	HTTP Over TLS
RFC 2826	IETF	Internet Architecture Board	Mai 2000	IAB Technical Comment on the Unique DNS Root
RFC 3041	IETF	T. Narten et R. Draves	Janvier 2001	Privacy Extensions for Stateless Address Autoconfiguration in IPv6
RFC 3552	IETF	E. Rescorla, B. Korver et Internet Architecture Board	Juillet 2003	Guidelines for Writing RFC Text on Security Considerations
RFC 3693	IETF	J. Cuellar, J. Morris, D. Mulligan, J. Peterson and J. Polk	Février 2004	Geopriv Requirements
RFC 3935	IETF	H. Alvestrand	Octobre 2004	A Mission Statement for the IETF
RFC 4745	IETF	H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar et J. Polk, J. Rosenberg	Février 2007	Common Policy: A Document Format for Expressing Privacy Preferences
RFC 4941	IETF	T. Narten, R. Draves et S. Krishnan	Septembre 2007	Privacy Extensions for Stateless Address Autoconfiguration in IPv6
RFC 6280	IETF	R. Barnes, M. Lepinski, A. Cooper, J. Morris, H. Tschofenig et H. Schulzrinne	Juillet 2011	An Architecture for Location and Location Privacy in Internet Applications
RFC 6973	IETF	A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, M. Hansen et R. Smith	Juillet 2013	Privacy Considerations for Internet Protocols

RFC 7258	IETF	S. Farrell et H. Tschofenig	Mai 2014	Pervasive Monitoring Is an Attack
RFC 7437	IETF	M. Kucherawy	Janvier 2015	IAB, IESG, and IAOC Selection, Confirmation, and Recall Process: Operation of the Nominating and Recall Committees
RFC 7776	IETF	P. Resnick et A. Farrel	Mars 2016	IETF Anti-Harassment Procedures
RFC 8174	IETF	B. Leiba	Mai 2017	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words
RFC 8280	IETF	N. ten Oever et C. Cath	Octobre 2017	Research into Human Rights Protocol Considerations
RFC 8318	IETF	S. Dawkins	Janvier 2018	IAB, IESG, and IAOC Selection, Confirmation, and Recall Process: IAOC Advisor for the Nominating Committee
W3C P3P 1.0	W3C P3P	Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall et Joseph Reagle	16 avril 2002	The Platform for Privacy Preferences 1.0 (P3P1.0) Specification
W3C P3P 1.1	W3C P3P	Rigo Wenning et Matthias Schunter	13 novembre 2006	The Platform for Privacy Preferences 1.1 (P3P1.1) Specification
W3C Device API Privacy	W3C APIs and Policy Working Group	Alissa Cooper, Frederick Hirsch et John Morris	23 juin 2010	Device API Privacy Requirements
W3C TPWG Charter	W3C		2011[3]	Tracking Protection Working Group Charter
W3C PING Charter	W3C		Juillet 2011	Privacy Interest Group Charter
W3C SPA	W3C PING	Frank Dawson	28 juin 2013	Specification Privacy Assessment (SPA) Creating Privacy Considerations for W3C Technical Specifications

3 Il s’agit de la seule information indiquée dans le document

W3C Geolocation API	W3C Geolocation Working Group	Andrei Popescu	24 octobre 2013	Geolocation API Specification
W3C Fingerprinting Guidance	W3C PING	Nick Doty	24 novembre 2015	Fingerprinting Guidance for Web Specification Authors (Draft)
W3C TAG Security and Privacy 2015	W3C TAG	Mike West	10 décembre 2015	Self-Review Questionnaire: Security and Privacy
W3C Battery Status API	W3C Device and Sensors Working Group	Anssi Kostiainen et Mounir Lamouri	7 juillet 2016	Battery Status API
W3C WAI-ARIA 1.1	W3C Accessible Rich Internet Applications Working Group	Joanmarie Diggs, Shane McCarron, Michael Cooper, Richard Schwerdtfeger et James Craig	14 décembre 2017	Accessible Rich Internet Applications (WAI-ARIA) 1.1
W3C Process	W3C	Neville McCathie	1er février 2018	World Wide Web Consortium Process Document
W3C TPE	W3C TPWG	Roy Fielding et David Singer	17 janvier 2019	Tracking Preference Expression
W3C TCS	W3C TPWG	Nick Doty	22 janvier 2019	Tracking Compliance and Scope
W3C Privacy Considerations	W3C PING	Hannes Tschofening et Nick Doty	29 avril 2019	Privacy Considerations for Web Protocols
W3C TAG Security and Privacy 2019	W3C TAG	Lukasz Olejnik et Jason Novak	10 septembre 2019	W3C TAG Self-Review Questionnaire: Security and Privacy

Autres rapports et documents institutionnels

AFPA, 2019, « Règlement Général sur la Protection des DonnéesLe métier de Délégué à la Protection des Données (DPO) 1 an après - Premiers Résultats », Paris, Ministère du travail.

AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE, CONSEIL DE L'EUROPE (DIRS.), 2014, *Manuel de droit européen en matière de protection des données*, Luxembourg, Office des publications de l'Union européenne (Handbook / FRA, European Union Agency for Fundamental Rights).

AGENCE NATIONALE DE LA RECHERCHE (FRANCE), 2013. *Plan d'action 2014*. (document reçu par mail sur à une demande de communication)

ALBRECHT, J.P. (rapporteur), 2013, *Rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)*, document A7-0402/2013, Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures. 21 novembre. Disponible en ligne à l'URL : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//FR (page consultée le 20 décembre 2019)

BARLOW J.P., 1996, « A Declaration of the Independence of Cyberspace », *Electronic Frontier Foundation*.

BERNERS-LEE, T., 1997, *Platform for Privacy Preferences*, présentation faite à la FTC disponible en-ligne à l'URL : https://web.archive.org/web/19970731002534/http://www.w3.org/Talks/970612-ftc/overview.htm (page consultée le 20 décembre 2019)

BLEKELI R.D., 1974, « Normes à observer pour le traitement de l'information et les procédures de contrôle », dans *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire*, Paris, Organisation de Coopération et de Développement Economique (OCDE) (Collection études d'informatique), p. 75-95.

BRANDEIS L.D., 1928, *Dissenting Opinion in Olmstead v. United-States*, 277 U.S. 438.

BRITISH COMPUTER SOCIETY, 1971, « Submission of Evidence to the Committee on Privacy », London, England, British Computer Society.

BRITISH COMPUTER SOCIETY, 1972, *Privacy and the computer--steps to practicality: a review of recent work carried out by the Privacy and Public Welfare Committee of the British Computer Society*, London, British Computer Society.

BVA, 2018, *Les Français et les données personnelles*. Observatoire de la vie quotidienne des Français. 24 mai. Disponible en-ligne à l'URL : HTTPS://STATICSWWW.BVA-GROUP.COM/WP-CONTENT/UPLOADS/2018/05/PRESSE-REGIONALE-OBSERVATOIRE-DE-LA-VIE-QUOTIDIENNE-MAI-2018-LES-DONN%C3%A9ES-PERSONNELLES.PDF (page consultée le 20 décembre 2019)

CASTEX L., GONZÁLEZ FUSTER G., IWAŃSKA K., MUSIANI F., ROSSI J., 2018, « European Civil Society Workshop on the Compensation of Data Protection Harms - Policy Brief », Paris, Internet Society France.

CDT, 1997, *Submission request to W3C*, 17 octobre. Disponible en-ligne : https://www.w3.org/Submission/1997/17/ (page consultée le 20 décembre 2019)

CERF V., 2013, « Internet of Things Workshop », *Federal Trade Commission*, 19 novembre 2013, p. 118-153.

CHURCH F., TOWER J.G., 1976, « Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Book III. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities », United States Senate.

CLARK D.D., 1992, « A Cloudy Cristal Ball -- Visions of the Future », Présentation faite à la conférence IETF 24, à Cambridge, Massuchussets, juillet 1992.

CNIL, 1988. *Dix ans d'informatique et libertés*. Paris:Economica

CNIL, 2015. *Rapport d'activité 2014*. Disponible en-ligne : https://www.cnil.fr/sites/default/files/typo/document/CNIL-35e_rapport_annuel_2014.pdf.pdf (ressource consultée le 7 décembre 2019)

COMMISSION EUROPÉENNE, 1990. *Proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel*. COM (90) 314 FINAL.

COMMISSION EUROPÉENNE, 2010a, *Le respect de la vie privée des Européens sera mis à l'épreuve dans la prochaine décennie, a déclaré un membre de la Commission européenne*, communiqué de presse IP/10/63 FR du 28 janvier. Disponible en ligne à l'URL : https://ec.europa.eu/commission/presscorner/detail/fr/IP_10_63 (page consultée le 20 décembre 2019)

COMMISSION EUROPÉENNE, 2010b. *Communication de la Commission. Europe 2020. Une stratégie pour une croissance intelligente, durable et inclusive.* COM (2010) 2020 FINAL, 3 mars. Disponible en ligne à l'URL : https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:FR:PDF (document consulté le 20 décembre 2019)

COMMISSION EUROPÉENNE, 2010c, *Protection des données: la Commission européenne présente sa stratégie pour renforcer les règles de l'Union en la matière*, communiqué de presse IP/10/1462 FR du 4 novembre. Disponible en ligne à l'URL : https://ec.europa.eu/commission/presscorner/detail/fr/IP_10_1462 (page consultée le 20 décembre 2019)

COMMISSION EUROPÉENNE, 2012a, *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions. Protection de la vie privée dans un monde en réseau. Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle*, COM (2012) 9 FINAL, 25 janvier. Disponible en ligne à l'URL : https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:FR:PDF (document consulté le 20 décembre 2019)

COMMISSION EUROPÉENNE, 2012b, *Proposition de Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des*

infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données. COM (2012) 010, 25 janvier. Disponible en ligne à l'URL : https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:FR:PDF (document consulté le 20 décembre 2019)

COMMISSION EUROPÉENNE, 2012c, *Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)*. COM (2012) 011, 25 janvier. Disponible en ligne à l'URL : https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF (document consulté le 20 décembre 2019)

COMMISSION EUROPÉENNE, 2012d, *La Commission propose une réforme globale des règles en matière de protection des données pour accroître la maîtrise que les utilisateurs ont sur leurs données, et réduire les coûts grevant les entreprises*, communiqué de presse IP-12-46 FR du 25 janvier. Disponible en ligne à l'URL : https://ec.europa.eu/commission/presscorner/detail/fr/IP_12_46 (page consultée le 20 décembre 2019)

COMMISSION EUROPÉENNE, 2013. *LIBE Committee vote backs new EU data protection rules*, Memo 13/923 du 22 octobre. Disponible en ligne à l'URL (page consultée le 20 décembre 2019) : http://europa.eu/rapid/press-release_MEMO-13-923_fr.htm

COMMISSION EUROPÉENNE, 2017. Proposition de Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive2002/58/CE (règlement «vie privée et communications électroniques»), COM (2017) 10 FINAL FR. Disponible en ligne à l'URL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017PC0010&from=EN (document consulté le 20 décembre 2019)

COMMISSION EUROPÉENNE, 2018a. Proposition de Règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM (2018) 225 FINAL. Disponible en ligne à l'URL : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52018PC0225&from=EN (document consulté le 20 décembre 2019)

COMMISSION EUROPÉENNE, 2018b. *Déclaration de M. Ansip, vice-président, et de Mme Jourová, commissaire européenne, à la veille de l'entrée en application du règlement général sur la protection des données*. 24 mai. Déclaration n° 18/3889. Disponible en ligne : http://europa.eu/rapid/press-release_STATEMENT-18-3889_fr.htm (page consultée le 7 décembre 2019)

CONSEIL D'ETAT (FRANCE), 1970, « Les conséquences du développement de l'informatique sur les libertés publiques et sur les décisions administratives », *Rapport annuel 1969-1970*, Paris, Conseil d'Etat.

CONSEIL DE L'UNION EUROPÉENNE, 2012, Note du secrétariat général au DAPIX, Document 9897/12, 21 mai

CONSEIL DE L'UNION EUROPÉENNE, 2012b, Note du secrétariat général au DAPIX, Document 9897/12 REV 1, 24 mai

CONSEIL DE L'UNION EUROPÉENNE, 2013, Note du secrétariat général au DAPIX, Document 7105/4/13 REV 4, 19 juin

CONSEIL DE L'UNION EUROPÉENNE, 2014, Note du secrétariat général au DAPIX, Document 6762/14, 24 février

CONSEIL EUROPÉEN, 2000. *Conclusions de la Présidence. Conseil européen de Lisbonne. 23 et 24 mars 2000.* Disponible en ligne à l'URL : HTTPS://WWW.CONSILIUM.EUROPA.EU/UEDOCS/CMS_DATA/DOCS/PRESSDATA/FR/EC/00100-R1.F0.HTM (page consultée le 20 décembre 2019)

DIGITALEUROPE, 2013. « DIGITALEUROPE Comments on the Risk-Based Approach ». 28 août. Disponible en ligne : https://teknologiateollisuus.fi/sites/default/files/file_attachments/elinkeinopolitiikka_digitalisaatio_tietosuoja_digitaleurope_risk_based_approach.pdf (document consulté le 15 mai 2019)

EDRI, 2011. *Annual reports 2009-2010.* Disponible en ligne à l'URL : https://edri.org/wp-content/uploads/2014/01/EDRi-yearly-reports-2009-2010.pdf (document consulté le 20 décembre 2019)

EDPS, 2005. *Rapport annuel 2004*. Contrôleur européen de la protection des données. Disponible en ligne à l'URL : https://edps.europa.eu/sites/edp/files/publication/annual_report_2004_fr.pdf (document consulté le 20 décembre 2019)

FALQUE-PIERROTIN, I., KOHNSTAMM, J., SOUHRADA-KIRCHMAYER, E., DEBEUCKELAERE, W., MATEVA, M., NEMEC, I., SCHAAR, P., CHRISTOFFERSEN, J., LÜVRAND, S., CHRISTOFOROS, P., RODRÍGUEZ ÁLVAREZ J.L., AARNIO, R., HAWKES, B., SORO, A., PÉTERFALVI, A., SZABÓ, E.GY., DANIELIDES, Y., KUNČINAS, A., LOMMEL, G., EBEJER, J., WIEWÓROWSKI, W.R., CALVÃO, F., GRÄSLUND, G., PIRC MUSAR, N., KROČIANOVÁ, E., GRAHAM, C., BILIĆ, D. & MITTELBERGER P., 2012, *Letterfrom the Article 29 Working Party*, 16 octobre. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/other-document/index_en.htm (document consulté le 20 décembre 2019)

VLADECK, D., 2011. *A Word from Washington about Behavioral Advertising and Do Not Track*, communiqué de presse de la FTC du 8 mars. Disponible en ligne à l'URL : https://www.ftc.gov/sites/default/files/documents/public_statements/word-washington-about-behavioral-advertising-and-do-not-track/110308forasspeech.pdf (document consulté le 20 décembre 2019)

G29, 1997. *Premier rapport annuel.* Document WP 3. 25 juin. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/annual-report/files/1997/wp3_fr.pdf (document consulté le 20 décembre 2019)

G29, 2002. *Cinquième rapport annuel sur l'état de la protection des personnes à l'égard du traitement des données à caractère personnel et de la vie privée dans l'Union européenne et les pays tiers, portant sur l'année 2000. Partie I.* Document WP 54. 6 mars. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/annual-report/files/2002/wp54_1_fr.pdf (document consulté le 20 décembre 2019)

G29, 2003. *Document de travail : Transferts de données personnelles vers des pays tiers : Application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données.* Document WP 74. 3 juin. Disponible à l'URL : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_fr.pdf (document consulté le 20 décembre 2019)

G29, 2005a. *Document de travail relatif à une procédure de coopération en vue de l'émission d'avis communs sur le caractère adéquat de la protection offerte par les « règles d'entreprise contraignantes »*. Document WP107. 14 avril. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp107_fr.pdf (document consulté le 20 décembre 2019)

G29, 2005b. *8e rapport annuel du Groupe de travail « Article 29 » sur la protection des données*. Novembre. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/annual-report/files/2005/8th_annual_report_fr.pdf (document consulté le 20 décembre 2019)

G29, 2013. *Statement of the Working Party on current discussions regarding the data protection reform package.* 27 février. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_reform_package_en.pdf (document consulté le 20 décembre 2019)

G29, 2014b. *Statement on the role of a risk-based approach in data protection legal frameworks*. Document WP 218. 30 mai. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (document consulté le 20 décembre 2019)

G29, 2015. *Annexe. Points fondamentaux dans la perspective du trilogue.* 17 juin. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_fr.pdf (document consulté le 20 décembre 2019)

GASSMAN H.-P., 2010, « 30 Years after: The Impact of the oECD Privacy Guidelines », Address to the OECD Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and Its Working Party on Information Security and Privacy (WPISP). Document disponible en ligne à l'adresse : https://www.oecd.org/internet/ieconomy/44945922.doc (document consulté le 20 décembre 2019)

GASSMAN H.-P., PIPE G.R., 1974, « Rapport de synthèse », dans *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire*, Paris, Organisation de Coopération et de Développement Economique (OCDE) (Collection études d'informatique), p. 96-109.

ICANN, 2016. *Transfert de la supervision des fonctions IANA à la communauté Internet mondiale à l'expiration du contrat avec les États-Unis*. Communiqué du 1er octobre disponible en ligne à l'URL : https://www.icann.org/news/announcement-2016-10-01-fr (page consultée le 20 décembre 2019)

JOINET, LOUIS, 18 mars 2014. « Audition de M. Philippe Boucher, conseiller d'État honoraire, et M. Louis Joinet, ancien directeur juridique de la Commission nationale de l'informatique et des libertés (CNIL) », *Comptes-rendu de la MCI sur la gouvernance mondiale de l'Internet*. Disponible en-ligne sur le site du Sénat (France) : https://www.senat.fr/compte-rendu-commissions/20140317/mci_gouv.html (page consultée le 8 décembre 2019)

KÄLLNER C.-G., FREESE J., 1974, « Données individuelles : la méthode du libre-accès », dans *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire*, Paris, Organisation de Coopération et de Développement Economique (OCDE) (Collection études d'informatique), p. 67-74.

KOHNSTAMM J., 2011, *Letter from the Article 29 Working Party addressed to Vice-President Reding regarding the Article 29 WP's reaction to the Commission Communication "A comprehensive approach to personal data protection in the EU"*, 14 janvier. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_01_14_letter_artwp_vp_reding_commission_communication_approach_dp_en.pdf (document consulté le 20 décembre 2019)

KOHNSTAMM J., 2012a, *Comments on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS data*, 26 septembre. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120926_letter_to_icann_en.pdf (document consulté le 20 décembre 2019)

KOHNSTAMM J., 2012b, *Letter from the Article 29 Working Party addressed to Google regarding the upcoming change in their privacy policy*, 2 février. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120202_letter_google_privacy_policy_en.pdf (document consulté le 20 décembre 2019)

KOHNSTAMM J., 2012c, *Letter to Alain Heureux and Angela Mills-Wade, OBA Industry*, 1er mars. Disponible en ligne à l'URL : https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120301_reply_to_iab_easa_en.pdf (page consultée le 20 décembre 2019)

LABORATORY FOR COMPUTER SCIENCE (LCS), 1994. « LCS announces Web industry consortium », Communiqué de presse du MIT du 19 octobre 1994. Disponible en-ligne à l'URL : http://news.mit.edu/1994/lcs-1019 (page consultée le 20 décembre 2019)

LEIBOWITZ J., 2010, « Prepared Statement of the Federal Trade Commission on Consumer Privacy Before the Committee on Commerce, Science and Transportation of the United States Senate », Washington, D.C., Federal Trade Commission, 27 juillet. Disponible en ligne à l'URL : https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-consumer-privacy/100727consumerprivacy.pdf (document consulté le 20 décembre 2019)

NIBLETT G.B.F., 1971, « Digital Information and the Privacy Problem », *OECD Informatics Studies*, 2, Paris, OCDE.

