Le consentement dans le Règlement européen sur la protection des données (RGPD)

Katia Bouslimani

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ GRENOBLE ALPES

École doctorale : EDSJ - Ecole Doctorale Sciences Juridiques
Spécialité : Droit International
Unité de recherche : Centre d'Etudes sur la Sécurité Internationale et les Coopérations Européennes

Le consentement dans le Règlement européen sur la protection des données (RGPD)

Consent in the General Regulation for Data Protection (GDPR)

Présentée par :

Katia BOUSLIMANI

Direction de thèse :

Karine BANNELIER-CHRISTAKIS MAITRE DE CONFERENCES, Université Grenoble Alpes	Directrice de thèse
Théodore CHRISTAKIS PROFESSEUR DES UNIVERSITES, Université Grenoble Alpes	Co-directeur de thèse

Rapporteurs :

Brunessen BERTRAND
PROFESSEUR DES UNIVERSITES, Université Rennes 1
Gloria GONZÁLEZ FUSTER
PROFESSEUR, Vrije Universiteit Brussel

Thèse soutenue publiquement le **16 décembre 2022**, devant le jury composé de :

Karine BANNELIER-CHRISTAKIS MAITRE DE CONFERENCES HDR, Université Grenoble Alpes	Directrice de thèse
Théodore CHRISTAKIS PROFESSEUR DES UNIVERSITES, Université Grenoble Alpes	Co-directeur de thèse
Brunessen BERTRAND PROFESSEUR DES UNIVERSITES, Université Rennes 1	Rapporteure
Gloria GONZÁLEZ FUSTER PROFESSEUR, Vrije Universiteit Brussel	Rapporteure
Célia ZOLYNSKI PROFESSEUR DES UNIVERSITES, Université Paris 1 Panthéon Sorbonne	Examinatrice
Peter SWIRE PROFESSEUR, Georgia Tech Scheller College of Business	Examinateur
Jean-Michel BRUGUIÈRE PROFESSEUR DES UNIVERSITES, Université Grenoble Alpes	Président

Remerciements

Si la thèse peut paraître solitaire (est l'est parfois), j'ai eu la chance d'être entourée de personnes qui ont enrichi mes années de recherches de soutien, de conseils, mais également de rires et de joie. Ce sont ces personnes que je tiens à remercier très sincèrement.

J'adresse mes remerciements chaleureux à des directeurs de thèse, Madame Karine BANNELIER et Monsieur le Professeur Théodore CHRISTAKIS, pour leur confiance, leur amitié, les opportunités qu'ils m'ont créées et leur soutien.

Je remercie les membres du jury que sont Mesdames les professeures Brunessen BERTRAND, Gloria GONZÁLEZ FUSTER et Célia ZOLYNSKI ainsi que Messieurs les professeurs Jean-Michel BRUGUIÈRE et Peter SWIRE.

Je remercie l'ensemble des professionnels, maîtres de conférences et professeurs rencontrés lors du déroulé de la thèse qui ont pris le temps de me conseiller et de m'aiguiller lors de mes travaux.

Je remercie également mes relecteurs, qui ont pris le temps de me lire et dont les conseils m'ont été très précieux : Alex, Alexandre, Arnaud, Claire, François-Xavier, Islam, Julien et Stanislas.

S'ils sont trop nombreux pour être cités, je tiens à remercier l'ensemble des personnes qui m'ont accompagnée durant la thèse, et sans qui ces années auraient été bien plus calmes : mes amis, mes collègues, mes rencontres.

Enfin, je tiens à remercier affectueusement les personnes qui m'ont soutenue et encouragée tout au long de l'aventure de thèse.

Tout d'abord, ma famille. Merci à mes parents et à Yannis pour leurs encouragements constants, leur amour, leur patience et leur soutien infaillible dans les moments difficiles. Cette thèse vous est dédiée.

Ensuite, mon compagnon d'aventure Mickaël, pour avoir égayé mon quotidien, pour m'avoir conseillé personnellement et professionnellement, et avoir partagé mes joies et mes peines.

Enfin, Nicolas, pour sa patience et son soutien.

Liste des principales abréviations

AEPD	Agencia Española de Protección de Datos
APD	Autorité de protection des données
APEC	Coopération économique Asie-Pacifique (*Asia-Pacific Economic Cooperation*)
CAHAI	Comité *ad hoc* sur l'intelligence artificielle
CCPA	California Consumer Privacy Act
CEDH	Cour européenne des droits de l'Homme
CJUE / CJCE	Cour de justice de l'Union européenne / Cour de justice des communautés européennes
CNCDH	Commission nationale consultative des droits de l'Homme
CNIL	Commission nationale de l'informatique et des libertés
CNNum	Conseil national du numérique
CNPD	Commission nationale pour la protection des données
Conv. EDH	Convention européenne des droits de l'Homme
Convention 108	Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
COPPA	*Children's Online Privacy Protection Act*
CPRA	*Califonia Privacy Rights Act*
DMA	Acte sur les marchés numériques (*Digital Markets Act*)
DPC	Autorité de contrôle irlandaise (*Data Protection Commission*)
DPO	Délégué à la protection des données (*Data protection officer*)
DSA	Acte sur les services numériques (*Digital Services Act*)
EDPB	Comité européen sur la protection des données (*European Data Protection Board*)
EDPS	Contrôleur européen sur la protection des données (*European Data Protection Supervisor*)
FTC	*Federal Trade Commission*
G29	Groupe de travail « Article 29 » sur la protection des données
GPDP	*Garante per la Protezione dei Dati Personali*

HDPA	*Hellenic Data Protection Authority*
IA	Intelligence artificielle
ICCL	*Irish Council for Civil Liberties*
ICDPPC	Conférence internationale des commissaires à la protection des données (*International Conference of Data Protection & Privacy Commissionners*)
IP	*Informacijski pooblaščenec*
LGDP	Lei Geral de Proteção de Dados
LINC	Laboratoire d'innovation numérique de la CNIL
OCDE	Organisation de coopération et de développement économiques
ONU	Organisation des Nations unies
PDPA	*Personal Data Protection Act*
PIMS	Systèmes de gestion des informations personnelles
PNR	Données des dossiers passagers (*Passenger Name Record*)
RGPD	Règlement général sur la protection des données
TETs	Technologies permettant la transparence (*Transparency-Enhancing Technologies*)
TFUE	Traité sur le fonctionnement sur l'Union européenne
TGI	Tribunal de Grande Instance
UE / EU	Union européenne / *European Union*
UODO	*Urząd Ochrony Danych Osobowych*

Sommaire

INTRODUCTION

1. Le Règlement général sur la protection des données (RGPD) fonde la licéité et la légitimité du traitement de données à caractère personnel sur six bases légales, parmi lesquelles le consentement de la personne concernée. L'article 4(11) du Règlement définit le consentement par les conditions de sa validité. Ainsi, le RGPD comprend le consentement comme :

> « Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

2. La définition du consentement par ses critères de validité révèle l'approche fonctionnelle adoptée par le législateur : le consentement se définit par son objectif, celui de garantir à la personne concernée le contrôle de ses données à caractère personnel. Cette approche est commune à l'ensemble des dispositions du RGPD, qualifié par la Commission européenne de « pilier de l'autonomisation des citoyens »[1]. Par son approche fonctionnelle de la protection des données à caractère personnel, le RGPD aurait dès lors initié une « révolution copernicienne »[2] au sens kantien du terme, abandonnant l'aspect bureaucratique de la protection des données au profit d'une approche mêlant *compliance*[3], harmonisation et *empowerment*[4] des individus[5].