OCDE, 1974, *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire 24-26 juin 1974*, Paris, OCDE (Etudes d'informatique).

PARLEMENT EUROPÉEN, 2013a, *Amendements déposés en Commission LIBE*, documents PE506.169 v.2.0, 6 mars 2013, Disponible en ligne à l'URL : https://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=FR&reference=PE506.169 (document consulté le 20 décembre 2019

PARLEMENT EUROPÉEN, 2013b, *Résultats du vote du 12 mars 2014 sur le document A7-0402/2013 dans la procédure 2012/011 (COD)*. Disponible en ligne à l'URL : https://oeil.secure.europarl.europa.eu/oeil/popups/printsda.pdf?id=23714&l=fr (document consulté le 20 décembre 2019)

RODOTÀ S., 1974, « Protection de la vie privée et contrôle de l'information : deux sujets d'inquiétude croissante pour l'opinion publique », dans *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire*, Paris, Organisation de Coopération et de Développement Economique (OCDE) (Collection études d'informatique), p. 149-163.

SCHWARTZ A., SHERRY L., COOPER M., TIEN L., PIERCE D., BRANDT D., ELLIS SMITH R., GIVENS B., DIXON P., 2007, « Consumer Rights and Protections in the Behavioral Advertising Sector », Center for Democracy and Technology, Consumer Action, Consumer Federation of America, Electronic Frontier Foundation, Privacy Activism, Public Information Research, Privacy Journal, Privacy Rights Clearinghouse, *World Privacy Forum*. Disponible en ligne à l'URL : http://www.worldprivacyforum.org/wp-content/uploads/2008/04/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf (document consulté le 20 avril 2020)

SÉNAT (FRANCE), 7 mai 2019. Communiqué de presse : « La commission d'enquête sur la souveraineté numérique a constitué son Bureau ». Disponible en ligne : http://www.senat.fr/presse/cp20190507.html (page consultée le 26 juillet 2019)

SIMITIS S., 1974, « Établissement de structures institutionnelles pour le contrôle et la mise en place de la protection des données », dans *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire*, Paris, Organisation de Coopération et de Développement Economique (OCDE) (Collection études d'informatique), p. 96-109.

SVENONIUS P., 1974, « Déclaration succincte », dans *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire*, Paris, Organisation de Coopération et de Développement Economique (OCDE) (Collection études d'informatique), p. 10-12.

TEGNHED L., 1974, « Protection de la vie privée et contrôle de l'information : deux sujets d'inquiétude croissante pour l'opinion publique », dans *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire*, Paris, Organisation de Coopération et de Développement Economique (OCDE) (Collection études d'informatique), p. 123-132.

TEMPEST, A., 2009, « Data Protection Conference 2009. "Personal data – more use, more protection?" Profiling, Risk Assessment & Advertising », FEDMA. Présentation faite le 19 mai 2009 à la Commission européenne. Document TEMPEST_Alistair.ppt. Téléchargeable en ligne à l'URL : http://ec.europa.eu/justice/newsroom/data-protection/events/090519_en.htm (page consultée le 29 mai 2018)

TRICOT B., 1975, « Rapport de la commission Informatique et Libertés », Paris, La documentation française.

US HOUSE OF REPRESENTATIVES, 1966, *Hearings before a Subcommittee of the Committee on Government Operations*. House of Representatives, 89th Congress, Second Session.

W3C, 2012. *Fingerprint minutes.* Minutes IRC de la réunion sur le Fingerprinting au TPAC de 2012. Disponible en ligne à l'URL : https://www.w3.org/2012/10/31-fingerprint-minutes.html (page consultée le 20 décembre 2019)

W3C TPWG, 2012. *Tracking Protection Working Group: Getting to Closed*. Decision Policy. Disponible en ligne à l'URL : https://www.w3.org/2011/tracking-protection/decision-policy.html (page consultée le 20 décembre 2019)

WARE W.H., 1973, « Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems », U.S. Department of Health, Education and Welfare.

WESTIN A.F., 1974, « La règlementation des banques de données : une étape nouvelle et ses préliminaires », dans *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire*, Paris, OCDE (Études d'informatique), p. 110-120.

YOUNGER K., 1972, *Report of the committee on privacy. Chairman: Kenneth Younger. Presented to Parliament by the Secretary of State for the Home Department, the Lord High Chancellor and the Secretary of State for Scotland by command of Her Majesty, July 1972.*, London, H.M.S.O.

Autres documents et publications

Romans et nouvelles (fiction)

ASIMOV I., 1986, *Foundation and earth*, Garden City, N.Y, Doubleday.

DICK P.K., 1956, « The Minority Report », *Fantastic Universe*, *4*, 6

GIBSON W., 1984, *Neuromancer*, New York, Ace Books.

ORWELL G., 1949, *Nineteen Eighty-Four (1984)*, London, Secker & Warburg.

Livres de non-fiction

ALBRECHT J.P., 2015A, *Hands off our data!*, Bruxelles, Jan Philipp Albrecht.

BELLANGER P., 2014, *La souveraineté numérique*, Paris, Stock.

NITOT T., CERCY N., 2016, *Numérique : reprendre le contrôle*, Framabook.

QUINIOU J.-C., 1971, *Marxisme et informatique*, Editions Sociales.

Productions audiovisuelles

JONES, A., BROOKER, C. (producteurs), 2011-…, *Black Mirror*, Endemol Shine UK, format numérique

KUBRICK, S. (réalisateur), 1968, *2001: A Space Odyssey*, Metro-Goldwyn-Meyer, format numérique

REMINGTON RAND, 1954, *1954 commercial for the UNIVAC computer*, disponible en-ligne, disponible en-ligne à l'URL : https://archive.org/details/univac1954 (page consultée le 20 décembre 2019)

REMINGTON RAND, 1956, *Fifties Advertising: UNIVAC Computer Commercial (5 February 1956) (Ad 2 of 2)* , disponible en-ligne, disponible en-ligne à l'URL : https://archive.org/details/UNIVAC-AD-2 (page consultée le 20 décembre 2019)

RODDENBERRY, G. (scénariste et producteur), 1968, « Assignment: Earth », *Star Trek*, saison 2 épisode 26, Paramount, format numérique

VIDA, H. (présentatrice), 1976, « Le Journal », *Antenne 2*, 15 juillet 1976, format numérique, disponible en-ligne à l'URL : https://www.ina.fr/video/CAB7600764601 (page consultée le 20 décembre 2019)

Pages web

ANSSI, non daté. « The European Digital Sovereignty. A Common Objective for France and Germany ». Page consultée le 25 juillet 2019 à l'URL : https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany/

AUFRÈRE L., MAUREL L., 2018a, « Pour une protection sociale des données personnelles », -*S.I.Lex* -. Page consultée le 10 avril 2020 à l'URL : https://scinfolex.com/2018/02/05/pour-une-protection-sociale-des-donnees-personnelles/#p11

BANQUE MONDIALE, 2019. « GDP (current US$) - European Union, United States, China », Banque Mondiale. Page consultée le 19 décembre 2019 à l'URL : https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-US-CN

BERNERS-LEE T., 1989, « The original proposal of the WWW, HTMLized », W3C. Page consultée le 10 avril 2020 à l'URL : https://www.w3.org/History/1989/proposal.html

BIGO D., 2014, « Diagonal mass surveillance: Gulliver versus the Lilliputians », *openDemocracy*. Page consultée le 10 avril 2020 à l'URL : https://www.opendemocracy.net/en/can-europe-make-it/diagonal-mass-surveillance-gulliver-versus-lilliputians/

BOYD DANAH, 2010, « Facebook's Move Ain't about Changes in Privacy Norms », *Zephoria.org*. Page consultée le 20 décembre 2019 à l'URL : http://www.zephoria.org/thoughts/archives/2010/01/16/facebooks_move.html

CDT, 1996, « Democratic Values for a Digital Age First Annual Report and 1996 Work in Progress ». Page consultée le 20 décembre 2019 à l'URL : https://web.archive.org/web/19970215011945/http://www.cdt.org:80/publications/annuals/96_report.html#overview

CDT, 1997, *Submission request to W3C*, 17 octobre. Disponible en-ligne : HTTPS://WWW.W3.ORG/SUBMISSION/1997/17/ (page consultée le 20 décembre 2019)

CERF, V., 1995. « IETF and the Internet Society », Internet Society, 18 juillet. Page consultée le 20 décembre 2019 à l'URL : https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/

CLARKE R., 2006, « What's Privacy? », présentation faite pour un atelier de l'Australian Law Reform Commission du 18 juillet 2006, *Rogerclarke.com*. Page consultée le 20 décembre 2019 à l'URL : http://www.rogerclarke.com/DV/Privacy.html

COMMISSION EUROPÉENNE, non daté. « Registre de transparence ». *Commission européenne*. Page consultée le 20 décembre 2019 à l'URL : https://ec.europa.eu/transparencyregister/public/consultation/search.do?reset=&locale=fr#fr

CONNOLLY D.W., 2000, « A Little History of the World Wide Web », *W3C*. Page consultée le 20 décembre 2019 à l'URL : https://www.w3.org/History.html

FOTOPOULOU A., 2014, « The Quantified Self community, lifelogging and the making of “smart” publics », *openDemocracy*. Page consultée le 20 décembre 2019 à l’URL : https://www.opendemocracy.net/en/participation-now/quantified-self-community-lifelogging-and-making-of-smart-pub/

FOWLER A., 2011, « Advertisers and Publishers Adopt and Implement Do Not Track », *The Mozilla Blog*. Page consultée le 10 avril 2020 à l’URL : https://blog.mozilla.org/blog/2011/03/30/advertisers-and-publishers-adopt-and-implement-do-not-track/

HACKENBROICH J., 2018, « Reality bytes: Europe’s bid for digital sovereignty », *ECFR*, 17 octobre 2018. Page consultée le 20 décembre 2019 à l’URL : https://www.ecfr.eu/article/commentary_reality_bytes_europes_bid_for_digital_sovereignty

HOFFMAN P., 2012, « Le Tao de l’IETF : Guide destiné aux nouveaux participants à l’Internet Engineering Task Force », IETF. Page consultée le 20 décembre 2019 à l’URL : https://www6.ietf.org/tao-translated-fr.html

INSTITUT DES HAUTES ÉTUDES DE DÉFENSE NATIONALE (IHEDN), non daté. « Session nationale "Souveraineté numérique et cybersécurité" ». Page consultée le 25 juillet 2019 à l’URL : https://www.ihedn.fr/formation/session-nationale-souverainete-numerique-et-cybersecurite

LA QUADRATURE DU NET, 27 mai 2013, « Privacy Alert #1 : le consentement explicite ». Page consultée le 19 décembre 2019 à l’URL : https://www.laquadrature.net/2013/05/27/privacy-alert-1-le-consentement-explicite-la-pierre-centrale/

LE HÉGARET P., S. D., « W3C Working/Interest Group Chair », *W3C Art of Consensus Guide*. Page consultée le 19 décembre 2019 à l’URL : https://www.w3.org/Guide/chair/role.html

LOBBYPLAG, date inconnue. « Lobbyplag ». Page consultée le 19 décembre 2019 à l’URL : https://lobbyplag.eu/lp

LYNCH B., 2012, « Advancing Consumer Trust and Privacy: Internet Explorer in Windows 8 – Microsoft on the Issues », *Microsoft TechNet*. 31 mai 2012. Page consultée le 20 avril 2020 à l’URL : https://blogs.microsoft.com/on-the-issues/2012/05/31/advancing-consumer-trust-and-privacy-internet-explorer-in-windows-8/

PARLTRACK, non daté. « Dossier 2012 (011) COD ». Page consultée le 19 décembre 2019 à l’URL : http://parltrack.euwiki.org/dossier/2012/0011%28COD%29

PELLEGRINI F., 2016, « Penser la souveraineté numérique », *La liberté n’est pas soluble dans la technique – Pellegrini.cc.*. Page consultée le 19 décembre 2019 à l’URL : http://www.pellegrini.cc/2016/06/penser-la-souverainete-numerique/

QUANTIFIED SELF, non daté. « Quantified Self. Self Knowledge Through Numbers ». Page consultée le 29 avril 2016 et le 19 juillet 2019, à l’URL : https://quantifiedself.com/

ROSSUM G. VAN, 2008, « Origin of BDFL », *Artima*. 31 juillet 2008. Page consultée le 19 décembre 2019 à l’URL : https://www.artima.com/weblogs/viewpost.jsp?thread=235725

SCHECHTER E., 2018, « A secure web is here to stay », *Google Online Security Blog*. 8 février 2018. Page consultée le 19 décembre 2019 à l'URL : https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

SMITH, B., 23 octobre 2019. « Brad Smith: Keynote Speaker ». Vidéo mise en ligne sur le site web de Youtube le 11 novembre 2019 à l'URL : https://www.youtube.com/watch?v=g_0k5vwxN0k (page consultée le 7 décembre 2019)

SOGHOIAN C., 2011, « The History of the Do Not Track Header », *slight paranoia*. Page consultée le 20 décembre 2019 à l'URL : http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html

SOGHOIAN C., STAMM S., 2009, *Universal Behavioral Advertising Opt-out*. Plug-in pour Firefox. Page consultée le 6 août 2018 https://addons.mozilla.org/en-US/firefox/addon/universal-behavioral-advertisi/ (page devenue indisponible)

SWICK R., 1997. « Comment on OPS and Web Privacy Submissions », *W3C*, 6 septembre. Page consultée le 20 décembre 2019 : https://web.archive.org/web/19970730075056/http://www.w3.org:80/Submission/1997/7/Comment.html

TUMMARELLO K., 2016, « We Won't Let You Forget It: Why We Oppose French Attempts to Export the Right To Be Forgotten Worldwide », *Electronic Frontier Foundation*. Page consultée le 20 décembre 2019 à l'URL : https://www.eff.org/fr/deeplinks/2016/11/we-wont-let-you-forget-it-why-we-oppose-french-attempts-export-right-be-forgotten

W3C, non daté (a). « W3C Privacy Interest Group ». Page consultée le 20 décembre 2019 à l'URL : https://www.w3.org/Privacy/

W3C, non daté (b). « Facts about W3C ». Page consultée le 20 décembre 2019 à l'URL : https://www.w3.org/Consortium/facts.html

W3C, non daté (c), « The Art of Consensus ». Page consulté le 20 décembre 2019 à l'URL : https://www.w3.org/Guide/

W3C, 1997. « W3C Platform for Privacy Preferences (P3) Project Approved », *W3C*, 7 juillet. Page consultée le 20 décembre 2019 à l'URL : https://web.archive.org/web/19980213180636/http://www13.w3.org:80/P3P/P3Approval.html

W3C, 2011. « Tracking Protection Working Group Initial Teleconference », *W3C*, 14 septembre. Page consultée le 20 décembre 2019 à l'URL : https://www.w3.org/2011/09/14-dnt-minutes.html

W3C, 2008. « Enabling Trust and Privacy on the Social Web ». Page consultée le 20 décembre 2019 à l'URL : https://www.w3.org/2008/09/msnws/papers/trustprivacy.html

WIEWÓROWSKI, W., 2018. « Civil society organisations as natural allies of the data protection authorities ». EDPS. 15 mai. Page consultée le 20 décembre 2019 à l'URL : https://edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection_de

YUDKOWSKY E., 2001, « Staring into the Singularity 1.2.5 », *Yudkowsky.net*. Page consultée le 20 décembre à l'URL : http://yudkowsky.net/obsolete/singularity.html

ZEIGLER A., BATEMAN A., GRAFF E., 2011, « Web Tracking Protection - W3C Member Submission ». 24 février. Page consultée le 20 décembre 2019 à l'URL : https://www.w3.org/Submission/web-tracking-protection/

Annexe 1 : Tableau comparatif entre la listes des principes énumérés dans les Lignes directrices de l'OCDE et ceux de la Convention 108 du Conseil de l'Europe

Lignes directrices de l'OCDE	Convention 108 du Conseil de l'Europe
« Principe de la limitation en matière de collecte » (art. 7[1])	« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont […] obtenues et traitées loyalement et licitement » (art. 5 a))
« Principe de la qualité des données » (art. 8)	« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont […] exactes et si nécessaire mises à jour » (art. 5 d))
« Principe de la spécification des finalités » (art. 9)	« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont […] adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées » (art. 5 c))
« Principe de la limitation de l'utilisation » (art. 10)	« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont […] enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités » (art. 5 b))
-	« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont […] conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. » (art. 5 e))
« Principe des garanties de sécurité » (art. 11 et 12)	« Article 7 – Sécurité des données Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers

1 Cet article précise que : « Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement. ». Il ne porte donc pas réellement sur la limitation des finalités (qui est, dans le vocabulaire des Lignes directrices de l'OCDE, le principe de la « limitation de l'utilisation »)

	automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés. »
« Principe de la participation individuelle » (art. 13)	« Article 8 – Garanties complémentaires pour la personne concernée Toute personne doit pouvoir: a) connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier; b) obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible; c) obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention; d) disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article. »
« Principe de responsabilité » (art. 14)	-

Annexe 2 : Tableau de l'évolution de la notion de « donnée à caractère personnel »

Date[1]	Nom de la notion dans le texte	Texte	Emplacement dans le texte	Contenu de la définition	Langue
1972	Personal Information	Privacy and the computer--steps to practicality	Chaptre 3, page 12	Statement of the form - Individual name, factual statement. The factual statement may be implied or given by context: for example, if a magnectic tape containing only a list of names is said to be a list of prison inmates. The individual identity may be submerged in apparently anonymous statistics, but if it can be extracted then it must be considered to be there.	EN
15 août 1972	personal data	Bill on protection against the misuse of personal in data protection (translation of : Referentenentwurf Bundes-Datenschutzgesetz). Conseil de l'Europe. EXP/Prot.Priv./EDB (73) 2	Section 2	By « personal data » are meant particulars concerning the personal or material condition of an identified or identifiable natural or juristic person in private law or of an identified or identifiable association of persons (hereinafter termed « the person concerned »). Public undertakings, services or administrative bodies exercising similar functions, which are or belong to public-law corporations, shall be considered equivalent to the persons referred to in sentence 1.	EN
29 septembre 1972	personal data	Draft resolution relating to the	Page 7	data concerning physical or legal persons	EN

1 Les dates en rouge indiquent des dates approximatives, lorsque le jour exact et/ou le mois exact n'ont pas pu être déterminés.

		protection of privacy vis-à-vis electronic data banks in the private sector and Preliminary draft explanatory report. Document EXP/Prot.Priv./EDB (72) 14			
22 novembre 1972	information processed by data banks as relates to the private life or privacy of the individuals whom it concerns	Appendix V Convention on transnational data banks in the private sector. Preleminary draft proposed by Mr. J.P. COSTA, French expert. EXP/Prot.Priv./EDB (72) 17 Council of Europe	Art. 2	data […] as relates to the private life or privacy of individuals whom it concerns, and particularly information concerning their race, religion, political opinions, morals, health or past judicial record	EN
16 février 1973	personuppgift	Proposition nr. 33 år 1973, devenue Datalag 1973:289 après adoption	Art. 1	upplysning som avser enskild person	SE
16 février 1973	personal data	Proposition nr. 33 år 1973, devenue Datalag	Art. 1	information relating to a unique individual	EN

		1973:289 après adoption			
26 septembre 1973	personal information	Council of Europe Resolution 73 (22) On the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector	Annex	information relating to individuals (physical persons)	EN
20 septembre 1974	personal information	Council of Europe Resolution 74 (29) On the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector	Annex	information relating to individuals (physical persons)	EN
31 décembre 1974	record	5 USC 552a. Privacy Act 1974	section (a)	any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to. his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual such as a finger or voice print or a photograph	EN
15 mars 1976	données	DSTI/CUG/ 76.9 1ère révision.	Art 1	[la convention s'applique à :] [aux] systèmes de traitement électronique de données qui traitent des données de	FR

		Annexe III. Convention nordique sur le traitement des données de caractère personnel. Projet soumis par un expert		caractère personnel [et] aux autres systèmes de traitement des données dans la mesure où ils contiennent : des données concernant la nationalité, la race, les opinions politiques ou les croyances religieuses des individus ; des données concernant des activités criminelles des individus et les sanctions pénales encourues ; des données concernant le comportement sexuel : des données concernant les enquêtes pour l'octroi de crédit et la solvabilité ; des données concernant l'attribution d'une aide sociale, d'une assistante sociale et d'autres interventions analogues ; d'autres données de caractère nettement intime ou personnel	
6 janvier 1978	données nominatives	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Art. 4	les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale	FR
23 septembre 1980	données de caractère personnel	Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel	Art. 1 sous b)	toute information relative à une personne physique identifiée ou identifiable (personne concernée)	FR
23 septembre 1980	personal data	Recommendation of the Council on Guidelines Governing the	Art. 1 sous b)	any information relating to an identified or identifiable individual (data subject)	EN

		Protection of Privacy and Transborder Flows of Personal data			
28 janvier 1981	données à caractère personnel	Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention 108 du Conseil de l'Europe)	Art. 2 sous a)	toute information concernant une personne physique identifiée ou identifiable («personne concernée»)	FR
23 septembre 1980	Personal data	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)	Art. 2 sous a)	any information relating to an identified or identifiable individual ("data subject")	EN
27 juillet 1990	données à caractère personnel	COM 90 314 FINAL FR (Commission européenne)	Art. 2 sous a)	toute information concernant une personne physique identifiée ou identifiable («personne concernée») ; est notamment réputée identifiable une personne qui peut être identifiée par une référence à un numéro d'identification ou à une information similaire	FR
27 juillet 1990	personal data	COM 90 314 FINAL EN (European Commission)	Art. 2 sous a)	any information relating to an identified or identifiable individual ("data subject") ; an identifiable individual is notably an individual who can be identified by reference to an identification number or a similar	EN

				identifying particular	
24 octobre 1995	données à caractère personnel	Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données	Art. 2 sous a)	toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale	FR
24 octobre 1995	personal data	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data	Art. 2 sous a)	any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity	EN
7 octobre 1996	données personnelles	Protection des données personnelles des travailleurs.	Paragraphe 3.1.	L'expression données personnelles s'applique à toute information relative à un travailleur identifié ou identifiable	FR

		Recueil des directives pratiques au BIT (1997)			
6 août 2004	donnée à caractère personnel	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Version consolidée au 07 août 2004	Art. 2	toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.	FR
16 février 2010	donnée à caractère personnel	Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO	Art. 1	toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique	FR
7 avril 2010	Personally Identifiable Information	NIST – SP 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	Section 2.1	PII is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.	EN
25 janvier 2012	données à caractère personnel	Proposition de Règlement du Parlement européen et	Art. 4 sous 2)	toute information se rapportant à une personne concernée	FR

		du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)			
25 janvier 2012	personal data	Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)	Art. 4 sous 2)	any information relating to a data subject	EN
5 mai 2012	personal data	Privacy Terminology – draft-hansen-privacy-	Page 2	information about an individual stored and/or transmitted electronically in Internet protocols	EN

		terminology-03.txt			
22 juin 2012	personal data	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Revised by the DAPIX meetings of 23-24 February and 14-15 March 2012	Art. 4 sous 1)	any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, by means likely to be used by the controller or by any other natural or legal person, in particular by reference to a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. If identification requires a disproportionate amount of time, effort or material resources the natural living person shall not be considered identifiable	EN
13 juillet 2012	personal data	Privacy Terminology – draft-iab-privacy-terminology-00.txt	Page 2	any information relating to a data subject	EN
24 juillet 2013	personal data	RFC6973	Section 3.2	information relating to an identified or identifiable individual	EN
23 janvier 2014	Personally Identifiable Information	PRIVACY THRESHOLD AN	Note de bas de page 2, page 3	any information that permits the identity of an individual to be directly or indirectly inferred, including any	EN

		ALYSIS (PTA). Version number 01-2014. Department of Homeland Security		information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department	
26 juin 2014	personal data	W3C Privacy Considerations		Any information relating to an individual who can be identified, directly or indirectly.	EN
3 juillet 2014	Personally Identifiable Information	USAID Privacy Threshold Analysis Template	Page 9	Personally Identifiable Information (PII) means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual	EN
11 janvier 2016	personal data/personal information	Privacy by Design Documentation for Software Engineers Version 1.0 - DRAFT Committee Specification 02 Working	Section 1.5	any data/information about an individual including (1) any data/information that can be used to distinguish or trace an individual‘s identity, and (2) any other data/information that is linked or linkable to an individual or an individual’s device	EN

		Draft 08			
27 avril 2016	données à caractère personnel	RGPD	Art. 4 sous 1)	toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale	FR
27 avril 2016	personal data	GDPR	Art. 4 sous 1)	any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	EN
17 mai 2018	donnée à caractère personnel	Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108+)	Art. 2 sous a)	toute information concernant une personne physique identifiée ou identifiable («personne concernée»)	FR

Annexe 3 : Chronologie de l’adoption du RGPD

19 et 20 mai 2009	**9/07/2009 au 31/12/2009**	**28 janvier 2010**	**4 novembre 2010**	**4/11/2010 au 15/01/2011**	**29/03/2011**	**25/01/2012**
Data Protection Conference. « Personal data – more use, more protection ? ». Conférence organisée par l'unité D5 « Protection des données » de la DG Justice de la Commission européenne	Consultation de la Commission européenne sur le cadre légal du droit fondamental à la protection des données à caractère personnel	Communiqué de presse de Viviane Reding annonçant sa volonté de réformer la directive 95/46/CE (IP/10/63)	Communiqué de presse « Protection des données: la Commission européenne présente sa stratégie pour renforcer les règles de l'Union en la matière » (IP/10/1462)	Consultation de la Commission européenne sur l’approche générale (« *comprehensive* ») de la Commission européenne en matière de protection des données à caractère personnel dans l’Union européenne	Projet de rapport de la Commission LIBE du Parlement européen sur une approche globale de la protection des données à caractère personnel dans l'Union européenne	Paquet législatif (COM (2012) 09) : la Commission européenne propose une Directive de protection des données dans le domaine de la coopération judiciaire et policière (COM (2012) 010), et un Règlement général de protection des données (COM (2012) 011)
16 février 2012	**7 mars 2012**	**12 avril 2013**	**23 mai 2012**	**10 octobre 2012**	**25 octobre 2012**	**7 décembre 2012**
Désignation de la commission LIBE pour le rapport sur le RGPD	Avis du Contrôleur européen de la protection des données (JO C/2012/192/7)	Jan Philipp Albrecht (Verts/ALE) est choisi comme rapporteur du RGPD	Avis du Comité économique et social européen (CESE/2012/1303)	Avis du Comité des régions (CDR/2012/625)	Premières discussions au Conseil de l'Union européenne selon le site du Parlement européen (3195e session du	Premières discussions de fond (de type « point B ») au sein du Conseil de l'Union européenne, dans sa formation « Justice et

					Conseil, formation Justice et affaires intérieures)	affaires intérieures » , selon le site web EUR-LEX (CSST/2012 /17486)
21 octobre 2013	**22 novembre 2013**	**12 mars 2014**	**3 septembre 2014**	**4 décembre 2014**	**11 juin 2015**	**15 décembre 2015**
Vote de la commission « LIBE » sur les amendements au RGPD. Adoption du rapport avec 48 voix pour, 1 voix contre et 3 abstentions	Dépôt du rapport de la commission LIBE	Avis du Parlement européen en première lecture (P7_TA(2014)0212)	Ouverture du trilogue	Accord politique du Conseil de l'Union européenne (3354e session du Conseil)	Adoption d'un texte d'approche générale par le Conseil de l'Union européenne (document 9565/15)	Adoption d'un compromis en trilogue (document 15039/15)
17 décembre 2015	**8 avril 2016**	**14 avril 2016**	**4 mai 2016**	**23 mai 2018**	**25 mai 2018**	**20 juillet 2018**
Adoption lors d'une réunion extraordinaire de la commission LIBE du Parlement européen d'un texte de compromis négocié en trilogue (document LIBE(2015)1217_1)	Publication de la position du Conseil de l'Union européenne (ST 5419 2016 REV 1)	Vote en deuxième lecture au Parlement européen et adoption du texte de compromis (P8_TA(2016)0125)	Publication au Journal officiel de l'Union européenne (JOUE) (JO L 119 04.05.2016, p. 0001)	Parution de rectificatifs au JOUE (JO L 127 23.05.2018, p. 0002)	Entrée en application du RGPD dans l’UE	Entrée en application du RGPD en Norvège, Islande et Liechtenstein

Annexe 4 : Liste exhaustive des « *policy papers* » et documents institutionnels intégrés au corpus pour l'étude de l'adoption du RGPD

Les listes présentées ici contiennent l'intégralité des documents téléchargés et utilisés. La liste des documents *cités* dans la thèse peut être consultée dans la bibliographie générale. Elle contient un certain nombre de détails supplémentaires sur les documents.

Corpus « Lobbyplag »

Ces fichiers ont été téléchargés sur le dépôt Github de Lobbyplag, à l'adresse : https://github.com/lobbyplag/lobbyplag-data/tree/master/raw/lobby-documents (page consultée le 31 mai 2019)

Nom du fichier	Organisation
DIGITALEUROPE_Amendments-to-Data-Protection-Regulation_final.pdf	DIGITALEUROPE
nokia_engström.pdf	Nokia
GDV_Tabelle_Datenschutz-Grundverordnung_Anmerkungen und Änderungsvorschläge_(Art 1-10).pdf	GDV
AMAZON-amendments.pdf	Amazon
FEAMSummaryDPR_ProposedAmendmentsNovember-2012.pdf	FEAM
Microsoft_final Änderungsvorschläge EU-Datenschutzgrundverordnung.pdf	Microsoft
DGB_Ergänzg _EMPL-ÄndAntr_DS-GVO-E_2012-12-03.pdf	DGB
Eurofinas-position-on-ITRE-draft-opinion.pdf	Eurofinas
20120615-EMMA_ENPA_data_protection_position_paper_short_version_final.pdf	EMMA et ENPA
Opower_CompanyOverview_October_2012.pdf	Opower
Insurance-Europe-Key-messages-to-ITRE-draft-opinion-report-on-Data-Prote....pdf	Insurance Europe
amcham_en.pdf	Amcham EU
Future of Privacy Forum White Paper on Jurisdiction.pdf	FPF
D1391E-2012-EBF-Amendments-to-EC-Proposal-for-a-Regulation-on-Data-Protection-31.10.12.pdf	EBF

Christian-Engström-letter.pdf	Nokia
Future of Privacy Forum White Paper on De-Id.pdf	FPF
GDV_Stellungnahme Artikel 79.pdf	GDV
VdH_Stellungnahme_EU-DSGVO.pdf	VdH
ACCIS-Data-Protection-Overview_FINAL.pdf	ACCIS
Proposals for amendments_Anonymous Data and Pseudonymous Data.pdf	Inconnu
Yahoo on Pseudonymous Data.pdf	Yahoo
Proposals for amendments_Aggregate Data Reports.pdf	Inconnu
International Chamber of Commerce.pdf	International Chamber of Commerce
ACCIS_Position Paper on Proposed Data Protection Regulation May 2012.pdf	ACCIS
ZDH_Änderungsanträge.pdf	ZDH
GDV_Tabelle_Datenschutz.Grundverordnung_Anmerkungen und Änderungsvorschläge (Art 22-37).pdf	GDV
DGRI_120220-stellungnahme-dgri.pdf	DGRI
ZAW_Änderungsanträge Artikel 17-18-21+.pdf	Zentralverband der Deutschen Werbewirtschaft
121212-Telefónica-Comments-on-KELLLY-draft-Opinion-.pdf	Telefónica
Gesetzl Krankenkassen_Stellungnahme DS-GVO.pdf	Deutschen Gesetzlichen Krankenkasse
1017-BUSINESSEUROPE-pp-data-protection-regulation.pdf	BUSINESSEUROPE
20120919-EMMA_ENPA-position-paper-on-proposed-Data-Protection-Regulation-September-2012.pdf	EMMA et ENPA
Kirchen_StellungnahmeEU Datenschutzgrundverordnung 09 11 2012endg.pdf	Kirchen
GDV_Tabelle Datenschutzgrundverordnung_Anmerkungen und Änderungsvo....pdf	GDV
DGB_Änderungsvorschläge zum DS-GVO-E_2012-12-07.pdf	DGB
COCIR-detailed-contribution-on-the-General-Data-Protection-Regulation-_detailed-version_25-October2012.pdf	COCIR
summary-responses-proposed-data-protection-legislation.pdf	Ministère de la justice du Royaume-Uni
x2012_039-kro-Data-protection_proposal-for-a-regulation.pdf	BEUC
FOI_Facebook_Lobbying.pdf	Facebook
Insurance-Europe-comments-on-the-ITRE-draft-opinion-report-December-	Insurance Europe

201....pdf	
20121026_Drafting-recommendations_IMCO-draft-opinion_final.pdf	Facebook
Opower_position_EU-Data-Privacy-Reform_October_2012_final.pdf	Opower
ESBA - ACT Position Paper.pdf	ESBA et ACT
EDRis-comments-on-the-JURI-draft-opinion-on-the-general-data-protection-regulation.pdf	EDRi
amazon_letter_26_1.pdf	Amazon
COCIR-Amendments-on-the-General-Data-Protection-Regulation-_-Final_25-October-2012.pdf	COCIR
COM-Rapporteur-Bits of Freedom.pdf	Bits of Freedom
FEAM-statement-Data-Protection-Regulation.pdf	FEAM
irl_dppaper.pdf	Présidence irlandaise du Conseil de l'UE et autorité irlandaise de protection des données
Adobe_EU Vorschlag zur Datenschutz Grundverordnung Änderungsvorschläge 20120713.pdf	Adobe
VDZ_endg Formulierungsvorschläge_DSVO.pdf	VDZ
Leaseurope_Observations_DPR.pdf	Leaseurope
NokiaAccountabilitypaper.pdf	Nokia
FEAM-proposed-amendments-on-the-EC-Data-Protection-Regulation.pdf	FEAM
ESBA - ACT Amendments.pdf	ESBA et ACT
1212_EuroISPA_contribution.pdf	EuroISPA
Fedil_ppdataprotection-final_17July2012.pdf	Fedil
bvh_SN_EU-DSGVO_v2.0.pdf	BVH
EDRis-comments-on-draft-imco-opinion-on-general-data-protection-regulation.pdf	EDRi
Opower-and-EED_12-10_2012.docx.pdf	Opower
data_protection_reform_latest_views_from_the_ico.pdf	ICO (autorité britannique de protection des données)
HDE_Stellungnahme Datenschutz-VO-final-Sept.2012.pdf	HDE
INTEL_Amendments_Data Protection_Tech neutrality and lawfulness of processing.pdf	Intel
BITKOM_Amendments GDPR_final.pdf	Bitkom
Set-of-Amendments-implementing-the-Accountability-Principle-into-Law-Nov-2012-3pdf.pdf	Nokia

BDIU_Stellungnahme_EU-DatenschutzGrundverordnung.pdf	BDIU
Future of Privacy Forum White Paper on Consent.pdf	FPF
Position-paper_eBay-Inc_JURI-opinion-on-data-protection-regulation.pdf	eBay
Kirchen_Data Protection Suggestions.pdf	Kirchen
D2153B-2012-EBF position onJURI draft opinion on EC Proposal for a Regulation on Data Protection.pdf	EBF
SMC-DAT-12-064-Insurance_Europe_key_messages_on_the_European_Commissions_proposed_General_Data_Protection_Regulation.pdf	Insurance Europe
ACCIS-DP-Amendments-Position-Paper_FINAL.pdf	ACCIS
Telefonica-Amendments-on-GDPR-Proposal.pdf	Telefónica
ITRE-submission.pdf	Leaseurope
Nokia-Letter-to-MEP-Andersdotter-1.pdf	Nokia
Amendments DP Regulation Bits of Freedom.pdf	Bits of Freedom
Position-paper_eBay-Inc_ITRE-opinion-on-data-protection-regulation.pdf	eBay
COCIR-position-paper-on-the-General-Data-Protection-Regulation-_Final_25-October2012.pdf	COCIR
CLOUD-Amendments-Telefónica-Nov.pdf	Telefónica
Equifax_Proposed Amendments.pdf	Equifax
DDV_Änderungsvorschläge Redline 1 - 21.pdf	DDV
GDV_Tabelle_Datenschutz.Grundverordnung_Anmerkungen und Änderungsvorschläge (Art 11-21).pdf	GDV
Microsoft_final DP amendments.pdf	Microsoft
FBF_position_protection_donnees_personnelles_EN1.pdf	FBF
BT-Amendments-DP-Regulation-08112012-FIN.pdf	British Telecom
bmi_auskunft.pdf	BMI
GDV_Tabelle Datenschutzgrundverordnung_Anmerkungen und Änderungsvor....pdf	GDV
EDRi Amendments.pdf	EDRi
EU-Data-Protection-Regulation-Multi-Association-Letter-MEP-Andersdotter-2012-October-16.pdf	AmCham EU, Digitaleurope, European-American Business Council, SIIA, USCIB
eBay-recommendation-ahead-of-IMCO-vote.pdf	eBay
us_position_20130114.pdf	États-Unis d’Amérique
facebook_imco.pdf	Facebook

eudataprotect.pdf	ICDP
DIGITALEUROPE-priorities-of-Data-Protection-Regulation_March-2012.pdf	DIGITALEUROPE
Equifax_kontaktdaten.pdf	Equifax
GDV_Stellungnahme Art. 73 bis 78.pdf	GDV
Data-Protection-Regulation-Proposal-BEUC-analyse-of-Administrative-burden.pdf	BEUC
Eurofinas-amendments-final.pdf	Eurofinas
Facebook.pdf	Facebook
AmCham_EU_Proposed_Amendments_on_Data_Protection.pdf	Amcham EU
Agoria_Stellungnahme zu Delegated Acts_02102012.pdf	Agoria

Documents issus de la consultation de 2009

Ces fichiers avaient été téléchargés à partir de la page https://ec.europa.eu/home-affairs/what-is-new/public-consultation/2009/consulting_0003_en. Cette page semble depuis avoir disparu (dernière tentative de consultation le 20 février 2019)