---

[1] Commission européenne, *La protection des données : un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique – deux années d'application du règlement général sur la protection des données*, Communication de la Commission au Parlement européen et au Conseil, Bruxelles, 24 juin 2020, COM(2020) 264 final.

[2] KUNER Christopher, « The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law », *Bloomberg BNA Privacy and Security Law Report*, 6 février 2012, p. 1.

[3] La « *compliance* » (parfois traduite « conformité » en français) est une approche imposant aux acteurs du marché un objectif général à atteindre tout en laissant cet acteur libre de la définition des moyens qu'il souhaite déployer pour atteindre cet objectif. V. PLANE Eugénie, « Le droit de la compliance : quel bénéfice pour l'entreprise ? » *in* SAVALL Henri, ZARDET Véronique (dir.), *Tétranormalisation : profusion des normes et développement des entreprises*, EMS Edition, Collection Management socio-économique et recherche-intervention, 2020, p. 174. La notion de compliance est plus précisément développée dans le §2, B de la présente introduction.

[4] L'« *empowerment* » (parfois traduit « empouvoirement en français) est une notion héritée de divers mouvements protestataires sociaux et désignant un processus global d'acquisition du pouvoir par et au profit d'une population définie. v. CALVÈS Anne-Emmanuèle, « « Empowerment » : généalogie d'un concept clé du discours contemporain sur le développement », *Revue Tiers Monde*, 2009/4, n°200, pp. 735-749 ; BACQUÉ Marie-Hélène, BIEWENER Carole, « L'empowerment, un nouveau vocabulaire pour les pour parler de participation ? », *Idées économiques et sociales*, 2013/3, n°179, pp. 25-32. La notion de compliance est plus précisément développée dans le §2, A de la présente introduction.

[5] KUNER Christopher, *in Bloomberg BNA Privacy and Security Law Report*, *op. cit,* . p. 1.

3. Les termes d'autonomisation, de contrôle, d'*empowerment* révèlent le souci du législateur européen de sortir, au moins partiellement, la personne concernée de sa condition de partie vulnérable subissant la domination économique, sociale et politique des acteurs du numérique[6]. Le consentement apparaît alors comme un instrument privilégié qui permet à la personne concernée d'exercer un contrôle sur le sort de ses données à caractère personnel. Cependant, pour que le consentement soit réellement vecteur de contrôle et de liberté pour la personne concernée, le législateur ne pouvait pas faire l'économie de replacer la personne concernée dans son contexte socio-économique. Cette démarche a ainsi conduit le législateur à renforcer le consentement en lui attribuant des conditions de validité supplémentaires dans le RGPD[7]. L'équilibre entre consentement vecteur de pouvoir et protection de la personne concernée dans la relation de pouvoir déséquilibrée qu'elle entretient avec les acteurs du numérique est perçu comme atteint par le RGPD, à l'image des propos du Comité européen sur la protection des données (EDPB) :

> « S'il a été obtenu dans le plein respect du RGPD, le consentement est un outil qui confère aux personnes concernées un contrôle sur le traitement éventuel de leurs données à caractère personnel. Dans le cas contraire, le contrôle de la personne concernée devient illusoire et le consentement ne constituera pas une base valable pour le traitement des données »[8].

4. Néanmoins, la doctrine n'évalue pas unanimement le RGPD comme protégeant de manière suffisante et adéquate le consentement. Plus encore, le principe même de consentement est considéré comme un mécanisme ne permettant pas une protection adéquate de la personne concernée face aux phénomènes de profilage évalués indésirables par la société dans son ensemble[9] ou encore face au phénomène de « *Big Data* »[10] de plus en plus présent dans l'économie numérique[11]. La question de savoir si le consentement est un instrument

---

[6] GALUSTIAN Gohar, « La protection des données personnelles à l'épreuve du numérique », *Revue du droit public*, n°5, p. 1389.

[7] CLIFFORD Damian, GRAEF Inge, VALCKE Peggy, « Pre-formulated Déclarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections », *German Law Journal*, Cambridge University Press, 2019, n°20, p. 685.

[8] Comité européen sur la protection des données (EDPB), *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679*, version 1.1, adoptées le 4 mai 2020, p.5.

[9] NISSENBAUM Helen, « A Contextual Approach to Privacy Online », *Dædalus*, Fall 2011, Volume 140, Issue 4, pp. 34-35.

[10] Le « *Big Data* » (parfois traduit en français « données massives » correspond à des traitements sophistiqués de très grands volumes de données grâce à des outils permettant de combiner volume de données, vélocité du traitement et variété des données traitées. CNIL, « Big data », disponible sur https://www.cnil.fr/fr/definition/big-data (consulté en avril 2022).

[11] MANTELERO Alessandro, « The future of consumer data protection in the E.U. Re-thinking the « notice and consent » paradigm in the new area of predictive analytics », *Computer Law & Security Review*, 2014, n°30, pp. 649-653.

d'*empowerment* ou de *« disempowerment »*[12] de la personne concernée n'est ainsi pas encore aussi clairement tranchée que ce que laissent entendre les propos suscités de l'EDPB.

5. L'étude de la place du consentement dans le RGPD s'inscrit dans une démarche d'analyse fonctionnelle du consentement comme outil de contrôle de la personne concernée sur ses données à caractère personnel. Pour ce faire, il apparaît tout d'abord nécessaire de comprendre les notions de consentement et de RGPD (Section 1) et le contexte dans lequel ces notions sont étudiées (Section 2). Une fois le cadre théorique posé, la démarche de l'étude sera introduite à travers la présentation de la méthodologie adoptée pour mener cette étude (Section 3) et la problématique qu'elle poursuit (Section 4).

Section 1 – Objet de l'étude

6. Le choix d'analyser la place du consentement dans le RGPD sous le prisme de sa fonction en matière de protection des données à caractère personnel permet d'étudier le consentement dans une approche situant le consentement de la personne concernée dans le contexte dans lequel il est émis, dépassant ainsi le simple prisme théorique. Par conséquent, l'étude du consentement nécessite de contextualiser l'adoption du RGPD dans l'histoire et le système de la protection des données à caractère personnel, afin de comprendre la philosophie du cadre juridique de la protection des données à caractère personnel (§1). Le contexte ainsi présenté, la notion de consentement sera définie dans son acception philosophique, étymologique, courante et juridique ainsi que dans sa définition propre au RGPD (§2).