Nom du fichier	**Organisation**
eadp_en.pdf	EADP
bag_en.pdf	BAG
association_for_fair_data_processing_en.pdf	Bertelsmann
bell_raymond_en.pdf	Individu
epof_en.pdf	EPOF
karhula_paivikki_en.pdf	Individu
symantec_en.pdf	Symantec
dutch_government_en.pdf	Gouvernement des Pays-Bas
edri_en.pdf	EDRi
cipl_en.pdf	CIPL
aure_en.pdf	AURE
kapsch_trafficCom_en.pdf	Kapsch TraficCom
consejo_general_abogacia_espanola_es.pdf	Conseil général des

	avocats d’Espagne
bundesministerium_des_innern_de.pdf	Ministère de l’Intérieur fédéral d’Allemagne
in_house_charity_lawyers_group_en.pdf	In House Charity Lawyers Group
bitkom_en.pdf	Bitkom
gdd_en.pdf	GDD
ripe_ncc_en.pdf	RIPE NCC
american_chamber_commerce_to_eu_en.pdf	AmCham EU
freriks_gerard_en.pdf	Individu
bba_en.pdf	BBA
joint_reply_by_vno_ncw_mkb_nederland_en.pdf	VNO-NCW, MKB-Nederland
austrian_federal_economic_chamber_de.pdf	Chambre économique fédérale d’Autriche
privacy_international_en.pdf	Privacy International
center_for_democary_technology_en.pdf	CDT
british_medical_association_en.pdf	British Medical Association
visa_en.pdf	VISA
anec_en.pdf	ANEC
2_french_senators_fr.pdf	Sénateurs français
theissen_sascha_en.pdf	Individu
european_publishers_council_en.pdf	European Publishers Council
intel_corporation_en.pdf	Intel
hatscher_jordan_en.pdf	Individu
uld_schleswig_holstein_en.pdf	Autorité de protection des données du Schelswig-Holstein
the_global_privacy_alliance_en.pdf	Global Privacy Alliance

carfax_europe_en.pdf	Carfax Europe
kpf_poland_en.pdf	KPF
skype_en.pdf	Skype
yahoo_europa_en.pdf	Yahoo Europe
kortbaek_frederik_en.pdf	Individu
linklaters_llp_en.pdf	Linklaters LLP
rannenberg_kai_en.pdf	Individu
european_privacy_association_en.pdf	European Privacy Association
ppa_uk_en.pdf	PPA UK
fla_en.pdf	FLA
austrian_bar_en.pdf	Barreau autrichien
french_banking_federation_en.pdf	Fédération bancaire française
segaud_olivier_en.pdf	Individu
intrum_en.pdf	Intrum
dietrich_daniel_en.pdf	Individu
european_privacy_officers_forum_en.pdf	European Privacy Officers Forum
pounder_chris_en.pdf	Individu
henno_jacques_en.pdf	Individu
digital_europe_en.pdf	DIGITALEUROPE
emota_en.pdf	Emota
abi_en.pdf	ABI
joint_reply_esomar_efamro_en.pdf	ESOMAR et EFAMRO
cancer_research_uk_en.pdf	Cancer Research UK
bird_bird_en.pdf	Bird & Bird LLP
mpa_ivf_fiad_fiapf_en.pdf	MPA, IVF, FIAD et FIAPF
strangar_gerhard_en.pdf	Individu
bcs_en.pdf	BCS
tech_america_europe_en.pdf	Tech America Europe

eurofinas_en.pdf	Eurofinas
danish_consumer_council_en.pdf	Conseil danois des consommateurs
the_number_en.pdf	The Number
vodafone_en.pdf	Vodafone
fluck_nick_en.pdf	Individu
hide_rise_consortia_en.pdf	Projets HIDE et RISE
aldhouse_francis_en.pdf	Individu
orange_en.pdf	Orange
microsoft_corporation_2nd_document_en.pdf	Microsoft
act_en.pdf	ACT
joint_reply_enpa_faep_en.pdf	ENPA et FAEP
bt_en.pdf	British Telecom
german_insurance_association_en.pdf	Association allemande des assurances
act_joint_response_en.pdf	ACT, AER, AIG, EACA, EGTA, EPC, FEDMA et IAB
wada_en.pdf	WADA
laubacher_gerard_en.pdf	Individu
benton_dustin_en.pdf	Individu
business_software_alliance_en.pdf	BSA
ccbe_en.pdf	CCBE
international_chamber_of_commerce_icc_en.pdf	Chambre de commerce internationale
iab_europe_en.pdf	IAB Europe
ispa_en.pdf	ISPA
liberty_global_europe_en.pdf	Liberal Global Europe
council_for_healthcare_regulatory_excellence_en.pdf	CHRE
ngfg_en.pdf	NGFG
microsoft_corporation_en.pdf	Microsoft

art29_wp_and_wppj_en.pdf	Groupe de travail de l’Article 29
vlad_ioan_luca_en.pdf	Individu
ebay_en.pdf	Ebay
janet_uk_en.pdf	JANET
ueapme_en.pdf	UEAPME
euro_ispa_en.pdf	EuroISPA
international_pharmaceutical_privacy_consortium_en.pdf	Consortium international sur la vie privée de l’industrie pharmaceutique
national_aids_trust_nat_en.pdf	Fonds national contre le SIDA (Royaume-Uni)
etno_en.pdf	ETNO
rackspace_us_inc_en.pdf	Rackspace US
guernsey_data _protection_commissioner_en.pdf	Autorité de protection des données de Guernesey
edpr_en.pdf	EDPR
beuc_en.pdf	BEUC
acro_en.pdf	ACRO
corbet_rob_en.pdf	Individu
cisco_en.pdf	Cisco
uk_government_en.pdf	Gouvernement britannique
ernst_young_en.pdf	Ernst & Young
sigacus_gestion_en.pdf	Sigacus Gestion
acxiom_en.pdf	Acxiom
telecom_italia_en.pdf	Telecom Italia
the_direct_marketing_association_UK_en.pdf	Association du marketing direct (Royaume-Uni)
mcafee_en.pdf	McAfee
kanellopoulou_nadja_en.pdf	Individu

field_fisher_waterhouse_llp_en.pdf	Field Fisher Waterhouse
nursing_and_midwifery_Council_en.pdf	Conseil des infimières et des sages-femmes (Royaume-Uni)
cbi_en.pdf	CBI
berlin_data_protection_commisioner_de.pdf	Autorité de protection des données de Berlin
eiaa_en.pdf	EIAA
ecta_en.pdf	ECTA
phorm_inc_en.pdf	Phorm Inc.
data_protection_forum_en.pdf	Data Protection Forum
kilian_wolfgang_en.pdf	Individu
matthios_fabien_en.pdf	Individu
telefonica_en.pdf	Telefónica
fedma_en.pdf	FEDMA
ico_uk_en.pdf	Autorité britannique de protection des données
associazione_bancaria_italiana_en.pdf	Association bancaire italienne
vzbv_en.pdf	VZBV
isfe_en.pdf	ISFE
nhs_en.pdf	NHS
telekom_austria_en.pdf	Telekom Austria
bdi_en.pdf	BDI
yamada_yasuhide_en.pdf	Individu
fenca_en.pdf	FENCA
gsma_europe_en.pdf	GSMA Europe
european_banking_federation_en.pdf	Fédération bancaire européenne
alcatel_lucent_en.pdf	Alcatel Lucent
icmp_en.pdf	ICMP

national_information_governance_board_en.pdf	NIGB
roy-toole_christopher_en.pdf	Individu
ehfcn_en.pdf	EHFCN
european_fundraising_association_en.pdf	Association européenne de levées de fonds
ericsson_in_registering_process_en.pdf	Ericsson
general_medical_council_en.pdf	Conseil général des médecins (Royaume-Uni)
law_society_uk_en.pdf	Law Society UK
accis_en.pdf	ACCIS
nbc_universal_en.pdf	NBC Universal

Documents issus de la consultation de 2010

Ces fichiers ont été téléchargés à partir des liens trouvés sur la page https://web.archive.org/web/20101107205129/http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm (dernière consultation le 31 mai 2019).

Nom du fichier	**Organisation**
dp_at_csls_study_group_en.pdf	University of Oxford
christoforidis_k_en.pdf	Individu
deutsche_vereinigung_en.pdf	Deutsche Vereinigung für Datenschutz
dihk_de.pdf	DIHK
eadp_en.pdf	EADP
naid_en.pdf	NAID
bell_raymond_en.pdf	Individu
sabi_en.pdf	SABI
consumer_focus_en.pdf	Consumer Focus
epof_en.pdf	European Privacy Officers Forum

symantec_en.pdf	Symantec
edri_en.pdf	EDRi
krenker_andrej_en.pdf	Individu
ata_en.pdf	Air Transport Association of America
xuereb_patrick_en.pdf	Individu
aure_en.pdf	AURE
epa_en.pdf	EPA
advertising_association_en.pdf	Advertising Association UK
data_industry_platform_en.pdf	Data Industry Platform
pi_en.pdf	Privacy International
eabc_en.pdf	EABC
simon_molina_francisco_en.pdf	Individu
world_check_en.pdf	Field Fisher Waterhouse
data_inspection_board_en.pdf	Autorité suédoise de protection des données
bitkom_en.pdf	Bitkom
gdd_en.pdf	GDD
von_en.pdf	VON Europe
lo_and_tco_sv.pdf	LO et TCO
amcham_en.pdf	AmCham EU
mersault_stephan_en.pdf	Individu
feb_fr.pdf	FEB
fiad_fiapf_ivf_mpa_en.pdf	FIAD, FIAPF, IVF et MPA
deutscher_anwaltverein_de.pdf	Deutscher Anwaltverein
iab_poland_pl.pdf	IAB Pologne
lachaud_eric_en.pdf	Individu
jones_eric_en.pdf	Individu
verbraucherzentrale_de.pdf	Verbraucherzentrale

	Bundesverband
edps_en.pdf	Contrôleur européen de la protection des données
bundesministerium_des_innern_1_en.pdf	Ministère fédéral de l’Intérieur (Allemagne)
cdt_en.pdf	CDT
dsci_en.pdf	DSCI (Inde)
bird_and_bird_en.pdf	Bird & Bird LLP
godf_fr.pdf	Grand Orient de France
young_pirates_en.pdf	Young Pirates
creis_terminal_fr.pdf	CREIS Terminal
anec_en.pdf	ANEC
idnetters_en.pdf	IDNetters
bouygues_telecom_fr.pdf	Bouygues Telecom
hunton_and_williams1_en.pdf	Hunton & Williams LLP
eul_harald_de.pdf	Individu
air_berlin_en.pdf	Air Berlin
ceep_en.pdf	CEEP
ungpirat_sv.pdf	Ung Pirat
kuner_christopher_en.pdf	Individu
bdi_de.pdf	BDI
ebf_en.pdf	EBF
sncd_fr.pdf	SNCD
thl_fi.pdf	THL
enpa_and_faep_en.pdf	ENPA et FAEP
bar_council_en.pdf	Barreau d’Angleterre et du Pays-de-Galles
enacso_en.pdf	ENACSO
afep_fr.pdf	AFEP
la_poste_fr.pdf	La Poste
crid_fr.pdf	CRID

skype_en.pdf	Skype
fbf_en.pdf	FBF
activision_en.pdf	Activision
ncpi_pl.pdf	NCPI
ifpi_en.pdf	IFPI
dierks_and_bohle_de.pdf	Dierks + Bohle
step_en.pdf	STEP
at_republik_bundeskanzleramt_de.pdf	Chancellerie fédérale autrichienne
cpme_en.pdf	CPME
pl_min_pl.pdf	Ministère polonais
intrum_justitia_en.pdf	Intrum Justitia
at_republik_datenschutzkommission_de.pdf	Autorité autrichienne de protection des données
zdh_de.pdf	ZDH
ufc_fr.pdf	UFC Que Choisir
iata_en.pdf	IATA
swr_1_de.pdf	SWR
wko_de.pdf	WKO
alain_bensoussan_selas_en.pdf	Individu
zaw_de.pdf	ZAW
morpho_groupe_safran_fr.pdf	Morpho Safran
vdh_de.pdf	VDH
swedma_en.pdf	SWEDMA
emota_en.pdf	Emota
dgri_de.pdf	DGRI
abi_en.pdf	ABI
facebook_en.pdf	Facebook
gpa_en.pdf	Global Privacy Alliance
garrigues_en.pdf	Garrigues, Gide Loyrette Nouel, Noerr et Pinsent Masons

the_direct_mktg_en.pdf	DMA
gse_en.pdf	GSE
info_center_finland_en.pdf	Info Center Finland
fep_en.pdf	FEP
icc_en.pdf	ICC
fevad_fr.pdf	FEVAD
mediaset_it.pdf	Mediaset
privowny_en.pdf	Privowny
aepd_dpa_es.pdf	Autorité espagnole de protection des données
bcs_en.pdf	BCS
pinar_manas_jose_luis_es.pdf	Individu
vbw_de.pdf	VBW
euphex_en.pdf	European Public Health Experts Workshop on Privacy Protection
tech_america_europe_en.pdf	Tech America Europe
eurofinas_en.pdf	Eurofinas
breyer_patrick_1_de_attachment.pdf	Individu
Bdma_en.pdf	BDMA
the_number_en.pdf	The Number
encepp_en.pdf	ENCEPP
vodafone_en.pdf	Vodafone
gsma_en.pdf	GSMA Europe
everix_patrick_en.pdf	Individu
croft_sylvia_en.pdf	Individu
h7b1_en.pdf	h7b1
Bundesarbeitskammer_de.pdf	Bundesarbeitskammer
minjust_lv_en.pdf	Ministère de la justice de Lettonie
debet_anne_fr.pdf	Individu
orange_en.pdf	Orange

bsa_en.pdf	BSA
vno_ncw_en.pdf	VNO-NCW, MKB-Nederland
guzman_rodriguez_hector_en.pdf	Individu
cea_en.pdf	CEA
datenschutzstelle_li_de.pdf	Autorité liechtensteinoise de protection des données
ak_wien_de.pdf	Österreichische Bundesarbeitskammer
act_en.pdf	ACT
datatilsynet_en.pdf	Autorité norvégienne de protection des données
task_force_copyright_en.pdf	Copyright Task Force
a_and_n_media_en.pdf	A&N Media
arge_daten_de.pdf	Arge Daten
betfair_en.pdf	Betfair
amberhawk_en.pdf	Amberhawk Training LTD
Navigator.pdf	Individu
ippc_en.pdf	International Pharmaceutical Privacy Consortium
anacom_en.pdf	Anacom
bt_en.pdf	British Telecom
ufmd_fr.pdf	UFMD
efamro_and_esomar_en.pdf	EFAMRO et ESOMAR
etuc_en.pdf	ETUC
aktion_freiheit_de.pdf	Aktion Freiheit statt Angst
psni_en.pdf	PSNI
europeansocialnetworks_en.pdf	European Social Networks

coueignoux_philippe_and_leprat_marc_en.pdf	Individu
eBay_en.pdf	eBay
ogb_de.pdf	OGB
carrefour_fr.pdf	Carrefour
eco_de.pdf	ECO
dif_en.pdf	DIF
general_electric_en.pdf	General Electric
allen_and_overy_en.pdf	Allen & Overy
schneider_robert_en.pdf	Individu
panoptykon_fundacja_pl.pdf	Fundacja Panoptykon
mendez_raul_en.pdf	Individu
ccbe_en.pdf	CCBE
green_harry_en.pdf	Individu
minjust_uk_en.pdf	Ministère de la justice du Royaume-Uni
open_society_en.pdf	Open Society Foundations
finnish_industries_en.pdf	EK
ddv_de.pdf	DDV
wko_de2.pdf	WKO
bda_de.pdf	BDA
zentralen_kreditausschuss_en.pdf	Zentraler Kreditausschuss
gs1_en.pdf	GS1
vprt_de.pdf	VPRT
wolf_eike_de.pdf	Individu
dpoq_en.pdf	DPO Quartet
equifax_es.pdf	Equifax
iab_europe_en.pdf	IAB Europe
ispa_en.pdf	ISPA
strasser_maritta_en.pdf	Individu
ngfg_en.pdf	NGFG
pocs_matthias_en.pdf	Individu

bundesregierung_en.pdf	Gouvernement fédéral allemand
institute_innovative_progress_en.pdf	Institute for Innovative Progress
breyer_patrick_0_en.pdf	Individu
monaghan_mark_en.pdf	Individu
young_david_en.pdf	Individu
falkenberg_peter_de.pdf	Individu
at_aerztekammer_de.pdf	Chambre des médecins d'Autriche
masdevall_jordi _en.pdf	Individu
ueapme_en.pdf	UEAPME
bzak_bundeszahnarztekammer_de.pdf	Chambre fédérale des dentistes d'Allemagne
bfdi_de.pdf	Autorité fédérale allemande de protection des données
anker_wolfram_en.pdf	Individu
bundesrechtsanwaltskammer_de.pdf	Chambre fédérale des avocats d'Allemagne
egdf_en.pdf	EGDF
etno_en.pdf	ETNO
gdv_en.pdf	GDV
gmc_en.pdf	GMC
yahoo_en.pdf	Yahoo
berliner_datenschutzrunde_de.pdf	Berliner Datenschutzrunde
beuc_en.pdf	BEUC
asedie_en.pdf	ASEDIE
acro_en.pdf	ACRO
gonzalez_fuster_gloria_en.pdf	Individu
verdi_de.pdf	ver.di
uni_en.pdf	UNI Europe
efrn_en.pdf	EFRN

fiff_de.pdf	FIFF
febis_en.pdf	FEBIS
cisco_en.pdf	Cisco
at_republik_datenschutzrat_0_de.pdf	Österreichische Datenschutzrat
rihel_fr.pdf	Individu
bba_and_afme_en.pdf	AFME et BBA
natarchives_uk_en.pdf	Archives nationales du Royaume-Uni
ernst_young_en.pdf	Ernst and Young
bdiu_en.pdf	BDIU
zdf_de.pdf	ZDF
mutualite_francaise_fr.pdf	Mutualité Française
narusberg_ilona_en.pdf	Individu
digitaleurope_en.pdf	DIGITALEUROPE
wfa_en.pdf	WFA
ced_en.pdf	CED
kukk_urmas_en.pdf	Individu
vatm_de.pdf	VATM
telecom_italia_en.pdf	Telecom Italia
ojeda_enrique_en.pdf	Individu
lee_and_white_en.pdf	Lee & White
clcv_fr.pdf	CLCV
euroispa_en.pdf	EuroISPA
munich_re_en.pdf	Münchener Rückversicherungs-Gesellschaft
jbce_en.pdf	JBCE
cascianelli_paolo_en.pdf	Individu
encore_en.pdf	Projet EnCoRe
sifma_en.pdf	SIFMA
ppa_en.pdf	PPA
wood_john_en.pdf	Individu
intel_en.pdf	Intel

microsoft_en.pdf	Microsoft
ema_en.pdf	EMA
cbi_en.pdf	CBI
bbc_en.pdf	BBC
verizon_en.pdf	Verizon
aug_atheist_en.pdf	Union athéiste grècque
elra_en.pdf	ELRA
hewlett_packard_en.pdf	Hewlett Packard
oikeusministerio_fi.pdf	Ministère finlandais
foebud_en.pdf	FoeBuD
bisnode_en.pdf	Bisnode
ecta_en.pdf	ECTA
bma_en.pdf	BMA
bskyb_en.pdf	BskyB
ftc_federaltradecommission_en.pdf	FTC
telefonica_en.pdf	Telefónica
ectaa_en.pdf	ECTAA et Guild of European Business Travel Agents
fedma_en.pdf	FEDMA
van_den_broek_jasper_en.pdf	Individu
cocir_en.pdf	COCIR
hoppermann_p_en.pdf	Individu
fla_20110114.pdf	FLA
sfr_fr.pdf	SFR
cyberspace_en.pdf	Cyberspace Law and Policy Centre
brak_de.pdf	Chambre fédérale des avocats d’Allemagne
isfe_en.pdf	ISFE
icaew_en.pdf	ICAEW
nokia_en.pdf	Nokia
ntsi_fr.pdf	Master NTSI Université Paris X

ipc_info_and_privacy_comm_ca_en.pdf	Autorité ontarienne de protection des données
ico_infocommoffice_en.pdf	Autorité britannique de protection des données
oliver_paul_en.pdf	Individu
nhs_en.pdf	NHS
big_brother_en.pdf	Big Brother Watch
aea_en.pdf	AEA
fenca_en.pdf	FENCA
ebu_en.pdf	EBU
johnson_and_johnson_en.pdf	Johnson and Johnson
bdzv_and_vdz_de.pdf	BDZV et VDZ
hsk_fr.pdf	HSK Partners
invs_fr.pdf	INVS
afcdp_fr.pdf	AFCDP
epc_and_annex1_en.pdf	EPC
datev_de.pdf	DATEV
icmp_en.pdf	ICMP
deutsche_telekom _en.pdf	Deutsche Telekom
liberty_global_en.pdf	Liberty Global
dco_bestuur_onderwijs_nl.pdf	Commission Sécurité et Justice de la Seconde Chambre des Pays-Bas
dpof_en.pdf	DPOF
tuvit_en.pdf	TÜV IT
accis_en.pdf	ACCIS
cpvp_en.pdf	Autorité belge de protection des données
eurojust_en.pdf	Eurojust
laxen_jon_en.pdf	Individu
centralchambercommerce_fi_en.pdf	Chambre centrale de commerce de