§1 – Le Règlement européen sur la protection des données, un instrument ambitieux

7. En 2016, Jan Philipp Albrecht, rapporteur au Parlement européen pour le RGPD publiait un article dans la *European Data Protection Law Review* (EDPL) un article intitulé « *How the GDPR Will Change the World »*[13]. Le titre de ce court article exprime ouvertement l'ambition du texte : s'imposer comme le référentiel mondial en matière de protection des données à caractère personnel à l'ensemble des acteurs traitant les données des Européens ou au sein de l'Union européenne, que ces acteurs soient européens ou non. Les conséquences importantes de cet instrument juridique sur le marché et les entreprises et son ambition d'effectivité à travers des amendes administratives dissuasives et un champ d'application territorial très étendu,

[12] BIETTI Elterra, « Consent as a Free Pass: Platform Power and the Limits of the Informational Turn », *Pace Law Review*, 2020, Volume 40, Issue 1, p. 377.
[13] ALBRECHT Jan Philipp, « How the GDPR Will Change the World », *European Data Protection Law Review*, 2016, Volume 2, Issue 3, pp. 287-289.

expliquent certainement les quatre ans de débats sur le Règlement, dont le prérapport détient encore à ce jour le record absolu d'amendements déposés dans l'hémicycle du Parlement européen (3133 amendements)[14].

8. Les ambitions du RGPD sont également révélées à la lecture de ses premiers considérants : le règlement a pour premier objectif de protéger le droit fondamental de la protection des données à caractère personnel des personnes physiques[15] en tant que droit non absolu « considéré par rapport à sa fonction dans la société »[16]. Ainsi, le règlement a pour tâche de concilier la protection des personnes physiques avec d'autres objectifs importants tels que les intérêts du marché numérique ou encore la protection d'autres droits fondamentaux (notamment, la liberté d'expression). De plus, le règlement devait relever un défi légal spécifique puisque, s'appliquant au domaine des nouvelles technologies dont le développement est tout aussi imprévisible que rapide, le texte devait être suffisamment précis pour garantir la sécurité juridique, tout en étant suffisamment flexible pour ne pas devenir rapidement obsolète.

9. Ainsi, le RGPD a été dessiné comme le résultat de l'évolution de la protection des données à caractère personnel (1) afin de devenir un instrument central de la protection des données à caractère personnel au sein de l'Union européenne (2).

A. Le résultat de l'évolution de la protection des données à caractère personnel

10. En France, il est de tradition d'attribuer à l'affaire SAFARI l'apparition du premier instrument de protection des données à caractère personnel, même si les préoccupations en matière de protection des données à caractère personnel trouvent également leur source dans le fichage et la traque des juifs durant l'occupation nazie[17]. Les conséquences de l'affaire SAFARI ont cependant été inédites. En effet, la population s'est rapidement et massivement saisie de la question de la protection des données à caractère personnel. En l'espèce, le projet SAFARI porté par le ministère de l'Intérieur français, avait comme objectif l'interconnexion des fichiers

---

[14] Le Monde, « Jan Philipp Albrecht, forçat du RGPD », *LeMonde.fr*, 24 mai 2018, disponible sur https://www.lemonde.fr/economie/article/2018/05/24/jan-philipp-albrecht-forcat-du-rgpd_5303754_3234.html (consulté en juillet 2021) ; Le Figaro, « Données personnelles : plus de 3000 amendements en Europe », *LeFigaro.fr*, 15 mars 2013, disponible sur https://www.lefigaro.fr/medias/2013/03/15/20004-20130315ARTFIG00552-donnees-personnelles-plus-de-3000-amendements-en-europe.php (consulté en juillet 202&).

[15] 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) (RGPD), considérant 1.

[16] Règlement (UE) 2016/679 (RGPD), considérant 4.

[17] OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Thèse pour le doctorat en droit, Université Paris I – Panthéon-Sorbonne, 8 décembre 2014, p. 11.

de l'ensemble de l'administration française[18]. La protection des données à caractère personnel a donc d'abord été envisagée dans le cadre du rapport vertical entre l'individu et l'État, la société civile craignant, à la suite de la révélation du projet par le journal *Le Monde* en 1974[19], la réalisation concrète d'œuvres d'anticipation populaires telles que *1984* de Georges Orwell. Ainsi, le traitement des données à caractère personnel par les autorités publiques a été à l'origine « de la prise de conscience, par les politiques, des enjeux de l'informatisation au regard des libertés individuelles »[20].

11. La révélation du projet SAFARI a donné naissance, quatre ans plus tard, à la loi informatique et libertés du 7 janvier 1978. Si le texte de loi s'adresse aux traitements de données à caractère personnel publics et privés, la lecture du texte révèle une inquiétude – ou du moins, une demande de garanties – plus importante lorsqu'il s'agit de traitement de données à caractère personnel dont le responsable de traitement est une autorité publique. Par exemple, son article 2 interdit directement les décisions de justice et les décisions administratives utilisant un traitement automatisé pour définir le profil ou la personnalité de la personne concernée. De plus, alors qu'un acteur du secteur privé n'est soumis qu'à un simple régime de déclaration préalable à la Commission nationale de l'informatique et des libertés (CNIL)[21], tout traitement automatisé opéré pour le compte d'une autorité publique[22] doit faire l'objet d'une loi ou d'un décret adopté après avis conforme de la CNIL, ou à défaut d'un acte réglementaire après avis conforme du Conseil d'État[23].

12. La loi informatique et libertés proposait une protection des données à caractère personnel des Français qui s'inscrivait dans le paysage technologique et économique de la fin des années 1970. L'adoption plus de vingt ans plus tard de la directive 95/46/CE s'inscrit également dans un développement technologique daté et limité. En effet, poursuivant l'objectif

---

[18] Le Monde, « Safari et la (nouvelle) chasse aux français », *LeMonde.fr*, BugBrother, 23 décembre 2010, disponible sur https://www.lemonde.fr/blog/bugbrother/2010/12/23/safari-et-la-nouvelle-chasse-aux-francais/ (consulté en juillet 2021).

[19] Le Monde, « Une division de l'informatique est créée à la chancellerie "Safari" ou la chasse aux Français », *LeMonde.fr*, Archives, 21 mars 1974, disponible sur https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux-francais_3086610_1819218.html (consulté en juillet 2021).

[20] Le Monde, « Safari et la (nouvelle) chasse aux français », *op. cit.*

[21] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (« Loi informatique et libertés »), Journal Officiel de la République Française, Loi et décrets, n°006, 7 janvier 1978, telle qu'adoptée en 1978, Article 16.

[22] L'article 15 de la Loi informatique et libertés de 1978 mentionne l'État, les établissements publics, les collectivités territoriales ou encore les personnes morales de droit privé gérant un service public.

[23] Loi informatiques et libertés, telle qu'adoptée en 1978, Article 15.

d'harmoniser la protection des données à caractère personnel au sein de l'Union européenne[24], la directive s'inspire très nettement de la loi informatique et libertés de 1978. La directive 95/46 modernise cependant la protection des données à caractère en France : elle permet de mieux protéger les personnes concernées face aux acteurs privés dont les activités numériques s'étaient développées depuis 1978, renforce les pouvoirs d'investigation de la CNIL, étaye l'obligation de transparence et crée un régime de protection spécifique aux transferts de données à caractère personnel hors Union européenne[25].

13. Le remplacement de la directive 95/46/CE par le RGPD s'est principalement justifié « au regard de l'explosion technique de ces dernières années à laquelle la directive 95/46/CE semblait ne plus pouvoir faire face »[26]. En 2010, la Commission relevait certains défis posés au cadre législatif créé par la directive, parmi lesquels l'évolution technologique, la complexification et l'invisibilisation des modes de collectes de données à caractère personnel, ou encore la mondialisation[27]. À ces considérations s'ajoutait la dimension marché intérieur des données à caractère personnel. La Commission constatait ainsi que :

> « L'une des principales préoccupations récurrentes des parties prenantes, et notamment des entreprises multinationales, est l'harmonisation insuffisante des législations des États membres en matière de protection des données, en dépit de l'existence d'un cadre juridique commun de l'UE. Celles-ci ont souligné la nécessité d'accroître la sécurité juridique, d'alléger la charge administrative et d'assurer des conditions égales aux acteurs économiques et autres responsables du traitement »[28].

14. Deux ans plus tard, la Commission européenne publiait une proposition de règlement poursuivant trois objectifs : « renforcer la dimension « marché intérieur » de la protection des données, rendre l'exercice du droit à la protection des données par les personnes physiques plus effectif et instaurer un cadre global et cohérent couvrant tous les domaines de compétence de

---

[24] La première loi européenne protégeant globalement les données à caractère personnel est une loi adoptée par le Lantag de Hesse en 1970. Elle a été suivie par l'adoptions de lois nationales en Suède (1973), Allemagne (1977), France, Danemark, Autriche et Norvège (1978). v. SCHWARTZ Paul M., « The EU-U.S. Privacy Collision : A Turn to Institutions and Procedures », *Harvard Law Review*, 2013, vol. 126, p. 1969.

[25] GOUZES Gérard, *Rapport fait au nom de la commission des Lois constitutionnelles, de la législation et de l'administration générale de la république sur le projet de loi (n°3250), relatif à la protection des personnes physiques à l'égard des traitement 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*, Rapport à l'Assemblée Nationale n°3526, enregistré à la Présidence de l'Assemblée nationale le 9 janvier 2002.

[26] SAURON Jean-Luc, « Le RGPD : outil ou entrave de la société d'information ? », *Dalloz IP/IT*, 2018, p. 17.

[27] Commission européenne, *Une approche globale de la protection des données à caractère personnel dans l'Union européenne*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Bruxelles, 4 novembre 2010, COM(2010) 609 final, p. 3.

[28] *Idem*, p. 4.

l'Union, y compris la coopération policière et la coopération judiciaire en matière pénale »[29]. Pour atteindre ce troisième objectif, la Commission européenne a proposé, en 2012, un « paquet législatif » composé d'un règlement, le RGPD, chargé d'harmoniser les dispositions européennes en matière de protection des données, et de deux directives permettant aux États membres de disposer de plus de marge de manœuvre sur la protection des données à caractère personnel dans les domaines régaliens de la justice, de la police (directive 2016/680 également appelée « directive police-justice ») et de l'utilisation des données dites *Passenger Name Record* ou « PNR »[30] (directive 2016/681, également appelée « directive PNR »), c'est-à-dire l'utilisation de données des dossiers passagers pour la prévention, la détection, l'enquête et les poursuites en matière d'infractions terroristes ou de criminalité grave.

15. En dehors des activités régaliennes, l'exploitation des données à caractère personnel a rendu nécessaire la mutation du champ d'application de la protection des données à caractère personnel. Le législateur européen a ainsi procédé à l'élargissement des champs d'application *ratione personae*, *ratione loci* et *ratione materiae*.

16. Premièrement, l'élargissement du champ d'application *ratione personae* a été rendu nécessaire par le développement de l'économie des données à caractère personnel. En effet, les acteurs numériques privés sont devenus des acteurs incontournables du marché économique, responsables de traitements intrusifs, d'une ampleur inédite et emportant des conséquences importantes sur les droits et libertés des personnes concernées. Des dires mêmes de la Commission européenne,

> « les données sont vitales pour le développement économique : elles constituent la base de nombreux produits et services nouveaux à l'origine de gains de productivité et d'efficacité dans l'utilisation des ressources dans tous les secteurs de l'économie, permettant de proposer des produits et des services plus personnalisés, d'améliorer l'élaboration des politiques et de moderniser les services publics »[31].

---

[29] Commission européenne, 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), Bruxelles, 25 janvier 2012, COM(2012) 11 final.

[30] Le traitement de données « PNR » signifie l'utilisation de données des dossiers passagers pour la prévention, la détection, l'enquête et les poursuites en matière d'infractions terroristes ou de criminalité grave. Les données des dossiers passagers (nom du passager, dates du voyage, itinéraire, numéro de siège, données relatives aux bagages, coordonnées du passager, moyen de paiement utilisé) sont conservées par les transporteurs aériens qui peuvent être amenés à les communiquer aux autorités répressives nationales. v. Conseil européen, Conseil de l'Union européenne, « Réglementer l'utilisation des données des dossiers passagers (PNR) », disponible sur https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/passenger-name-record/ (consulté en avril 2022).

[31] Commission européenne, *Une stratégie européenne pour les données*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Bruxelles, 19 février 2020, COM(2020) 66 final, p. 3.

17. Par conséquent, les préoccupations liées à l'instauration d'un *Big Brother* orwellien désignant la surveillance des citoyens par l'État ont été rejointes par les préoccupations liées à « la petite sœur orwellienne »[32] désignant la surveillance des citoyens par d'autres citoyens, et par conséquent l'exploitation des données à caractère personnel par des acteurs privés. Plus encore, la collaboration entre acteurs publics et acteurs privés dans un projet commun de surveillance a été mise en lumière par Edward Snowden en 2013. En effet, le lanceur d'alerte américain a révélé le programme PRISM permettant à la *National Security Agency* d'accéder directement aux données collectées et stockées notamment par les GAFAM (Google, Apple, Facebook, Amazon, Microsoft)[33]. Ces révélations ont d'autant plus été un tournant dans la protection des données à caractère personnel que de nombreux indices montrent que les révélations PRISM ont permis au RGPD d'être adopté, alors même que le projet souffrait alors d'une campagne de lobbying d'une agressivité inédite du fait de la valeur économique importante des données à caractère personnel[34].

18. Deuxièmement, l'élargissement du champ d'application *ratione loci* résulte du développement de l'économie des données à caractère personnel, qui a conduit à l'accélération de la mondialisation des traitements de données à caractère personnel. La mondialisation a notamment été facilitée par la nature d'internet, dont John Barlow revendiquait l'absence de frontières pour rejeter l'application de la souveraineté sur cet espace[35]. Cependant, force est de constater qu'à l'image de la loi informatique et libertés de 1978, les États ont tout de même adopté des lois régulant les activités numériques, notamment en matière de protection de données à caractère personnel. En 1980, quasiment la moitié des pays de l'organisation de coopération et de développement économiques (OCDE) avaient adopté ou étaient sur le point d'adopter des lois de protection des données à caractère personnel[36]. Les organisations internationales ont alors commencé à s'inquiéter de la multiplication de tels instruments dans un contexte d'échanges transfrontières de données à caractère personnel, à commencer par l'OCDE qui, dès 1980, déclare :

---

[32] DUTTON William H. *et al.*, *Freedom of Connection – Freedom of Expression. The Changing Legal and Regulatory Ecology Shaping the Internet*, Paris, Unesco, 2011, p. 53.
[33] The Guardian, « NSA Prism program taps in to user data of Apple, Google and others », *TheGuardian.com*, 7 juin 2013, disponible sur https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (consulté en juillet 2021).
[34] ROSSI Augustín, « How the Snowden Revelations Saved the EU General Data Protection Regulation », *The International Spectator*, 2018, vol. 53, n°4, pp. 95-111.
[35] BARLOW John Perry, « Déclaration d'indépendance du cyberespace », *in* BLONDEAU Olivier (dir.), *Libres enfants du savoir numérique. Une anthologie du « Libre »*, Paris, Éditions de l'Éclat, 2000, pp. 47-54.
[36] OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, 23 septembre 1980, Préface.