	Finlande
ziemba_krzysztof_en.pdf	Individu
equipe_obm_fr.pdf	Équipe Obligations Biens Marché de l'Université Paris Est Créteil

Documents du Conseil de l'Union européenne

Identifiant du document	**Titre ou description du document (descriptions en italique)**	**Date**
7375/12 EN	Opinion of the European Data Protection Supervisor on the data protection reform package	8 mars 2012
7455/12 EN	Commission proposal for a General Data Protection Subject: Regulation - 1995 Data Protection Directive	9 mars 2012
8366/12 EN	Opinion of the Article 29 Working Party on the data protection reform package	30 mars 2012
8699/12 EN	Letter from the Chair of the Working Party on Statistics	13 avril 2012
9897/12 EN	*Commentaires des délégations nationales sur les chapitres I et II de la proposition de RGPD*	21 mai 2012
11326/12 EN	*Texte révisé de proposition de RGPD proposé par la Présidence du Conseil suite aux réunions du DAPIX du 23-24 février et 14-15 mars*	22 juin 2012
14147/1/12 EN	*Commentaires des délégations nationales sur les articles 11 à 27 de la proposition de RGPD*	10 octobre 2012
7105/4/13 EN	*Commentaires des délégations nationales sur les chapitres VI et VII de la proposition de RGPD*	19 juin 2013

7464/1/14 EN	*Commentaires des délégations nationales sur le mécanisme de guichet unique*	27 mars 2014
6723/6/13 EN	*Commentaires des délégations nationales sur le chapitre V de la proposition de RGPD*	23 avril 2014
11289/14 EN	*Note de la présidence du Conseil de l'Union européenne sur le droit à l'oubli et l'arrêt Google contre AEPD de 2014*	3 juillet 2014
11481/14	*Note de la présidence du Conseil de l'Union européenne sur l'approche basée sur le risque*	3 juillet 2014

Annexe 5 : Nombre d’amendements par disposition de la proposition de RGPD

Liste des dix dispositions ayant fait l’objet du plus grand nombre de propositions d’amendements en commission par des parlementaires européens selon les données de Lobbyplag.eu

Disposition	Thème	Nombre d’amendements proposés
Ajout après l’art. 6 paragraphe 1	Création d’une nouvelle base légale à l’article 6	32
Art. 6 par. 1 sous f)	Définition de l'intérêt légitime comme base légale pour un traitement	27
Ajout après l’art. 2 paragraphe 2	Propositions diverses sur le champ d’application de la proposition de règlement	26
Art. 33 paragraphe 7	Durée du mandat du délégué à la protection des données	25
Art. 35 paragraphe 1, sous b)	Obligation de nommer un délégué à la protection des données si le traitement est effectué par une entreprise de 250 salariés ou plus	25
Art. 20 paragraphe 1	Interdiction au profilage de produire des effets juridiques	24
Art. 18 paragraphe 1	Droit à la portabilité des données	24
Ajout après l’art. 82 paragraphe 1	Renforcement de la protection de la vie privée sur le lieu de travail	24
Art. 4 paragraphe 1	Définition de la notion de « personne concernée »	23
Art. 35 paragraphe 1	Régime d'obligation de nomination d'un délégué à la protection des données	23

Liste des douze[1] dispositions ayant fait l'objet du plus grand nombre de propositions d'amendements rédigés et proposés aux députés européens par des groupes d'intérêt selon les données de Lobbyplag.eu

Disposition	Thème	Nombre d'amendements proposés
Considérant 34	Définition du consentement	9
Art. 6 paragraphe 1 sous f)	Définition de l'intérêt légitime comme base légale pour un traitement	8
Considérant 25	Définition du consentement	7
Art. 4 paragraphe 8	Définition du consentement	7
Art. 20 paragraphe 1	Interdiction au profilage de produire des effets juridiques	6
Art. 4 paragraphe 1	Définition de la notion de « personne concernée »	6
Art. 7 paragraphe 4	Restriction de la définition du consentement : le consentement n'est pas un fondement juridique valable pour le traitement s'il existe un déséquilibre entre les parties	6
Art. 4 paragraphe 13	Définition de la notion d'établissement principal	6
Art. 6 paragraphe 4	Traitement ultérieur incompatible avec les finalités initiales	6
Art. 31 paragraphe 1	Obligation de notification à l'autorité de contrôle des violations de données à caractère personnel	6
Considérant 27	Définition de la notion d'« établissement principal »	6
Art. 3 paragraphe 2 sous a)	Champ d'application du règlement : application si le responsable du traitement offre des biens ou services à des personnes concernées dans l'UE	6

1 Le choix initial était une sélection de dix propositions, mais nous avons inclus la 11e et la 12e qui ont le même nombre d'amendements proposés que la 10e

Annexe 6 : Tableau comparatif entre l’art. 7 de la directive 95/46/CE, l’art. 6 paragraphe 1 de la proposition de RGPD de 2012, et l’art. 6 paragraphe 1 du RGPD tel qu’adopté en avril 2016

Art. 7 de la directive de 1995	Art. 6 paragraphe 1 de la proposition de la Commission	Art. 6 paragraphe 1 du RGPD
Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si : **a) la personne concernée** a indubitablement donné son consentement ou **b)** il **est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci** ou **c)** il **est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis** ou d) il **est nécessaire à la sauvegarde** de l'intérêt vital **de la personne concernée** ou e) il est **nécessaire à**	**Le traitement de données à caractère personnel n'est licite que si et dans la mesure où l’une au moins des situations suivantes s'applique :** a) la personne concernée **a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques** ; b) **le traitement** est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; c) **le traitement** est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; d) **le traitement** est nécessaire à la sauvegarde **des intérêts vitaux** de la personne concernée ; e) **le traitement** est nécessaire	Le traitement n'est licite que si, et dans la mesure où, **au moins une des conditions** suivantes **est remplie** : a) **la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;** b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée **ou d'une autre personne physique** ; e) le traitement est nécessaire à l'exécution d'une mission

l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ou f) il est **nécessaire** à la réalisation de l'intérêt légitime poursuivi par le **responsable du traitement** ou par le ou les **tiers** auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux **de la personne concernée**, qui appellent **une protection** au titre de l'article 1er paragraphe 1.	à l'exécution d'une mission **effectuée dans l'intérêt général ou** relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; f) **le traitement** est nécessaire **aux fins des intérêts légitimes poursuivis par un** responsable du traitement**, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux** de la personne concernée, **qui exigent** une protection **des données à caractère personnel, notamment lorsque la personne concernée est un enfant. Ces considérations ne s'appliquent pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.**	d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement **ou par un tiers**, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. **Le point f) du premier alinéa ne s'applique** pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.
En gras : le texte repris à l'identique dans le RGPD adopté en 2016	En gras : les changements textuels par rapport à la directive de 1995	En gras : les changements par rapport à la proposition initiale de la Commission

Annexe 7 : Exemple de grille d'entretien du terrain sur le RGPD

Chaque grille d'entretien a été adaptée à la marge en fonction du profil de la personne interrogée, et de la durée prévue pour l'entretien.

Les entretiens ayant été conçus pour être semi-directifs, l'ensemble des questions n'ont pas été nécessairement été posées. Elles ont pu être regroupées, reformulées, ou remplacées par d'autres questions, lorsque ces questions ont semblé être plus pertinentes que celles initialement prévues au cours de l'entretien.

Les grilles d'entretien suivent toutefois une structure similaire.

La grille d'entretien montrée ici est celle qui a servi de base à l'entretien avec une employée de la Fondation Panoptykon à Varsovie.

1) Cerner les objectifs (deep core / near policy core)

- What is the aim of Fundacja Panoptykon?
- What was the Fundacja Panoptykon's position on the GDPR?
- What motivated the involvement of Fundacja Panoptykon in the GDPR process? What are the sources of inspiration? (academic literature, philosophy, news, people, organisations, arts, movies, religion...)
- Why do we need data protection? What is it about? Are data protection and privacy the same thing?
- Can the Law, the State, provide data protection? Is it a good idea?
- Are privacy and technological progress compatible at all?

2) Exemples concrets d'objectifs (secundary aspects)

- Do you have examples of concrete disposals that you would have wished to have changed, or concrete disposals that you believe go in the right direction?
- Do you have an example of a „victory" and of a „defeat" in the provisions that were finally adopted?

3) Structure des arguments

- What were the toughest arguments of your opponents that you had to debunk?
- What were your most winning arguments?

4) Identification des alliances et rivalités

- Who do you believe were the most influential groups or people during the whole process, besides the obvious involvement of people like Jan Philipp Albrecht, Axel Voss and Bruno

Giencarelli? (it can also include people working for MEP's, or low-level members of the DAPIX)

- Who did you have a good working relation with?
- Would you say that Access, Privacy International, EPIC, La Quadrature, EDRi, CDT and Mozilla all have the same objectives, and that those objectives are the same as you?
- Who were your rivals? Were they united or not?
- Did you feel that the left/right opposition was relevant during the GDPR process?
- Did you have any contact with industry representatives?
- Have you heard of the word "privacy community"? Who do you feel are part of it, and how influential are they?
- Do you work only at EU institution level, or are you also active in private regulatory fora like the W3C, in the US, etc. ? Did you have contacts with the Article 29 WP? If not, do you know about those fora, do you have contact with people there? Who do you consider the most important regulator, the one with the biggest impact on the industry you were working
  For?
- How do you evaluate the role of DPA's and DPO organisations in this process?

5) Identifier des documents pertinents

- Do you have any policy papers, by either you or other organisations (allies or rivals or official institutions) that you can share? I did not find any position paper in English by Panoptykon either on Lobbyplag or on the Commission's website...
- Is there anyone you believe I should absolutely meet in the frame of this research?

6) Question finale

- Is there anything you would like to add that you feel we should have talked about during this interview?

Annexe 8 : Composition de l'Industry Coalition for Data Protection en septembre 2012

En septembre 2012, l'ICDP fédérait, selon un communiqué d'euroISPA[1], la fédération d'associations européennes de représentation des intérêts des fournisseurs d'accès à Internet, les associations suivantes :

- *The Association for Competitive Technology* (ACT AIBSL), qui représente des entreprises de développement d'applications mobiles, et indiquait en 2012 être également financée par eBay, Microsoft, Oracle, Intel et Verisign[2] ;
- AmCham EU, la chambre de commerce des États-Unis d'Amérique en Europe, regroupant des entreprises états-uniennes implantées en Europe[3] ;
- *The Business Software Alliance* (BSA), représentant les intérêts d'industriels du logiciel, avec des membres, en septembre 2012, comme Adobe, Apple, McAfee, Microsoft et Symantec[4] ;
- DIGITALEUROPE, qui, en septembre 2012, prétendait disposer de plus de 100 entreprises adhérentes présentes sur le marché des produits et services informatiques, sans toutefois permettre l'accès à une liste de ces adhérents[5] ;
- *The European Digital Media Association* (EdiMA), qui regroupe aujourd'hui des entreprises comme Apple, Facebook, Airbnb, Oath, Tripadvisor ou encore Amazon[6] ;
- *The European Multi-channel and Online Trade Association* (EMOTA), qui regroupait en 2012 des associations nationales comme une association tchèque d'industriels du marketing direct (*Asociace direkt marketingu a zásilkového obchodu*), ou l'*Interactive Media in Retail Group* britannique[7], qui représentent des industriels de la vente en ligne ;

1 Communiqué de presse daté de septembre 2012 d'euroISPA : « Industry Coalition for Data Protection. Reforming Europe's Privacy Framework – How to find the right balance »
2 Voir la page web https://web.archive.org/web/20121029153712/http://actonline.org/about-us/ (consultée le 10 mai 2019)
3 Le site amchameu.eu de 2012 n'a pas été correctement par Archive.org et n'est donc plus accessible
4 Voir la page web https://web.archive.org/web/20120714133332/http://www.bsa.org/country/BSA%20and%20Members/Our%20Members.aspx (consultée le 10 mai 2019)
5 Voir la page web https://web.archive.org/web/20121101114417/http://www.digitaleurope.org/ (consultée le 10 mai 2019)
6 Voir : http://edima-eu.org/ (page consultée le 10 mai 2019). Archive.org ne dispose pas d'archives de ce site web remontant à avant décembre 2015.
7 Voir : https://web.archive.org/web/20120927215357/http://www.emota.eu/members.html (page consultée le 10 mai 2019)

- *The European Publishers Council* (EPC), qui regroupait en septembre 2012 plusieurs maisons d'édition et groupes de presse comme Axel Springer, Sanoma, Thomson Reuters, ou encore Der Standard[8] ;
- EuroISPA, qui se décrit comme « la voix des fournisseurs d'accès à Internet en Europe »[9], et fédérait en septembre 2012 différentes fédérations nationales de fournisseurs d'accès à Internet, comme l'Association des fournisseurs d'accès et de services internet et la Fédération française des telecom pour la France, ou encore la *Verband der deutschen Internetwirtschaft* allemande[10]
- *The Federation of European Direct and Interactive Marketing* (FEDMA), qui se décrit comme représentant les intérêts des entreprises du domaine du marketing direct, et qui en septembre 2012 regroupait à la fois des fédérations nationales comme l'Union française du marketing direct[11], et des entreprises directement membres, comme Acxiom, la Deutsche Post, La Poste, ou encore le Reader's Digest[12] ;
- *The Interactive Advertisement Bureau Europe* (IAB Europe), branche européenne de l'IAB, qui avait pour membres en septembre 2012 des entreprises comme Adobe, Alcatel-Lucent, Criteo, Deutsche Post, eBay, Viacom et Yahoo[13] ;
- *The Interactive Software Federation of Europe* (ISFE), qui se décrit comme représentant les intérêts des éditeurs de jeux vidéo, et regroupait en septembre 2012 à la fois des associations nationales comme *Games Ireland* et des entreprises directement adhérentes comme Sega, Nintendo, Ubisoft et Microsoft[14] ;
- *The Japan Business Council in Europe* (JBCE), regroupant des entreprises japonaises présentes sur le marché européen, comme, à la date de septembre 2012, Canon, Casio, Hitachi, Kyocera, Toshiba ou encore Yamaha[15] ;
- TechAmerica Europe, branche européenne de l'association américaine TechAmerica, qui en septembre 2012 avait pour membres 745 entreprises de taille et de cœur d'activité variés, comme Adobe, Amazon, Apple, AT&T, Cisco, et Hewlett-Packard, mais aussi des

8 Voir : https://web.archive.org/web/20120818192534/http://epceurope.eu/about/our-values/ (page consultée le 10 mai 2019)
9 « The voice of ISPs in Europe »
10 Voir : https://web.archive.org/web/20121019184914/http://www.euroispa.org/about/who-we-are/members (page consultée le 10 mai 2019)
11 Voir : https://web.archive.org/web/20121017112437/http://www.fedma.org/index.php?id=150&L=2%27 (page consultée le 10 mai 2019)
12 Voir : https://web.archive.org/web/20121017112533/http://www.fedma.org/index.php?id=151&L=2%27 (page consultée le 10 mai 2019)
13 Voir : https://web.archive.org/web/20120919092801/http://iabeurope.eu/Corporate-Members.aspx (page consultée le 10 mai 2019)
14 Voir : https://web.archive.org/web/20120906082625/http://www.isfe.eu/about-isfe/members (page consultée le 10 mai 2019)
15 Voir : https://web.archive.org/web/20130226050352/http://www.jbce.org/cms/about_jbce/members.aspx (page consultée le 10 mai 2019)

entreprises moins connues[16] ayant pour point commun, selon le descriptif sur le site web de l'association américaine, d'être des entreprises « technologiques »[17] ;

- *The World Federation of Advertisers* (WFA) qui, en août 2012, comptait parmi ses adhérents des entreprises comme Emirates, AB InBev, MasterCard, SAP et Vodafone[18], et des associations nationales dont la liste à la date d'août ou septembre 2012 n'est plus accessible.

16 Voir la liste complète sur : https://web.archive.org/web/20120909065424/http://www.techamerica.org/Members/search.cfm (page consultée le 10 mai 2019)

17 Voir : https://web.archive.org/web/20120909065110/http://www.techamerica.org/about-techamerica (page consultée le 10 mai 2019)

18 Voir : https://web.archive.org/web/20120730192353/http://www.wfanet.org/en/about-wfa/member-companies (page consultée le 10 mai 2019)

Annexe 9 : Composition du W3C PING et du W3C TPWG

Les noms énumérés dans le tableau ci-dessous proviennent des listes officielles des membres du Privacy Interest Group *et du* Tracking Protection Working Group *du W3C au 26 février 2016, qui étaient disponibles aux adresses suivantes à cette date-là :*

- https://www.w3.org/2000/09/dbwg/details?group=49311&public=1
- https://www.w3.org/2000/09/dbwg/details?group=52497&public=1

Les personnes appartenant officiellement aux deux groupes sont indiquées en gras.