> « il est à craindre que des disparités dans les législations nationales n'entravent la libre circulation des données de caractère personnel à travers les frontières ; or, cette circulation s'est considérément intensifiée au cours des dernières années et elle est appelée à se développer encore par suite de l'introduction généralisée de nouvelles technologies des ordinateurs et des télécommunications. Des restrictions imposées à ces flux pourraient entraîner de graves perturbations dans d'importants secteurs de l'économie »[37].

19. Une série de conventions internationales de protection des données à caractère personnel ont alors été adoptées, poursuivant dans un premier temps l'objectif d'harmoniser les législations nationales autour de principes communs. Ainsi, en France, la loi informatique et libertés a été complétée par différentes conventions internationales plus au moins contraignantes, parmi lesquelles les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE (1980), la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (également appelée « Convention 108 ») du Conseil de l'Europe (1981) ou encore les Lignes directrices concernant les fichiers informatisés de données personnelles de l'Organisation des Nations unies (ONU, 1990). Au sein de l'Union européenne, le choix se porte d'abord sur l'adoption d'une directive, la directive 95/46/CE dont l'objectif est d'aboutir à un niveau de protection des données à caractère personnel « équivalent dans tous les États membres » en rapprochant des législations encore largement divergentes dans les États membres de l'Union[38].

20. L'harmonisation de la protection des données à caractère personnel des États membres de l'Union européenne a été grandement achevée par l'adoption d'un règlement européen en 2016. Cependant, il a fallu également réfléchir au champ d'application territorial des dispositions européennes face à la multiplication de traitements des données à caractère personnel de citoyens européens par des acteurs non européens, et en particulier les GAFAM. La réflexion sur le champ d'application *ratione loci* de la protection des données à caractère personnel européenne a été motivée par deux enjeux importants : l'effectivité de la protection des citoyens européens et la concurrence[39]. La Cour de Justice de l'Union européenne a initié un tel élargissement en 2014, en proposant une interprétation volontairement large de l'article 4(1)(a) dans la directive 95/46/CE établissant la portée territoriale du droit des États membres.

---

[37] *Ibidem.*

[38] 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, considérant 8.

[39] V. notamment Comité européen de protection des données, *Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3)*, 12 novembre 2019, version 2.0, p. 3.

La Cour a ainsi établi, à l'occasion de l'affaire *Google Spain*, que le droit national de l'État membre s'appliquait si un traitement de données à caractère personnel était effectué dans le cadre des activités d'un établissement établi dans cet État, même lorsque ce traitement n'était pas effectué par l'établissement en question[40]. La solution a été réaffirmée lors de l'affaire *Verein für Konsumenteninformation c. Amazon,* la Cour de Justice préférant réserver à la protection des données à caractère personnel l'application large de la directive 95/46/CE plutôt que de se positionner sur le terrain du droit international privé[41]. L'élargissement du champ d'application *ratione loci* est définitivement établi par le RGPD qui crée le critère de « ciblage »[42] aux côtés du critère plus classique du lieu d'établissement. En effet, l'article 3(2) du RGPD dispose :

> « Le présent règlement 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 de traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitements sont liées :
>
> 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 ».

Le critère du ciblage permet ainsi au RGPD de se détacher définitivement de la localisation dans l'Union européenne (soit de l'établissement responsable de traitement soit des moyens utilisés pour effectuer le traitement)[43] au profit d'une compétence territoriale fondée sur la localisation de la personne concernée par le traitement.

21. Troisièmement, l'élargissement du champ d'application *ratione materiae* s'est avéré nécessaire au regard des progrès technologiques qui ont conduit à des traitements innovants des données à caractère personnel, en particulier en matière de publicité. La loi informatique et

---

[40] v. par exemple CJUE, Gde Ch.,13 mai 2014, *Google Spain*, C-131/12, §51-55. La Cour de Justice interprète de manière volontairement large l'expression de traitement établi « dans le cadre des activités » d'un établissement pour établir l'application des règles de protection des données espagnoles à l'égard des activités de Google Search, alors même que l'activité de la filiale espagnole Google Spain se limitait « à la fourniture d'un soutien à l'activité publicitaire du groupe Google qui est distincte de son service de moteur de recherche ».

[41] Il s'agissait en l'espèce d'un litige visant à établir quel était le droit applicable à Amazon dans le cadre de la conclusion de contrats électroniques avec des consommateurs. CJUE, 3e ch., 28 juillet 2016, *Verein für Konsumenteninformation*, C-191/15, §72-81 ; PAILLER Ludovic, « L'applicabilité spatiale du Règlement général sur la protection des données (RGPD) – Commentaire de l'article 3 », *Journal du droit international (Clunet)*, n°3, juillet 2018, doctr. 9.

[42] Comité européen de protection des données, *Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3)*, 12 novembre 2019, version 2.0, p. 3.

[43] PAILLER Ludovic, « L'applicabilité spatiale du Règlement … », *op. cit.,* doctr. 9.

libertés du 6 janvier 1978 est en effet très marquée par l'état de la technologie de son époque et était ainsi « conçue pour réglementer des traitements définis en termes de stocks et des fichiers caractérisés par leur cloisonnement et leur stabilité »[44] . La définition large de la donnée à caractère personnel proposée par le RGPD a été le résultat de plusieurs décennies de jurisprudence[45] : sont par exemple désormais couvertes par la protection des données à caractère personnel les données « publiques »[46], les données professionnelles[47], ou encore les données « subjectives »[48].

22. Si certains auteurs voient dans la définition de la donnée à caractère personnel certaines limites, il semble pourtant que celles-ci aient un fondement légitime[49]. La première des limites est la protection des données à caractère personnel des personnes morales. Néanmoins, il semblerait qu'accorder une telle protection aux personnes morales relèverait d'un « anthropomorphisme excessif »[50]. En effet, la protection des données à caractère personnel relève de la protection des droits de l'homme tant elle cherche à protéger la dignité, la vie privée et l'intimité de la personne[51]. Or, la dignité est fondamentalement rattachée à la personne humaine, la vie privée et l'intimité à la notion de sensibilité humaine. Réserver la protection des données à caractère personnel aux personnes physiques semble donc tout à fait justifié. La seconde limite est la protection des données anonymes. L'exclusion des données anonymes du champ d'application du RGPD peut se déduire de la définition même de la donnée à caractère personnel, ce que le considérant 26 rappelle en disposant qu'il n'y a « 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

---

[44] FAUVET Jacques, « La protection des données personnelles », *Revue internationale de droit comparé,* 1987, n°3, p. 553.