La présence de ces personnes dans les listes des membres officiels ne présume en rien de leur participation effective à ces groupes, et n'exclut pas la participation de facto *de personnes qui ne sont pas officiellement membres ou experts invités.*

Membre du PING	**Nom**	**Employeur ou autre organisme de rattachement (en italique si la personne est expert invité à titre individuel)**	**Membre du TPWG**
X	Jari Alvinen	Nokia	
	Rebecca Arbogast	Comcast Corporation	X
	Dan Auerbach	Electronic Frontier Foundation	X
	Adrian Bateman	Microsoft	X
X	Dominique Battré	Google	
	Elise Berkower	The Nielsen Company	X
	Chao Bian	Tencent	X
	Neil Bowman	BBC	X
	Rudy Brioche	Comcast	X
X	**Justin Brookman**	***CDT***	**X**
	Dan Caprio	Comcast	X
X	**Carl Cargill**	**Adobe**	**X**

	Qu Chao	Tencent	X
	Jeffrey Chester	*Center for Digital Democracy*	X
	Amy Colando	Microsoft	X
	Yaso Córdova	Brazilian Network Information Center	X
X	Frank Dawson	Nokia	
X	José M. del Alamo	Universidad Politécnica de Madrid	
X	**Nick Doty**	**UC Berkeley**	**X**
	Ian Fette	Google	X
	Roy Fielding	Adobe	X
X	**Joanne Furtsch**	**TRUSTe**	**X**
X	Narm Gadiraju	Intel	
	Hanrui Gao	Qihoo 360 Technology	X
	Paul Glist	Comcast	X
	Sue Glueck	Microsoft	X
X	**Vinay Goel**	**Adobe**	**X**
	Euan Grant	Microsoft	X
X	**Joseph Hall**	**CDT**	**X**
X	Katie Haritos-Shea	Knowbility	
	Sean Harvey	Google	X
	Ronan Hefferman	The Nielsen Company	X
X	Luke Herbert	*Deloitte*	
X	Jane Horvath	Apple	
	Bin Hu	AT&T	X
X	**Renato Ianella**	**Queensland University of Technology et University of Hong Kong**	**X**
	Susan Israel	Comcast	X
X	François Jacquenet	Université de Lyon	
	Daniel Jaffe	Association of National Advertisers	X
	Jeff Jaffe	W3C	X

	Simon Krauss	Cable Television Laboratories	X
	Brad Kulick	Yahoo!	X
	Kennie Kwong	AT&T	X
	Jason Lenhart	Comcast	X
	Ted Leung	Walt Disney	X
	Gerard Lewis	Comcast	X
X	**Jessica Li**	**Tencent**	**X**
X	Kepeng Li	Alibaba	
X	Charles McCathie Nevile	Yandex	
	Aleecia McDonald	Stanford University	X
	Walter Michel	Comcast	X
	Yue Min	Baidu	X
X	Ram Mohan	Affilias	
X	Hirotaka Nakajima	W3C	
	Erik Neuenschwander	Apple	X
X	Greg Norcie	CDT	
	Edward O'Connor	Apple	X
X	**Mike O'Neill**	***Baycloud***	**X**
X	Lukasz Olejnik	*Consultant indépendant*	
X	Marta Pierkarska	Deutsche Telekom	
X	Yrjana Rankka	OpenLink Software	
	MeMe Rasmussen	Adobe	X
X	Simon Rice	*ICO*	
X	Christine Runnegar	*ISOC*	
	Keith Scarborough	Association of National Advertisers	X
X	**Thomas Schauf**	**Bundesverband Digitale Wirtschaft**	**X**
	Matthias Schunter	Intel	X
X	**Wendy Seltzer**	**W3C**	**X**
X	**Rob Sherman**	**Facebook**	**X**
	John Simpson	*Consumer Watchdog*	X

X	**David Singer**	**Apple**	**X**
	Michael Smith	W3C	X
	Kevin Smith	Adobe	X
X	Rhys Smith	*Jisc*	
X	Eric Stephan	Pacific Northwest National Laboratory	
	Bryan Sullivan	AT&T	X
X	Keiji Takeda	W3C	
	Weihua Tao	Qihoo 360 Technology	X
X	Ted Thibodeau	OpenLink Software	
	Caten Tian	Qihoo 360 Technology	X
	Lee Tien	Electronic Frontier Foundation	X
	Vincent Toubiana	*CNIL*	X
X	**Kevin Trilli**	**TRUSTe**	**X**
X	**Rob van Eijk**	***Autoriteit Persoonsgegevens***	**X**
	Walter van Holst	*(affiliation inconnue)*	X
	Mark Vickers	Comcast	X
X	**Frank Wagner**	**Deutsche Telekom**	**X**
X	Rigo Wenning	W3C	
X	**Heather West**	**Mozilla**[1]	**X**
X	Mike West	Google	
X	Tara Whalen	Google	
X	**Shane Wiley**	**Yahoo!**	**X**
X	**Jing Wu**	**RITT**	**X**
	Xuemei Yan	Tencent	X
X	Xiaoqing Yang	Baidu	
X	**Yangguang Zhao**	**RITT**	**X**
	Horace Zhou	Tencent	X

1 Listée comme employée de la fondation Mozilla sur la page du PING, et à la fois comme employée de Google et de Mozilla sur la page du TPWG.

Annexe 10 : Chronologie des actions en matière de « *privacy* » dans les arènes de standardisation technique

Cette liste est un document de travail qui a été complété pendant l'enquête de terrain sur le W3C. Elle fournit un certain nombre de points de repères mais ne prétend pas être exhaustive.

Date de début	Date de fin	Événement	URL
14 avril 1980	16 avril 1980	Conférence : 1st IEEE Symposium on Security and Privacy	https://ieeexplore.ieee.org/document/6233694
16 mai 1997	-	Vote sur la création du projet Platform for Privacy Preferences du W3C	https://web.archive.org/web/19980213180636/http://www13.w3.org:80/P3P/P3Approval.html
23 mai 1997	-	Approbation par Tim Berners-Lee du projet Platform for Privacy Preferences au W3C	https://web.archive.org/web/19980213180636/http://www13.w3.org:80/P3P/P3Approval.html
2 juin 1997	-	Proposition : « Web Privacy - Privacy and Profiling on the Web » soumise au W3C	https://web.archive.org/web/199707300

			75050/ http:// www.w3.org:80/ Submission /1997/7/
2 juin 1997	-	Proposition : « OPS - Open Profiling Specification » soumise au W3C	https:// web.archive .org/web/ 19980213181518/ http:// www13.w3 .org:80/ Submission /1997/6/
11 juin 1997	-	Présentation d'un prototype de P3P devant la FTC américaine (par Tim Berners-Lee)	https:// web.archive .org/web/ 19980213181256/ http:// www13.w3 .org:80/ Talks/ 970612-ftc/
26 juin 1997	-	Kickoff meeting du projet Platform for Privacy Preferences au W3C	https:// web.archive .org/web/ 19980202184103/ http:// www.w3.org:80/P3P/
17 octobre 1997	-	Proposition officielle de l'Internet Privacy Working Group faite au W3C de reprendre le travail sur P3P	https:// web.archive .org/web/ 19980213181140/ http:// www13.w3 .org:80/ Submission /1997/17/
30 octobre	-	Communiqué de presse du W3C annonçant la fin de la « première	https://

1997		phase » du projet P3P	web.archive.org/web/19980213180947/http://www13.w3.org:80/P3P/press_release.html
19 mai 1998	-	Publication par le W3C de la première mouture de la recommandation P3P 1.0	https://www.w3.org/Press/1998/P3P
12 novembre 2003	13 novembre 2003	Conférence : W3C Workshop on the Future of P3P	https://www.w3.org/2002/12/18-p3p-workshop-report.html
17 octobre 2006	18 octobre 2006	Conférence : W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement	https://www.w3.org/2006/07/privacy-ws/
13 novembre 2006	-	Publication par le W3C du document : The Platform for Privacy Preferences 1.1 (P3P1.1) Specification	https://www.w3.org/TR/P3P11/
22 novembre 2006	-	Dernier e-mail avant la fermeture de la mailing-list public-p3p-spec (avec annonce de la création future d'un *Privacy Interest Group*)	https://lists.w3.org/Archives/Public/public-p3p-spec/2006Nov/0010.html
4 février 2007	-	Première téléconférence *Policy Language Internet Group* (PLING)	https://www.w3.org/Policy/pling/wiki/2007-12-04
17 novembre	18 novembre	Conférence : W3C Workshop on Access Control Application Scenarios	https://www.w3.or

2009	2009		g/2009/policy-ws/
12 juillet 2010	13 juillet 2010	Conférence : W3C Workshop on Privacy for Advanced Web APIs	https://www.w3.org/2010/api-privacy-ws/
19 juillet 2010		Premier e-mail sur la mailing-list *public-privacy* du W3C	https://lists.w3.org/Archives/Public/public-privacy/2010JulSep/0000.html
23 septembre 2010	-	Premier e-mail sur la mailing list *ietf-privacy* de l'IETF	https://mailarchive.ietf.org/arch/msg/ietf-privacy/h0ItYnwDE195RAXYAJ4tZvX3Rl8
4 octobre 2010	5 octobre 2010	Conférence : W3C Workshop on Privacy and data usage control	https://www.w3.org/2010/policy-ws/
8 décembre 2010	9 décembre 2010	Conférence : IAB/ISOC/W3C Internet Privacy Workshop 2010	https://www.iab.org/activities/workshops/internet-privacy-workshop-2010/
21 décembre 2010	-	Premier e-mail sur la mailing-list *privacydir* de l'IETF	https://mailarchive.ietf.org/arch/search/?email_list=privacydir&so=date

11 janvier 2011	-	Dernière téléconférence du PLING (W3C)	https://www.w3.org/Policy/pling/wiki/2011-01-11
7 mars 2011	-	Publication d'un brouillon de RFC sur le site de l'IETF intitulé : « Do Not Track: A Universal Third-Party Web Tracking Opt Out », par Jonathan Mayer, Arvind Narayanan et Sid Stamm	https://datatracker.ietf.org/doc/draft-mayer-do-not-track/
28 avril 2011	29 avril 2011	Conférence : Workshop on Web Tracking and User Privacy	https://www.w3.org/2011/track-privacy/report
3 juin 2011	5 juin 2011	Conférence : Workshop on Social Network Interoperability and Privacy	https://web.archive.org/web/20110717173330/http://d-cent.org/fsw2011/
14 septembre 2011	-	Téléconférence initiale de lancement du *Tracking Protection Working Group*	https://www.w3.org/2011/09/14-dnt-minutes.html
21 septembre 2011	-	Recontre « F2F » (en présentiel) initiale du *Tracking Protection Working Group*	https://www.w3.org/2011/tracking-protection/agenda-20110922
12 mars 2012	-	Publication de la RFC 6973 par l'IETF	https://tools.ietf.org/html/draft-iab-privacy-considerati

			ons-02
3 avril 2012	-	Mail de Tara Whalen (co-signé par Christine Runnegar) annonçant le premier *kick-off call* du PING	https://lists.w3.org/Archives/Public/public-privacy/2012AprJun/0007.html
13 avril 2012	-	Diffusion du mail de Christine Runnegar, co-signé par Tara Whalen, publiant l'ODJ pour le kick-off call	https://lists.w3.org/Archives/Public/public-privacy/2012AprJun/0018.html
19 avril 2012	-	Kick-off call de PING	https://lists.w3.org/Archives/Public/public-privacy/2012AprJun/0065.html
29 mai 2012	-	Dernier e-mail avant la fermeture de la mailing-list *privacydir* de l'IETF	https://mailarchive.ietf.org/arch/msg/privacydir/b8idQJFWkFmCkyFNyDEktAlCbaM
26 novembre 2011	27 novembre 2011	Conférence : W3C Workshop: Do Not Track and Beyond	https://www.w3.org/2012/dnt-ws/report
28 juin 2013	-	Publication par Frank Dawson, pour le W3C PING, du document : « Specification Privacy Assessment (SPA) »	http://yrlesru.github.io/SPA/
15 août 2013	-	Création à l'IETF de la liste de discussion Handling Pervasive Monitoring (*perpass*)	https://mailarchive.ietf.org/

			arch/msg/perpass/l2f63F2khcjHZl4lsLhEU4o772Q
6 novembre 2013	-	Réunion de la Mailing List Perpass de l'IETF lors de l'IETF 88	https://datatracker.ietf.org/doc/agenda-88-perpass/
28 janvier 2014	1er mars 2014	Conférence : A W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)	https://www.w3.org/2014/strint/
Mai 2014	-	Publication par l'IETF de la RFC7258	https://tools.ietf.org/html/rfc7258.html
3 septembre 2014	4 septembre 2014	Conférence : Next steps on trust and permissions for Web applications (W3C)	https://www.w3.org/2014/07/permissions/
20 novembre 2014	21 novembre 2014	Conférence : W3C Workshop on Privacy and User-Centric Controls	https://www.w3.org/2014/privacyws/
20 août 2015	-	Le document « Tracking Preference Expression (DNT) » devient une *Candidate Recommandation* du W3C	https://www.w3.org/TR/2015/CR-tracking-dnt-20150820/
24 novembre 2015	-	Publication par Nick Doty pour le W3C PING du document : « Fingerprinting Guidance for Web Specification Authors (Draft) »	https://www.w3.org/TR/fingerprinting-guidance/
10 décembre	-	Publication par le W3C TAG d'une première version du « Self-Review Questionnaire: Security and Privacy »	https://www.w3.or

2015			g/TR/security-privacy-questionnaire/
26 avril 2016	-	Le document « Tracking Compliance and Scope (DNT) » du W3C devient une *Candidate Recommandation*	https://www.w3.org/TR/tracking-compliance/
18 août 2016	-	Publication du document « Privacy Considerations for Web Protocols. Unofficial Draft » par Hannes Tschofening et Nick Doty pour le W3C PING	https://w3c.github.io/privacy-considerations/
17 avril 2018	18 avril 2018	Conférence : W3C Data Privacy Controls and Vocabularies	http://www.w3.org/2018/vocabws/
10 avril 2018	-	Extension de la charte du Tracking Protection Working Group Charter	https://lists.w3.org/Archives/Public/public-tracking/2018Apr/0002.html
18 septembre 2018	19 septembre 2018	Conférence : W3C Workshop on Permissions and User Consent	https://www.w3.org/Privacy/permissions-ws-2018/cfp.html
17 janvier 2019	-	Annonce de la fermeture du *Tracking Protection Working Group*	https://lists.w3.org/Archives/Public/public-tracking/2019Jan/0000.html

Annexe 11 : Grille d’entretien des entretiens exploratoires

Les entretiens ont duré entre 30 et 120 minutes selon les cas. Dans le cas des entretiens les plus courts, une sélection a été opérée en cours d’entretien.

Sauf une exception où deux personnes ont été interrogées en même temps, chaque entretien était individuel.

En pratique, les enquêtés ont répondu à l’ensemble des questions à partir d’un nombre limité de questions posées. Au cours de l’entretien, les questions auxquelles l’enquêté avait spontanément répondu étaient cochées.

La troisième partie devait représenter au moins 50 % du temps d’entretien. Les deux premières servaient à situer le niveau d’expérience de la personne interrogée, puis ses convictions à l’égard du droit à la *protection des données à caractère personnel*.

1. Situer le niveau d'expérience lié à la protection des données

- Avez-vous déjà entendu parler de protection des données ?
  - Si oui : dans quel contexte ?
- A quoi ça sert ? Est-ce important / utile ? (en option : à quoi s'oppose la protection des données ? Ex : Sécurité – économie – ou pas ?)
- Avez-vous été victime d'abus, d'atteinte à votre vie privée / à la protection de vos données ?
- Comment votre formation vous a-t-elle conduit à travailler dans le domaine de la protection des données ? [question posée à condition que la personne travaille dans le domaine de la protection des données]
- Dans votre expérience professionnelle, avez-vous déjà été amené à traiter de problématiques relatives à la protection des données à caractère personnel ?
- Avez-vous entendu parler de l'expression « privacy community ». Si oui, considérez-vous comme faisant partie de cette communauté ?
- Avez-vous des pratiques de gestion de votre confidentialité ?

2. Questions d’ordre général

- Êtes-vous technophile ou technophobe ? (comment vous vous définissez?)
- Que pensez-vous des objets connectés ? Du Big Data ? De la réalité augmentée ? De l'informatique à l'école ? De Wikipedia ? De Facebook et des réseaux sociaux ? Est-ce que Facebook joue un rôle en faveur de la démocratie, ou pas ? L'accès à Internet : quel rôle cela joue dans le développement économique (notamment des pays en voie de développement) ?
- Est-ce que vous donneriez un ordinateur à un enfant de moins de 10 ans ? Si oui, quel type d'ordinateur, et quel type de contrôle est-ce que vous exerceriez dessus ?

- Comment garantir la protection des données ? (par le droit ? Le code ? Privacy by design / by default ? Est-ce qu'il faut responsabiliser les usagers ? Le chiffrement ? Le rapatriement des données en France / en Europe ? L'ouverture des algorithmes ?)
- A qui faites-vous confiance pour traiter vos données ? A l'Etat, aux entreprises ?
- Lisez-vous de la science fiction ? Quelle utopie, quelle dystopie selon vous ?

2. Définitions

- Avez-vous le sentiment d'une différence d'approche entre informaticiens, juristes et politiques de la question de la protection des données ? Observez-vous des évolutions à ce sujet ?

- Que recouvre le terme « protection des données » ?
  - Notion de propriété : est-on propriétaire de ses données personnelles ? Notion de vie privée ? Notion de sécurité ? Notion de droit fondamental ?

- Selon vos propres mots, pouvez-vous définir (brièvement) les termes suivants ?
  - Donnée à caractère personnel
  - A quelles données s'applique la loi de protection des données ?
  - Fichier / Traitement de données / Sous-traitement de données
    - en rapport avec la jurisprudence française à ce sujet et le débat, du coup, autour de la notion. Qu'est-ce qu'un traitement automatisé ? qu'est-ce qu'un fichier, indépendamment du caractère automatisé
  - Anonymat / Anonymisation
  - Pseudonymat
  - Transfert de données (vers des pays tiers)
  - Identifiant / Quasi-identifiant
  - Donnée sensible
  - Consentement
  - Principe de loyauté des traitements
  - Internet / Cloud computing (infonuagique) / adresse IP / Big Data
  - Cookie / fingerprinting
  - Profilage
  - Droit à l'oubli (en théorie / en pratique)

- Selon vous, ai-je oublié dans la liste des concepts importants liés à la protection des données ?
  - Certains sont-ils de trop ?

- Selon vous, comment les informaticiens s'y prennent pour protéger les données ? Ou pour y accéder ? Qu'est-ce qui les motivent ?

- Selon vous, comment s'y prend l'Etat pour contrôler le respect de la loi ? Comment peut-il faire ? Qu'est-ce qui le motive ?