[45] DE TERWANGNE Cécile, ROSIER Karen (dir.), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Paris, Larcier, 2018, 1e ed., pp. 60-69.

[46] CJUE, Gde Ch., 16 décembre 2008, *Satamedia*, C-73/07.

[47] CNIL, *Délibération de la formation restreinte n°2014-041 du 29 janvier 2014 prononçant une sanction pécuniaire à l'encontre de l'Association X ;* Conseil d'État, 10e ch., 30 décembre 2015, *Association Juricom et associés*, n°376845. La Cour européenne des droits de l'homme étend également la notion de « vie privée » aux activités professionnelles et commerciales. CEDH, 16 décembre 1992, *Niemetz c. Allemagne*, req. n° 13710/88, §29 ; CEDH, 25 juin 1997, *Halford c. Royaume-Uni*, req. n°20605/92, §42 ; CEDH, 16 février 2000, *Amann c. Suisse*, req. n°27798/95, §65.

[48] CJUE, 2e ch., 20 décembre 2017, *Peter Nowak c. Data Protection Commissioner*, C-434/16, §34.

[49] V. par exemple POULLET Yves, « Avant-propos. Le RGPD – une volonté de bien faire : certes ! … mais appropriée ? », *in* DE TERWANGNE Cécile, ROSIER Karen (dir.), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Paris, Larcier, 2018, 1e ed., pp. 15-16.

[50] LEPAGE Agathe, « Droits de la personnalité – Personnes titulaires de droits de la personnalité », *Répertoire de droit civil*, septembre 2009, §176.

[51] V. notamment Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (« Convention 108 »), Strasbourg, 28 janvier 1981, Préambule.

ou plus identifiable ». La limite semble ici justifiée par son champ d'application restreint, et la volonté de n'exclure du régime de protection des données à caractère personnel que les données ne représentant pas de danger pour la dignité, la vie privée ou encore l'intimité de la personne physique. La qualification de « données anonymes » doit cependant faire l'objet de la plus grande prudence à l'égard de la probabilité de réidentification, le procédé d'anonymisation demandant plus d'effort que de simples pseudonymisation, chiffrement, ou importation de procédés d'anonymisation qui ne sont pas spécialement adaptés au traitement concerné[52].

23. Le RGPD a donc été élaboré comme un instrument général régissant la protection des données à caractère personnel de manière plus large que les instruments précédents, afin de combler les lacunes créées par le progrès technologique. Cette globalisation a permis au législateur de placer le règlement comme instrument central de la protection européenne des données à caractère personnel.

B. Un instrument central de la protection des données à caractère personnel au sein de l'Union européenne

24. L'étude du RGPD ne peut cependant être envisagée dans le cadre d'une isolation clinique du Règlement, tant il s'intègre au centre de la protection des données à caractère personnel. Au sein du système européen de la protection des données à caractère personnel, le RGPD doit se comprendre comme la *lex generalis*, complété et précisé par plusieurs dispositions de *lex specialis*.

25. En effet, la Commission européenne envisage expressément le RGPD comme un élément central de la protection des données à caractère personnel au sein de l'Union européenne[53]. Instrument général de protection des données, il permet l'application concrète du droit fondamental à la protection des données tel qu'établi par les différents instruments de protection des droits de l'homme applicables tout en permettant l'élaboration de règles plus spécifiques relatives à certains aspects de la protection des données à caractère personnel. Dans ce cadre, la protection des données à caractère personnel fait l'objet d'une protection internationale et européenne d'abord au prisme du droit à la vie privée puis à travers la consécration d'un droit autonome à la protection des données à caractère personnel.

---

[52] EDPS, AEPD, « 10 misunderstandings related to anonymisation », *AEDP-EDPS joint paper*, 27 avril 2021, disponible sur https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en (consulté en décembre 2021).

[53] Commission européenne, 24 juin 2020, COM(2020) 264 final, *op. cit.*, p. 1.

26. La protection des données à caractère personnel fait d'abord l'objet d'une protection internationale et européenne en tant que droit dérivé du droit à la vie privée. La déclaration universelle des droits de l'Homme (DUDH) dispose en son article 12 que « nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation »[54], disposition qui a par la suite été reprise dans l'article 17 du Pacte international relatif aux droits civils et politiques[55]. La protection des données à caractère personnel doit se comprendre dans ce cadre comme un droit dérivé du droit à la vie privée, comme en attestent les activités du rapporteur spécial sur le droit à la vie privée en la matière[56]. La Cour européenne des droits de l'homme (CEDH) protège également le droit à la protection des données à caractère personnel à travers la protection du droit à la vie privée tel qu'établi par l'article 8 de la Convention de sauvegarde des droits de l'Homme[57]. La CEDH a, en effet, affirmé à plusieurs reprises que « la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention »[58].

27. La protection des données à caractère personnel fait également l'objet d'une protection autonome au sein d'instruments internationaux et européens. Si les premiers textes nationaux relatifs à la protection des données à caractère personnel ont généralement fait leur apparition dans les années 1970[59], le premier instrument dédié à la protection des données à caractère personnel a, quant à lui, été publié en 1980 : il s'agit des *Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel* publiées

---

[54] Organisation des Nations unies, *Déclaration universelle des droits de l'Homme*, Paris, 10 décembre 1946, résolution 217 A(III), article 12.

[55] Organisation des Nations unies, *Pacte international relatif aux droits civils et politiques*, 16 décembre 1966, adopté et ouvert à la signature, à la ratification et à l'adhésion par l'Assemblée générale dans sa résolution 2200A(XXI).

[56] V. par exemple Rapporteur spécial sur le droit à la vie privée, *Projet de lignes directrices concernant la confidentialité des données dans le cadre de l'intelligence artificiel*, Appel à contribution, terminé le 2 novembre 2020, disponible sur https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI_data_privacy_guidelines.aspx (consulté en janvier 2022) ; Rapporteur spécial sur le droit à la vie privée, *Lettre adressée à l'Inde concernant le projet de loi sur la protection des données*, 12 novembre 2018, disponible sur https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24201 (consulté en janvier 2022).

[57] L'article 8(1) de la Convention dispose que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Convention de sauvegarde des droits de l'homme et des libertés fondamentales, version amendée par les Protocole n°11 et n°14, Rome, 1950.

[58] CEDH, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, 30562/04 et 30566/04, §103 ; CEDH, *Guide sur l'article 8 de la Convention européenne des droits de l'homme. Droit au respect de la vie privée et familiale, du domicile et de la correspondance*, mis à jour le 21 août 2020, p. 47.

[59] CHALAZONITIS Kimon M., « Expériences et approches nationales de mise en œuvre de la Convention sur la protection des données », *in* Conseil de l'Europe, *Protection des données, droits de l'Homme et valeurs démocratiques*, XIIIe Conférence des Commissaires à la protection des données, 2-4 octobre 1991, Strasbourg, p. 45.

par l'organisation de coopération et de développement économiques (OCDE)[60]. Un an plus tard, le Conseil de l'Europe adopte la Convention 108, appelée « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel »[61]. Au sein de l'Union européenne, la Charte des droits fondamentaux de l'Union européenne protège également de manière autonome le droit à la protection des données à caractère personnel à son article 8[62]. L'intégration de la protection des données à caractère personnel au sein du droit primaire de l'Union européenne est également établie par l'article 16(1) du Traité sur le fonctionnement de l'Union européenne[63].