Annexe 12 : Liste des décisions de la CEDH et de la CJUE étudiées

Juridiction	Date	Affaire	N° ECLI	Nom court
CEDH	06/09/1978	5026/71	-	Klass e.a. contre RFA
CEDH	02/08/1984	8691/79	-	Malone contre Royaume-Uni
CEDH	26/03/1987	9248/81	-	Leander contre Suède
CEDH	20/06/1988	11368/85	-	Schönenberger contre Suisse
CEDH	07/07/1989	10454/83	-	Gaskin contre Royaume-Uni
CEDH	25/02/1993	10828/84	-	Funke contre France
CEDH	25/02/1997	22009/93	-	Z. contre Finlande
CEDH	27/08/1997	20837/92	-	M. S. contre Suède
CEDH	16/02/2000	27798/95	-	Amann contre Suisse
CEDH	04/05/2000	28341/95	-	Rotaru contre Roumanie
CJUE/ CJCE	20/05/2003	C-465/00 , C-138/01 et C-139/01	ECLI:EU:C:2003:294	Österreichischer Rundfunk
CJUE/ CJCE	06/11/2003	C-101/01	ECLI:EU:C:2003:596	Lindqvist
CEDH	14/02/2006	57986/00	-	Turek contre Slovaquie
CEDH	06/06/2006	62332/00	-	Segerstedt-Wiberg e.a. contre Suède
CEDH	03/04/2007	62617/00	-	Copland contre Royaume-Uni
CJUE/ CJCE	29/01/2008	C-275/06	ECLI:EU:C:2008:54	Promusicae
CEDH	04/12/2008	30562/04 et 30566/04	-	S. et Marper contre Royaume-Uni
CJUE/ CJCE	16/12/2008	C-73/07	ECLI:EU:C:2008:727	Tietosuojavaltuutettu contre Satakunnan Markkinapörssi Oy et Satamedia Oy
CJUE/ CJCE	16/12/2008	C-524/06	ECLI:EU:C:2008:724	Huber contre Allemagne
CJUE/ CJCE	19/02/2009	C-557/07	ECLI:EU:C:2009:107	LSG contre Tele2
CJUE/ CJCE	07/05/2009	C-533/07	ECLI:EU:C:2009:257	Rotterdam contre Rijkeboer
CJUE/ CJCE	09/03/2010	C-518/07	ECLI:EU:C:2010:125	Commission contre Allemagne
CEDH	18/05/2010	26839/05	-	Kennedy contre Royaume-Uni
CJUE/ CJCE	29/06/2010	C-28/08	ECLI:EU:C:2010:378	Commission européenne contre Bavarian Lager
CEDH	02/09/2010	35623/05	-	Uzun contre Allemagne
CJUE/ CJCE	09/11/2010	C-92/09 et C-93/09	ECLI:EU:C:2010:662	Volker et Eifert contre Hesse
CJUE/ CJCE	05/05/2011	C-543/09	ECLI:EU:C:2011:279	Deutsche Telekom contre Allemagne

CEDH	24/05/2011	33810/07 et 18817/08	-	Association 21 décembre 1989 e.a. contre Roumanie
CJUE/ CJCE	24/11/2011	C-468/10 et C-469/10	ECLI:EU:C:2011:777	ASNEF et FECEMD contre Administracion del Estado
CJUE/ CJCE	24/11/2011	C-70/10	ECLI:EU:C:2011:771	Scarlet contre SABAM
CEDH	07/02/2012	39954/08	-	Axel Springer contre Allemagne
CEDH	14/02/2012	7094/06	-	Romet contre Pays-Bas
CJUE/ CJCE	19/04/2012	C-461/10	ECLI:EU:C:2012:219	Bonnier e.a. contre Perfect Communication Sweden
CEDH	03/07/2012	30457/06	-	Robathin contre Autriche
CJUE/ CJCE	16/10/2012	C-614/10	ECLI:EU:C:2012:631	Commission contre Autriche
CJUE/ CJCE	22/11/2012	C-119/12	ECLI:EU:C:2012:748	Josef Probst contre mr.nexnet
CJUE/ CJCE	30/05/2013	C-342/12	ECLI:EU:C:2013:355	Worten contre ACT
CJUE/ CJCE	17/10/2013	C-291/12	ECLI:EU:C:2013:670	Michael Schwarz contre Stadt Bochum
CJUE/ CJCE	07/11/2013	C-473/12	ECLI:EU:C:2013:715	IPI contre Engelbert et autres
CEDH	03/12/2013	64520/10	-	Ungváry et Irodalom Kft. contre Hongrie
CJUE/ CJCE	12/12/2013	C-486/12	ECLI:EU:C:2013:836	X contre Bois-le-Duc
CJUE/ CJCE	08/04/2014	C-288/12	ECLI:EU:C:2014:237	Commission contre Hongrie
CJUE/ CJCE	08/04/2014	C-293/12 et C-594/12	ECLI:EU:C:2014:238	Digital Rights Ireland
CJUE/ CJCE	13/05/2014	C-131/12	ECLI:EU:C:2014:317	Google contre Espagne
CJUE/ CJCE	17/07/2014	C-141/12	ECLI:EU:C:2014:2081	Y.S. contre minister voor immigratie
CJUE/ CJCE	2014.12.11	C-212/13	ECLI:EU:C:2014:2428	František Ryneš contre Úřad pro ochranu osobních údajů
CJUE/ CJCE	2015.07.16	C-615/13P	ECLI:EU:C:2015:489	ClientEarth et Pesticide Action Network Europe (PAN Europe) contre Autorité européenne de sécurité des aliments (EFSA) et Commission européenne
CJUE/ CJCE	01/10/2015	C-230/14	ECLI:EU:C:2015:639	Weltimmo
CJUE/ CJCE	01/10/2015	C-201/14	ECLI:EU:C:2015:638	Bara e. a.
CJUE/ CJCE	06/10/2015	C-362/14	ECLI:EU:C:2015:650	Schrems contre DPC Irlande

CEDH	04/12/2015	47143/06	-	Zakharov contre Russie
CEDH	12/01/2016	37138/14	-	Szabó et Vissy contre Hongrie
CEDH	12/01/2016	61496/08	-	Barbulescu contre Roumanie
CEDH	31/03/2016	34148/07	-	Šantare et Labaņikovs contre Lettonie
CJUE/ CJCE	28/07/2016	C-191/15	ECLI:EU:C:2016:612	Verein für Konsumenteninformation contre Amazon EU Sàrl (VKI contre Amazon UE)
CJUE/ CJCE	19/10/2016	C-582/14	ECLI:EU:C:2016:779	Patrick Breyer contre République fédérale d'Allemagne
CJUE/ CJCE	21/12/2016	C-203/15 et C-698/15	ECLI:EU:C:2016:970	Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson, Peter Brice et Geoffrey Lewis
CJUE/ CJCE	09/03/2017	C-398/15	ECLI:EU:C:2017:197	Camera di Commercio contre Salvatore Manni
CJUE/ CJCE	04/05/2017	C-13/16	ECLI:EU:C:2017:336	Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contre Rīgas pašvaldības SIA « Rīgas satiksme »
CEDH	05/09/2017	61496/08	-	Barbulescu contre Roumanie
CJUE	27/09/2017	C-73/16	ECLI:EU:C:2017:725	Peter Puškár contre Finančné riaditeľstvo Slovenskej republiky et Kriminálny úrad finančnej správy
CJUE	20/12/2017	C-434/16	ECLI:EU:C:2017:994	Peter Nowak contre Data Protection Commissioner
CEDH	22/02/2018	588/13	-	Libert contre France
CJUE	05/06/2018	C-210/16	ECLI:EU:C:2018:388	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH
CJUE	10/07/2018	C-25/17	ECLI:EU:C:2018:551	Jehovan todistajat – uskonnollinen yhdyskunta
CEDH	13/09/2018	62322/14 et 24960/15	-	Big Brother Watch et autres contre Royaume-Uni
CJUE	02/10/2018	C-207/16	ECLI:EU:C:2018:78	Ministerio Fiscal

			8	
CJUE	14/02/2019	C-345/17	ECLI:EU:C:2019:122	Sergejs Buivids

Annexe 13 : Évolution des « principes » de la protection des données, des propositions de la *British Computer Society* à la Résolution (73) 22 du Conseil de l'Europe

L'anglais est la seule langue commune à l'ensemble des documents dont sont extraites les citations ci-dessous. C'est pourquoi cette langue a été choisie pour analyser l'évolution de la rédaction des « principes » de la protection des données.

Submission made by the British Computer Society[1]	**Younger Report's principles**[2]	**Proposals made by the British delegation in 1972 (EXP/Prot.Priv./ EDB (72) 5 REV)**	**HEW Report**	**Principles in the 1973 (22) Council of Europe Resolution**
1. Personal information, whether of an individual, group or institution, should be defined as a right belonging to that person, and interference by public or private bodies with this right should be restricted by law.				
3. In particular, data in which individual identity is recognisable should be restricted in use to the purpose for	1. Information should be regarded as held for a specific purpose and not to be used, without	Principle 1 The information should be regarded as having been provided for a	#3 : There must be a way for an individual to prevent information about him that was	2. The information should be appropriate and relevant with regard to the purpose for which

1 Extraits des pages 22 à 25 du rapport de la *British Computer Society* (1971), qui comptait une liste numérotée de recommandations

2 Extrait des pages 183 et 184 du rapport du Comité Younger pp. 183-184 du rapport Younger (cité par Bennett, 1992, p. 98 - 99)

which it was collected unless there is specific authority from the individual concerned. Thus, for example, it could become a requirement that the purpose for the collection of data be stated on the form used for its collection and it would then be an offence to use it for any other purpose without express authority.	appropriate authorization, for other purposes.	specific purpose, and without appropriate autorisation it should not be used for other purposes, or communicated to third parties without the agreement of the person concerned.	obtained for one purpose from being used or made available for other purposes without his consent	it has been stored 5. Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.
	2. Access to information should be confined to those authorized to have it for the pruposes for which it was supplied.	Principle 2 Access to the information stored should be confined to persons who can establish a valid reason in obtaing the information	#5 : Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data	9. Access to the information stored should be confined to persons who have a valid reason to know it. The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy
Voir : #3	3. The amount of information collected and held should be the minimum necessary for the achievement of a specified purpose.	Principle 3 Information should not be stored if it is irrelevant or to an amount excessive according to the	*Voir* : #5	See 2.

		given purpose.		
	4. In computerised systems handling information for statistical purposes, adequate provisions should be made in their design and programs for separating identities from the rest of the data.	Principle 4 Statistical data may only be published in aggregate form and under conditions which will make it impossible to reconstitute information so as to permit the identification of individuals.		10. Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person.
(see #4, which did not provide for general information, but did provide for a right to access the data)	5. There should be arrangements whereby the subject could be told about the information held concerning them.	Principle 5 Measures should be taken in order to inform the person concerned of the nature of the information held about him, and if possible of the purposes for which the information will be used.	#1 : There must be no personal data record-keeping systems whose very existence is secret ; #2 : There must be a way for an individual to find out what information about him is in a record and how it used	6. As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.
4. […] Any installation holding sensitive data which is made available to third parties, particularly over remote terminals, must have proper means of limiting	6. The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse	Principle 6 The level of security to be achieved by a system should be spelled out in advance and should include precautions against deliberate		8. Precautions should be taken against any abuse or misuse of information. Electronic data banks should be equipped with security systems which bar access

access to files by such third parties to those authorised and of detecting attempts to make unauthorised changes to the contents of files. […]	of misuse of information.	abuse or misuse of information.		to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirections of information, whether intentional or not.
	7. A monitoring system should be provided to facilitate the detection of any violation of the security system.	Principle 7 Facilities should be provided for detecting as well as for preventing violation of the security systems.		
	8. In the design of information systems, periods should be specified beyond which the information should be not be retained.	Principle 8 In the design of information systems, periods should be specified beyond which information should no longer be kept and used.		4. Rules should be laid down to specify the periods beyond which certain categories of information should no longer be kept or used
	9. Data held should be accurate. There should be machinary for the correction of inaccuracy and the updating of information.	Principle 9 The information should be lawful, accurate and not obsolete. All reasonable steps should be taken in order to correct wrong information and to keep the information up to date.	#4 : There must be a way for an individual to correct or amend a record of identifiable information about him	1. The information stored should be accurate and should be kept up to date. […] 7. Every care should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way.
2. The use or circulation of personal information whether of an individual, group or institution by				

someone other than the owner should impose special duties and liabilities on the persons or organisations handling it.				
4. A person or his professional advisors should generally have the right to examine the data contained in files in which his personal identity is retained, at a reasonable fee, to question the source, to know by whom it can legitimately be accessed, to challenge its accuracy and relevance and to submit a reply or explanation, the existence of which would be noted in his data file. This right would no doubt need to be modified, for example, where criminal investigation by the police of national security are concerned, or where confidential, medical and other professional opinions are			*Voir* : #4	

recorded in a file, but should apply as widely as possible. An administrative process, subject to court review, would probably be desirable to deal with questions on sources of data and challenges regarding accuracy. […]				
4. […] Infringements of the personal privacy rights defined above should be criminal offences with compensation associated where relevant. Penalties for each infringement should be greater than the estimated extra cost of incorporating adequate additional safeguards into the filing system.				
5. A licensing system should be considered both for owners of banks of "sensitive" data (declared to be so by due administrative process), and for				

professionals engaged in their operation and construction. The object of this system would be to ensure the incorporation of proper privacy safeguards in data banks. It could also serve the raise technical standards in other respects. The Society sees the need for the development of professional standards among practitioners and intends to follow the example of other professional bodies, such as the engineering, scientific and accounting societies.				
6. The creation should be considered of a group (or groups) within the machinery of the State with the following specific responsibilities with respect to the privacy of individuals: i) Have a watchdog role over developments both here and abroad which				

represent intrusion into privacy, collect evidence of problems, and propose legislation as required. ii) Police the legislation covered in paragraphs 3, 4 and 5, and initiate change as is considered necessary. iii) Promote and direct basic research into the nature of privacy aimed at improving the type of safeguards that provide protection to the individual without stifling innovations. iv) Undertake educational activities to reduce the gap between fact and fantasy in the minds of the public in this area. It is envisaged that this group would act with respect to privacy in a manner similar to that in the Department of Trade & Industry with regard to company law or,				

perhaps, that an independent body like the Air Registration Board would be set up. Whilst action against infringement of the proposed law would, as for financial fraud, be the concern of the Police, a watchdogfunction would be carried out by licensed professionals, who would be at once the main source of evidence of potential infringements and the principal protection against any attempt to exploit them »				
	10. Care should be taken in coding value judgements			
				1. […] In general, information relating to the intimate life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.
				3. The information

				should not be obtained by fraudulent or unfair means

Annexe 14 : Structure du questionnaire exploratoire en ligne

Export réalisé à partir du logiciel Limesurvey, sur lequel étaient basés les sites web dataprotectionsurvey.eu *et* enqueteprotectiondesdonnees.eu.

Données démographiques

Quelques questions pour mieux cerner qui vous êtes et d'où vous venez

Quelle est votre année de naissance ? *

Votre réponse doit être comprise entre 1900 et 2017

Seul un nombre entier peut être inscrit dans ce champ.

Veuillez écrire votre réponse ici :

•

Vous pouvez indiquer votre adresse e-mail si vous souhaitez recevoir un exemplaire des résultats de recherche et que vous acceptez, le cas échéant, d'être contacté dans le cadre de la présente enquête.

Veuillez écrire votre réponse ici :

Répondre à cette question seulement si les conditions suivantes sont réunies :
La réponse n'était pas à la question '2 [emailaddress]' (Vous pouvez indiquer votre adresse e-mail si vous souhaitez recevoir un exemplaire des résultats de recherche et que vous acceptez, le cas échéant, d'être contacté dans le cadre de la présente enquête.)

Choisissez la réponse appropriée pour chaque élément :

	Oui	Incertain	Non
Je souhaite recevoir un exemplaire électronique du rapport statistique de cette enquête	○	○	○
Je souhaite recevoir un exemplaire des résultats finaux du projet de recherche de thèse dont la présente enquête fait partie	○	○	○
J'accepte d'être contacté(e) dans le cadre de cette enquête pour des questions supplémentaires et/ou pour une interview	○	○	○

Êtes-vous un homme ou une femme ? [1]

1 La réponse « autre » n'étant pas proposée par le logiciel Limesurvey, nous avons fait le choix de rendre cette question optionnelle.

Veuillez sélectionner une seule des propositions suivantes :

- ○ Féminin
- ○ Masculin

Quel est votre parcours de formation? *

Veuillez sélectionner une réponse ci-dessous

Au besoin, veuillez préciser le champ ‘Autre :’.

Veuillez sélectionner une seule des propositions suivantes :

- ○ Droit
- ○ Informatique
- ○ Autre

Dans quel pays vivez-vous ?

Veuillez sélectionner une réponse ci-dessous

Veuillez sélectionner une seule des propositions suivantes :

[Liste de pays]

Avez-vous déjà rempli l'une ou plusieurs des fonctions suivantes ? *

Cochez la ou les réponses

Veuillez choisir toutes les réponses qui conviennent :

- ☐ Dirigeant(e) d'une organisation (entreprise, association, établissement public ...)
- ☐ Employé(e) ou membre d'une autorité de protection des données
- ☐ Correspondant(e) informatique et libertés (CIL) ou délégué(e) à la protection des données (DPO)
- ☐ DSI ou responsable informatique
- ☐ Elu(e) politique
- ☐ Employé(e) d'un service juridique ou avocat(e) (secteur privé)
- ☐ Responsable de la sécurité des systèmes d'information (RSSI)
- ☐ Syndicaliste
- ☐ Je ne souhaite pas renseigner ces informations
- ☐ J'ai travaillé dans le secteur de la sécurité publique (police, armée, renseignement, et toute autre autorité en charge de sécurité publique)
- ☐ J'ai travaillé dans le secteur de la justice (secteur public)
- ☐ J'ai pris part dans des travaux de standardisation technique ou des organisations qui s'en occupent (ISO, IETF, IEEE, W3C...)

- ☐ **Je n'ai jamais rempli une ou plusieurs des fonctions ci-dessus**

A quelle organisation de normalisation technique avez-vous participé?

Répondre à cette question seulement si les conditions suivantes sont réunies :
La réponse était à la question '7 [prodpexp]' (Avez-vous déjà rempli l'une ou plusieurs des fonctions suivantes ?)

Cochez la ou les réponses

Veuillez choisir toutes les réponses qui conviennent :

- ☐ ISO
- ☐ IETF
- ☐ IEEE
- ☐ W3C
- ☐ ICANN
- ☐Autre:

Quel est votre emploi actuel ?

	Titre de votre fonction	Employeur
Votre emploi		

Protection des données

Pouvez-vous décrire brièvement, dans vos propres mots, ce que signifie le terme de "protection des données" ?

Veuillez écrire votre réponse ici :

Selon votre expérience, existe-t-il une différence d'approche entre juristes et informaticiens en matière de protection des données ?

Répondre à cette question seulement si les conditions suivantes sont réunies :

-------- Scenario 1 --------

La réponse était à la question '7 [prodpexp]' (Avez-vous déjà rempli l'une ou plusieurs des fonctions suivantes ?)

-------- ou Scenario 2 --------

La réponse était à la question '7 [prodpexp]' (Avez-vous déjà rempli l'une ou plusieurs des fonctions suivantes ?)

-------- ou Scenario 3 --------

La réponse était à la question '7 [prodpexp]' (Avez-vous déjà rempli l'une ou plusieurs des fonctions suivantes ?)

Veuillez sélectionner une seule des propositions suivantes :

- ○ Oui
- ○ Non

Pouvez-vous décrire la nature de cette différence d'approche ?

Répondre à cette question seulement si les conditions suivantes sont réunies :
La réponse était 'Oui' à la question '11 [lawitdiff]' (Selon votre expérience, existe-t-il une différence d'approche entre juristes et informaticiens en matière de protection des données ?)

Veuillez écrire votre réponse ici :

Définitions

Comment définieriez-vous les termes suivants ?

L'objectif de cette section est de cartographier et de comprendre de quelles manières certains termes relatifs au droit de la protection des données peuvent être interprétés.

Que recouvre le terme juridique de "donnée à caractère personnel" ?

Choisissez la réponse appropriée pour chaque élément :

	Oui	Incertain	Non
Seulement les informations relatives à la vie privée, à l'intimité, d'un individu	○	○	○
Cela recouvre toutes les informations sur une personne, qu'elles soient de nature sensible ou pas	○	○	○
Cela ne recouvre que les données relatives à des êtres humains, et exclut donc les personnes morales (entreprises, associations, etc.)	○	○	○
Une donnée est nominative, c'est-à-dire, personnelle si et seulement si elle contient le nom de la personne	○	○	○
Une donnée est personnelle même s'il n'y a que des moyens indirects de retrouver la personne à son origine, par exemple par croisement avec d'autres données	○	○	○
Pour qu’une donnée soit considérée personnelle et protégée par la loi, il	○	○	○

	Oui	Incertain	Non
faut que la personne qui la détient soit capable de retrouver seul la personne à l'origine de ces données, il ne suffit pas que cela soit possible dans l'absolu par quelqu'un d'autre			
Une donnée personnelle est nominative. Remplacer le nom par un pseudonyme ou un numéro aléatoire fait qu'elle n'est plus personnelle	○	○	○
Un email est une donnée personnelle même s'il ne contient pas le nom de la personne concernée	○	○	○
Un numéro de téléphone et une conversation téléphonique sont des données personnelles même si le contenu de la conversation n'est pas enregistré	○	○	○
Une information disponible publiquement sur quelqu'un (par exemple dans la presse, ou sur Twitter) n'est pas une donnée à caractère personnelle	○	○	○
La photo de quelqu'un est toujours une donnée à caractère personnel	○	○	○

Qu'est-ce qu'un traitement de données ?