28. Cette assise de la protection des données à caractère personnel dans le droit primaire offre à l'Union européenne les compétences pour régir celle-ci au niveau de l'Union. Une telle compétence s'est notamment traduite par l'adoption du paquet législatif contenant le RGPD de 2016. L'Union européenne a également adopté d'autres instruments en matière de protection des données à caractère personnel tel que la directive « vie privée et communications électroniques » ou *e-privacy*[64] ou le règlement sur le traitement des données à caractère personnel par les institutions et organes de l'Union[65]. Deux autres instruments sont actuellement en discussion devant le Parlement européen et le Conseil : le Règlement *e-privacy* dont l'objectif est de mettre à jour et remplacer la directive *e-privacy*[66] et le Règlement relatif à l'intelligence artificielle[67]. L'arsenal législatif européen est également complété par des dispositions protectrices qui sont plus tournées vers la dimension « marché intérieur » des

[60] OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, 1980.
[61] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (« Convention 108 »), Strasbourg, 28 janvier 1981.
[62] Charte des droits fondamentaux de l'Union européenne, 2010, 2010/C, 83/02.
[63] Traité sur le fonctionnement de l'Union européenne, Article 16(1).
[64] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n°45/2001 et la décision n°1247/2002/CE.
[65] 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 (directive vie privée et communications électroniques).
[66] Commission européenne, *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 »)*, COM/2017/010 final – 2017/03(COD).
[67] Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union,* COM/2021/206 final.

données à caractère personnel comme la proposition de règlement sur les services numériques[68] ou encore la proposition de règlement sur les marchés numériques[69].

29. La présence d'une telle constellation législative a pour conséquence que le RGPD ne peut être étudié sans prendre en compte les autres instruments qui peuvent s'appliquer de manière plus ponctuelle. L'exemple le plus évident d'une telle complémentarité du RGPD avec des instruments plus spéciaux est l'interaction entre le règlement et la directive *e-privacy*, que l'EDPB envisage comme un instrument qui « vise « à préciser et compléter » les dispositions du RGPD en ce qui concerne le traitement de données à caractère personnel dans le secteur des communications électroniques »[70]. Des activités de traitement, comme le placement de cookies sur le terminal des utilisateurs, constituent à la fois des traitements de données à caractère personnel au sens du RGPD et à la fois des traitements de données à caractère personnel qui relèvent du champ d'application de la directive *e-privacy*. De même, les propositions de Règlement aujourd'hui discutées au sein de l'Union européenne visent à compléter les dispositions du RGPD. Ainsi, le Règlement *e-Privacy* est envisagé comme « une *lex specialis* par rapport au RGPD »[71] ; le Règlement sur l'intelligence artificielle a pour objectif de compléter le RGPD et la directive « Police-Justice »[72] ; les dispositions proposées au sein Règlement relatif aux services numériques « complètent, mais ne modifient pas les règles existantes sur le consentement et le droit d'opposition au traitement des données à caractère personnel »[73] ; la proposition de Règlement relatif aux marchés numériques « complète le

[68] Commission européenne, *Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE*, COM/2020/825 final.
[69] Commission européenne, *Proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques)*, COM(2020) 842 final.
[70] EPDB, *Avis 5/2019 relatif aux interactions entre la directive « vie privée et communications électroniques » et le RGPD*, 12 mars 2019, §20.
[71] Commission européenne, *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 é002/58/CE (règlement « vie privée et communications électroniques »)*, COM/2017/010 final – 2017/03(COD), §1.2.
[72] Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union,* COM/2021/206 final, §1.2.
[73] Commission européenne, *Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE*, COM/2020/825 final, p. 5.

niveau de protection existant dans le cadre du RGPD » et contribue à en éclairer son application[74].

30. Parmi la constellation législative gravitant autour du RGPD, la directive *e-privacy* représente un intérêt particulier pour la question du consentement. En effet, l'article 5 de la directive dispose que le stockage d'informations sur le terminal d'un utilisateur ou leur accès (soit le stockage et la lecture des *cookies*) nécessite un consentement préalable de l'utilisateur sauf si ces actions sont soit strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur ou ont pour finalité exclusive de permettre ou faciliter une communication électronique[75]. Ainsi, l'image généralement associée au consentement RGPD est la bannière de cookie, résultat d'une application complémentaire du RGPD et de la directive *e-privacy*. Au contraire, la question du consentement dans le RGPD est quasi-indépendante de l'analyse de la directive « Police-Justice », puisque la nature régalienne des activités régies par cette directive justifie l'exclusion du consentement comme base légale du traitement.

31. Par conséquent, le cadre de l'étude est défini par le RGPD, ce qui nécessite, quand l'objet de l'étude fait l'objet de dispositions de *lex specialis*, l'étude de ces instruments à titre complémentaire. L'étude du consentement dans le RGPD implique donc également d'étudier la place du consentement dans le système européen de protection des données à caractère personnel. Une telle étude implique de définir le consentement non seulement dans sa définition établie par le RGPD, mais également en tant que notion autonome et fréquemment rencontrée en droit.

§2 – Le consentement

32. Si le consentement est une notion juridique centrale et couramment manipulée par le juriste, cette notion ne bénéficie pas pour autant d'une définition légale générale et positive[76]. Le consentement est souvent défini de manière négative – à l'image des vices du consentement

---

[74] Commission européenne, *Proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques)*, COM(2020) 842 final, p. 4.

[75] Directive 2002/58/CE, *op. cit.*, article 5 ; CNIL, « Cookies et traceurs : que dit la loi », 1e octobre 2020, disponible sur https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/que-dit-la-loi (consulté en septembre 2022).

[76] LE GOUES Morgan, *Le consentement du patient en droit de la santé*, Thèse pour obtenir le grade de docteur en droit sous la direction de BERNAUD Valérie, Université d'Avignon et des Pays de Vaucluse, 2015, p. 5 ; CHRISTELLE Maxence, *Consentement et subjectivité juridique. Contribution à une théorie émotivo-rationnelle du droit*, Thèse pour obtenir le grade de docteur en droit sous la direction de M Étienne PICARD, Université Paris I Panthéon-Sorbonne, 2014, p. 18.

– afin de tenir compte de sa fonction (A). Le consentement RGPD, différent du consentement de droit commun, fait également l'objet d'une définition fonctionnelle (B).