Veuillez écrire votre réponse ici :

Selon le Règlement général de protection des données : "Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier". Ce terme est défini dans le Règlement, mais dans la pratique et sur le terrain, il connaît plusieurs acceptions et interprétations que nous cherchons ici à cartographier.

Le Règlement général de protection des données ne s'applique qu'aux "traitements automatisés en tout ou en partie" et aux données personnelles ayant vocation à figurer dans un fichier structuré.

Un traitement informatisé (en tout ou partie) est-il nécessairement un traitement automatisé (en tout ou partie) ?

Veuillez sélectionner une seule des propositions suivantes :

- ○ Oui
- ○ Non

Si vous le souhaitez, vous pouvez expliquer pourquoi vous avez choisi cette réponse dans le champ ci-dessous :

Répondre à cette question seulement si les conditions suivantes sont réunies :
La réponse était 'Non' à la question '15 [automaticprocessing]' (Le Règlement général de

protection des données ne s'applique qu'aux "traitements automatisés en tout ou en partie" et aux données personnelles ayant vocation à figurer dans un fichier structuré. Un traitement informatisé (en tout ou partie) est-il nécessairement un traitement automatisé (en tout ou partie) ?)

Veuillez écrire votre réponse ici :

Que veut dire "transfert de données" ?

Cochez la ou les réponses

Veuillez choisir toutes les réponses qui conviennent :

- ☐ L'accès aux données par un tiers
- ☐ L'accès à des données à distance (avec ou sans copie de ces données)
- ☐ La copie d'une donnée d'un lieu A vers un lieu B
- ☐ L'acte de vendre ou de partager des données personnelles
- ☐ L'acte de partager des données spécifiquement avec des agences de renseignement
- ☐ Autre:

Est-ce que le droit à la vie privée et le droit à la protection des données personnelles sont pour vous la même chose ?

Veuillez sélectionner une seule des propositions suivantes :

- ○ Oui
- ○ Non

Quelle est selon vos propres mots la différence entre le droit à la vie privée et le droit à la protection des données personnelles ?

Répondre à cette question seulement si les conditions suivantes sont réunies :
La réponse était 'Non' à la question '18 [isdpprivacy]' (Est-ce que le droit à la vie privée et le droit à la protection des données personnelles sont pour vous la même chose ?)

Veuillez écrire votre réponse ici :

Questions générales sur la protection des données

A quel point est-ce que la protection des données est-elle importante pour vous ?

(1 étoile : très peu importante ; 5 étoiles : indispensable)

Veuillez sélectionner une seule des propositions suivantes :

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

Quelle importance accordez-vous à la protection de la vie privée ?

Veuillez sélectionner une seule des propositions suivantes :

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

Vous avez un espace ci-dessous si vous souhaitez donner plus de détails sur les raisons qui vous amènent à conclure soit à l'importance, soit à l'absence d'importance de protéger la vie privée :

Veuillez écrire votre réponse ici :

Quel degré d'effort êtes-vous prêt(e) à investir dans la protection des données personnelles ?

Veuillez sélectionner une seule des propositions suivantes :

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

Où avez-vous entendu parler pour la première fois de protection des données ?

Veuillez sélectionner une réponse ci-dessous

Veuillez sélectionner une seule des propositions suivantes :

- ○ Cette enquête est la première fois que j'entends parler de protection des données
- ○ J'en ai entendu parler par les médias
- ○ J'en ai entendu parler au travail
- ○ J'en ai entendu parler pendant ma formation
- ○ J'en ai entendu parler pour la première fois lorsqu'un site Internet m'a demandé de paramétrer des paramètres de confidentialité et/ou en lisant la politique de confidentialité d'un site Internet

- ○ J'en ai entendu parler par des ami.e.s
- ○ J'en ai entendu parler en milieu associatif ou syndical
- ○ Autre

Faites le commentaire de votre choix ici :

Vous pouvez rajouter plus de précisions (ex : nom de la revue dans laquelle vous avez lu un article sur le sujet, date ...) en commentaire

Avez-vous déjà eu des expériences relatives à la protection des données?

Veuillez sélectionner une seule des propositions suivantes :

- ○ Oui
- ○ Non

Par exemple : vous avez travaillé sur des éléments en rapport avec la protection des données, ou vous avez été en contact avec la CNIL pour protéger vos propres données, etc.

Comment avez-vous eu cette expérience relative à la protection des données ?

Vous pouvez utiliser les champs de commentaire sur la droite pour compléter l'information

Répondre à cette question seulement si les conditions suivantes sont réunies :
La réponse était 'Oui' à la question '25 [experience]' (Avez-vous déjà eu des expériences relatives à la protection des données?)

Ajoutez un commentaire seulement si vous sélectionnez la réponse.

Veuillez choisir toutes les réponses qui conviennent et laissez un commentaire :

- ☐ J'ai déjà été victime de fraude, d'un délit ou plus généralement d'un abus relatif à mes données personnelles
- ☐ J'ai déjà été obligé de protéger de façon active ma vie privée de quelqu'un, par exemple de mon patron
- ☐ J'ai déjà été en charge, au travail, de tâches en rapport avec la protection des données, comme la mise en conformité de nos activités avec la loi Informatique et Libertés
- ☐ J'ai déjà dû me tourner vers la CNIL (ou, selon les pays, une autre autorité de protection des données)
- ☐ J'ai reçu une formation ou ai assisté à une conférence sur le sujet

- Autre :

Qui représente selon vous le plus grand danger pour la protection des données ?

Veuillez sélectionner une réponse ci-dessous

Veuillez sélectionner une seule des propositions suivantes :

- ○ L'Etat
- ○ Les entreprises
- ○ Les consommateurs
- ○ L'Etat comme les entreprises
- ○ Les entreprises comme les consommateurs
- ○ L'Etat comme les consommateurs

Notez les phrases suivantes en fonction du degré auquel vous êtes d'accord avec elles

Choisissez la réponse appropriée pour chaque élément :

	1	2	3	4	5
La protection des données personnelles entre en contradiction avec la sécurité publique, la lutte contre le terrorisme et contre la criminalité	○	○	○	○	○
Les règles de protection des données personnelles sont un fardeau pour les entreprises	○	○	○	○	○
Les règles de protection des données personnelles ralentissent la croissance et l'innovation, qui sont de bonnes choses	○	○	○	○	○
La protection des données personnelles aboutit à cacher des informations du marché, ce qui crée des situations de concurrence déloyale (par exemple sur le marché du travail)	○	○	○	○	○

1 pour dire "pas du tout", 3 pour exprimer un point de vue neutre et 5 pour dire "oui tout à fait !"

Selon vous, d'où viendra la solution pour protéger efficacement les données personnelles ?

Vous pouvez noter les propositions suivantes en fonction du degré de crédibilité

Choisissez la réponse appropriée pour chaque élément :

	1	2	3	4	5
La solution viendra du marché	○	○	○	○	○
La solution viendra de la Loi et des autorités publiques	○	○	○	○	○

	1	2	3	4	5
La solution viendra des évolutions techniques	○	○	○	○	○
La solution viendra du développement de normes techniques comme celles de l'ISO, de l'IETF ou du W3C (par exemple le W3C développe les normes techniques sur lesquelles est basé le Web)	○	○	○	○	○
Il n'y a pas besoin de solution car la technologie ne met pas la vie privée en danger	○	○	○	○	○
Trouver une solution au problème de la vie privée est moins important que de soutenir l'innovation technique, car in fine, les progrès technologiques nous apportent plus de bien que de mal	○	○	○	○	○
La solution, c'est de consommer moins de technologie et d'utiliser moins d'appareils informatiques	○	○	○	○	○
La solution repose sur l'emploi de techniques d'anonymisation	○	○	○	○	○

1 pour dire "pas du tout", 3 pour exprimer un point de vue neutre et 5 pour dire "oui tout à fait !"

Quelles sont les trois bonnes pratiques les plus importantes à adopter lorsqu'on collecte et/ou traite des données à caractère personnel ?

Cochez la ou les réponses

Veuillez sélectionner 3 réponses maximum

Veuillez choisir toutes les réponses qui conviennent :

- ☐ Demander l'autorisation de la personne pour collecter ses données
- ☐ Informer les personnes de ce qui est fait de leurs données
- ☐ Ne pas collecter plus que ce qui est nécessaire à l'objectif dans lequel les données ont été collectées, ce qui implique de déterminer cet objectif en amont
- ☐ Mettre en œuvre les mesures de sécurité informatique approprié eu égard à l'état des menaces contre la confidentialité de ces données
- ☐ Faire en sorte que les données soient à jour et correctes
- ☐ Donner un droit d'accès aux personnes dont les données sont collectées / traitées
- ☐ Autre (veuillez préciser)
- ☐ Rémunérer les personnes dont vous monétisez les données

Le nombre de réponses a été volontairement limité à trois pour permettre la comparaison entre ce que différents groupes de répondants considèrent comme étant les pratiques les plus importantes à adopter

Presque fini ...

Merci d'avoir répondu au questionnaire jusqu'ici !

Nous avons presque terminé. La dernière série de questions, ci-dessous, a pour objectif de compléter les séries de questions précédentes en les insérant dans un contexte sociopolitique d'une part et technique d'autre part plus large.

Avez-vous déjà entendu parler de la "privacy community" ?

Veuillez sélectionner une seule des propositions suivantes :

- ○ Oui
- ○ Non

Diriez-vous que vous en faites partie ?

Répondre à cette question seulement si les conditions suivantes sont réunies :
La réponse était 'Oui' à la question '31 [privacycommunity]' (Avez-vous déjà entendu parler de la "privacy community" ?)

Veuillez sélectionner une seule des propositions suivantes :

- ○ Oui
- ○ Non

Êtes-vous d'accord avec les phrases suivantes ?

Choisissez la réponse appropriée pour chaque élément :

	Oui	Incertain	Non
Internet est ingouvernable	○	○	○
Le droit a toujours un temps de retard sur la technologie	○	○	○
Le droit est parfaitement en mesure de réguler l'Internet	○	○	○
Le big data va permettre de trouver un remède au cancer	○	○	○
Les objets connectés m'offrent des mesures utiles à mon développement et à mon autonomie personnelles	○	○	○
La technologie va rendre l'être humain meilleur, il ne faut donc pas en entraver le progrès	○	○	○
Le droit des données personnelles est tellement complexe et si peu utile que je ne l'appliquerai que si je suis contrôlé	○	○	○
Nous devrions être propriétaires de nos données personnelles et ainsi obtenir une rémunération en l'échange de leur exploitation	○	○	○
Les données personnelles sont ou devraient être un bien commun	○	○	○
Il faut rendre accessibles et transparents les codes sources des logiciels dans le but de mieux protéger notre vie privée	○	○	○
Une communauté a le droit de savoir des choses sur ses membres pour se	○	○	○

	Oui	Incertain	Non
protéger (par exemple : un quartier sur ses riverains potentiellement dangereux, comme un ancien criminel sorti de prison)			
Le droit à l'oubli est contraire à la liberté d'expression	○	○	○
Est-ce que vous donneriez un smartphone à votre enfant de dix ans ?	○	○	○
Je n'ai à rien à cacher, donc je n'ai pas besoin de protection des données	○	○	○
J'accepte que l'on collecte mes données si elles sont anonymisées	○	○	○
La vie privée sert à cacher des modes de vie minoritaires et les violences de la sphère domestique	○	○	○
La protection des données personnelles aide les criminels à se cacher	○	○	○
Il est légitime de collecter des données de santé contre la volonté des personnes lorsqu'il s'agit de suivre la progression d'une épidémie comme le SIDA ou Ebola	○	○	○
Protéger les données personnelles est nécessaire pour protéger l'autonomie individuelle	○	○	○
Il ne peut pas y avoir de poursuite du bonheur sans autonomie individuelle	○	○	○
Certaines entreprises génèrent du profit illégitime à partir de l'exploitation des données personnelles que nous produisons car elles ne nous rémunèrent pas pour ce travail que nous effectuons	○	○	○
Le Big Data c'est comme Big Brother	○	○	○
Le stockage de mes données personnelles à l'étranger nuit à la souveraineté de mon pays	○	○	○

Les phrases suivantes ne reflètent pas l'opinion des concepteurs du présent projet de recherche, mais ont été extraites de la littérature existante sur la protection des données et de la vie privée, ainsi que d'entretiens qualitatifs réalisés préalablement à l'élaboration du questionnaire.

Lisez-vous, ou regardez-vous de la science fiction ?

Veuillez sélectionner une seule des propositions suivantes :

- ○ Oui
- ○ Non

Pouvez-vous donner des exemples d'œuvres de science fiction qui vous inspirent, que vous souhaitez voir se réaliser à l'avenir ?

Répondre à cette question seulement si les conditions suivantes sont réunies :
La réponse était 'Oui' à la question '34 [scienfiction]' (Lisez-vous, ou regardez-vous de la science fiction ?)

Pouvez-vous donner des exemples d'œuvres de science fiction qui vous effraient et dont vous ne souhaitez pas la réalisation ?

Répondre à cette question seulement si les conditions suivantes sont réunies :
La réponse était 'Oui' à la question '34 [scienfiction]' (Lisez-vous, ou regardez-vous de la science fiction ?)

Si vous le souhaitez, le champ ci-dessous vous permet de rajouter vos commentaires :

Vous pouvez ajouter vos éventuels commentaires et questions ci-dessous

Annexe 15 : Éléments biographiques sur les personnes interrogées en entretien

Les tableaux ci-dessous contiennent un résumé d'éléments biographiques sur les personnes interrogées en entretien qui permettent de comprendre les raisons qui nous ont conduit à les interroger.

Les personnes ayant requis l'anonymat en sont exclues.

Seules des informations succinctes et strictement pertinentes au regard de l'étude menée sont indiquées.

Les personnes dont la biographie n'est pas publiquement et facilement accessible ont été exclues de ces tableaux.

Entretiens sur l'Histoire de la protection des données

	Nom	Prénom	Éléments biographiques
HIST1	Hustinx	Peter	Peter Hustinx a fait partie dès le début des années 1970 du groupe d'experts du Conseil de l'Europe qui a rédigé la Convention 108. Il a présidé l'autorité néerlandaise de protection des données à partir de 1991, puis présidé le G29 avant d'être désigné Contrôleur européen de la protection des données en 2004.
HIST2	Simitis	Spiros	Spiros Simitis est un professeur de droit qui a travaillé sur la rédaction de la première loi de « protection des données » du monde, adoptée en 1970 par le Land de Hesse. Il a ensuite joué un rôle important dans la structuration du réseau transnational des autorités de protection des données.
HIST3	Kirby	Michael	Michael Kirby est un juriste australien qui a présidé, entre 1978 et 1980, le groupe d'experts de l'OCDE ayant rédigé les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.
HIST4	Frank	Alice	Alice Frank a été secrétaire du groupe d'experts de l'OCDE ayant rédigé, entre 1978 et 1980, les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.
HIST5	Delahaie	Henri	Henri Delahaie est consultant en protection des données depuis le début des années 1980. Il a été co-auteur avec Félix Paoletti d'un

			ouvrage intitulé *Informatique et libertés*, publié aux éditions de la Découverte en 1987.
HIST6	Sólyom	László	László Sólyom est un professeur de droit à la retraite, qui a publié, dès les années 1980, des articles sur la protection des données inspirés notamment des travaux de Spiros Simitis. Premier président de la Cour constitutionnelle hongroise après la chute du régime communiste, il prit une part importante dans la décision 15/1991/AB qui posa les bases du droit hongrois *de la* protection des données.
HIST7	Corell	Hans	Hans Corell a été membre des délégations suédoises aux groupes d'experts de l'OCDE et du Conseil de l'Europe ayant respectivement rédigé les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel et la Convention 108.
HIST8	Vitalis	André	André Vitalis a publié une thèse publiée en 1981 sous le titre *Informatique, pouvoir et libertés* aux éditions Economica. Il a également été consultant pour la CNIL et a, à ce titre, côtoyé et travaillé avec certains fondateurs de cette institution.
HIST9	Georges	Marie	Marie Georges a joué un rôle important dans la création de la CNIL puis dans la négociation de la directive 95/46/CE.

Entretiens sur l'adoption du RGPD

	Nom	**Prénom**	**Éléments biographiques**
Euro2	Walko-wiak	Anna	Employée de la Fundacja Panoptykon (ONG polonaise membre d'EDRi) au moment de l'entretien
Euro3	Hötzen-dorfer	Walter	Chercheur et consultant à l'AT Research Institute (entreprise) et membre d'Epicenter Works (ONG) au moment de l'entretien
Euro4	Antemir	Razvan	Ancien employé de la FEDMA et employé d'Emota, des groupes d'intérêt industriels européens, au moment de l'entretien
Euro6	Jeppesen	Jens-Henrik	Directeur-général de CDT Europe au moment de l'entretien
Euro7	Blanco	Laura	Employée de CDT Europe au moment de l'entretien
Euro8	McNa-mee	Joe	Directeur exécutif d'EDRi pendant les négociations sur le RGPD et au moment de l'entretien.
Euro9	Kallas	Kaja	Députée européenne libérale au moment de l'entretien. Élue en 2014, rapporteuse du projet de règlement e-Privacy à la

			commission de l'Industrie, de la recherche et de l'énergie du Parlement européen.
Euro10	Maurel	Lionel	Membre de l'ONG française *La Quadrature du Net* au moment de l'entretien.

Entretiens sur le *Privacy Interest Group* et le *Tracking Protection Working Group* du W3C

	Nom	**Prénom**	**Éléments biographiques**
W3C2	Rice	Simon	*Technology Group Manager* de l'ICO, l'autorité britannique de protection des données, au moment de l'entretien. Membre du *Privacy Interest Group*.
W3C3	Hall	Joseph	*Chief Technologist* de CDT, membre du *Privacy Interest Group* et du *Tracking Protection Working Group*.
W3C4	Toubiana	Vincent	Employé de la CNIL au moment de l'entretien. Membre du *Tracking Protection Working Group*.
W3C6	Stamm	Sid	Sid Stamm, ingénieur chez Mozilla et chercheur en informatique, a été l'un des principaux promoteurs du projet Do Not Track et a participé activement à la liste de discussion *public-tracking*.
W3C7	Olejnik	Lukasz	Docteur de l'INRIA, consultant indépendant, et expert invité du *Privacy Interest Group*. Élu membre du *Technical Architecture Group* du W3C en 2018.
W3C8	Wenning	Rigo	Juriste employé par l'*European Research Consortium for Informatics and Mathematics*, l'une des universités formant le consortium du W3C. Il fait partie de l'équipe du W3C, et participé à ce titre, depuis 1999, aux travaux du projet P3P, du *Tracking Protection Working Group* et du *Privacy Interest Group*.
W3C9	Dawson	Frank	Ingénieur travaillant pour la compagnie Nokia, membre du *Privacy Interest Group*, et auteur du document *Specification Privacy Assessment* (W3C SPA).