A. Définition du consentement

33. Le Vocabulaire technique et critique de la philosophie définit le consentement comme un « acte de volonté par lequel on décide ou même on déclare expressément qu'on ne s'oppose pas à une action déterminée dont l'initiative est prise par autrui »[77]. Le consentement comme expression de la volonté est ainsi intrinsèquement lié à la notion de liberté dans la mesure où c'est à la volonté « qu'on a historiquement attribué la liberté »[78]. D'ailleurs, certains auteurs voient dans le consentement une expression de liberté plus grande que la volonté. Par exemple, selon Serge Boarini,

> « La volonté déterminerait une relation instrumentale à l'action (je suis cause de mon action et la volonté cesse quand l'action a eu lieu) alors que le consentement assurerait la pérennité de cette détermination : le consentement vaut encore quand la volonté qui m'a fait consentir a disparu. Le consentement donnerait à la volonté une effectivité et une matérialité – celle-ci est déjà constituée par les échanges et le dialogue : la volonté est le simple pouvoir de dire oui ou non, dira Descartes –, alors que le consentement sera le pouvoir de dire oui ou non à quelqu'un, selon des raisons et conformément à des valeurs, et par une forme visible dans une sorte de quasi-contrat sinon avec autrui du moins toujours avec moi-même »[79].

34. Ainsi, par le consentement s'exerce la liberté puisqu'il permet l'expression de la volonté en destination d'un objet, d'autrui. La définition philosophique rejoint la définition juridique puisque, si le Code civil ne définit pas le consentement, « le consentement nécessaire à la formation du contrat existe lorsque se rencontrent deux ou plusieurs volontés concordantes »[80]. Plus largement, les lexiques juridiques font apparaître la fonction principale du consentement : l'approbation[81]. La fonction approbatrice du consentement entraîne des conséquences sur ses caractéristiques[82].

---

[77] LALANDE André, *Vocabulaire technique et critique de la philosophie*, Paris, Quadrige / PUF, 2010, 3e édition, p. 177.
[78] CITOT Vincent, « Liberté et volonté. L'illusoire attestation phénoménologique d'une liberté ontologique », *Le Philosophoire*, n°18, 2002/3, p. 81.
[79] BOARINI Serge, « Le consentement : pacte et impacts », *in* AFDS (dir.), *Consentement et santé*, Paris, Dalloz, 2014, p. 50.
[80] STORCK Michel, « Synthèse – Consentement », *JurisClasseur Civil Code*, mis à jour le 1e juin 2020.
[81] Ainsi, les lexiques juridiques utilisent des termes qui, s'ils ne constituent pas des synonymes exacts de la notion d'approbation, appartiennent au même champ lexical : « acceptation », « autorisation », « approbation ». CORNU Gérard, *Vocabulaire juridique*, Paris, Quadrige / PUF, 2016, 11e édition, p. 245 ; DEBARD Thierry, GUINCHARD Serge, *Lexique des termes juridiques 2020-2021*, Dalloz, édition n°28, août 2020, p. 266.
[82] BOARINI Serge, « Le consentement : pacte et impacts », *op. cit.*, p. 47.

35. Premièrement, le consentement suppose l'affranchissement de tout lien d'autorité entre l'émetteur du consentement et son destinataire. Ainsi, « le consentement n'est pas une relation à la personne, ou du moins il n'est pas une relation à la personne du seul fait de son rôle dans la société »[83]. Dans l'émission du consentement, les parties sont réputées se trouver sur un pied d'égalité. Afin que l'égalité des parties constitue une fiction juridique acceptable, le législateur s'est appliqué à la garantir : l'émetteur du consentement trop vulnérable sera soit dépossédé de sa capacité à consentir[84], soit particulièrement protégé face à l'agent qui exercerait un lien d'autorité sur lui de manière intentionnelle[85] ou situationnelle[86]. L'égalité de pouvoir entre les deux parties a pour conséquence que le refus de consentir ne peut pas être sanctionné de quelconque manière parce qu'il ne peut pas être une « rébellion »[87].

36. Deuxièmement, le consentement implique une réflexion personnelle sur son objet. Le consentement relève du raisonnable : il n'est pas « une opération spontanée ou immédiate »[88]. La possibilité pour l'émetteur du consentement d'être à même de mener une réflexion sur l'objet du consentement conditionne la validité du consentement. Ainsi, « le consentement suppose une connaissance des raisons et […] une conception intellectualiste de l'action (je sais ce que je fais) – avec son collège d'incertitudes »[89]. Le consentement ne saurait se comprendre comme une volonté spontanée ou aveugle, ni d'une « envie subite et irréfléchie »[90], au risque de ne considérer le consentement sous le prisme unique de la protection contre l'extérieur[91]. Au

---

[83] *Ibidem.*

[84] Il s'agit notamment du cas des mineurs et des majeurs protégés. La place du consentement dans le régime applicable des majeurs protégés a tout de même évolué afin de garantir la dignité de la personne protégée, dans une recherche d'articulation entre autonomie et protection. EYRAUD Benoît, VIDAL-NAQUET Pierre A., « Consentir sous tutelle. La place du consentement chez les majeurs placés sous mesure de protection », *Tracés. Revue de Sciences humaines*, 2008, n°14, disponible sur http://journals.openedition.org/traces/378 (consulté en avril 2022) ; SCHOLTEN Matthé, GATHER Jakov, VOLLMANN Jochen, « Equality in the Informed Consent Process: Competence to Consent, Substitute Decision-Making, and Discrimination of Persons with Mental Disorders », *The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine*, Février 2021, Volume 46, Issue 1, pp. 108-136.

[85] La violence et le dol constituent des vices du consentement intentionnels, dont l'objectif est de créer un rapport d'autorité entre les cocontractants par la force (violence) ou par la ruse (dol).

[86] Constitue un rapport d'autorité situationnel la relation asymétrique entre deux contractants : le patient et le médecin, le consommateur et le professionnel, la personne concernée et le responsable de traitement. L'erreur peut également constituer un vice du consentement situationnel. En effet, l'erreur est excusable non pas par une évaluation subjective de la personne source du consentement, mais par une évaluation objective : l'erreur est caractérisée lorsque « d'autres personnes placées dans la même situation que le demandeur se seraient trompées comme lui ». ROUVIÈRE Frédéric, « Le moment d'appréciation de l'erreur », *D.*, 2014, pp. 1782-1786.

[87] BOARINI Serge, « Le consentement : pacte et impacts », *op. cit.*, p. 47.

[88] *Ibidem.*

[89] *Ibidem.*

[90] MARZANO Michela, *Je consens, donc je suis …*, Paris, Presses Universitaires de France (PUF), 2006, Hors collection, Philosophie, p. 140.

[91] *Ibidem.*

contraire, le consentement est avant tout un acte intérieur et réfléchi qui, dans une rencontre entre la volonté et la raison, « exprime un projet de gouvernement de soi »[92].

37. La fonction approbatrice du consentement met ainsi en lumière les deux caractéristiques principales accordées par le droit au consentement : le consentement est libre et éclairé. Le consentement est libre parce que l'émetteur du consentement s'engage par sa propre volonté, sans que le destinataire ne puisse l'influencer au-delà de ce que l'autonomie de la volonté de l'émetteur ne le permette. Le consentement est éclairé parce qu'il est un acte de la raison, et en tant que tel, il suppose une connaissance de l'objet, des raisons, de l'action et de ses conséquences.

38. Cette approbation matérialisée par le consentement a pour objectif de créer un rapport juridique entre l'émetteur du consentement et son destinataire. Dès lors, le consentement est la concrétisation du courant philosophique construisant les rapports juridiques sur les fondements de la volonté individuelle.[93] Ce rapport juridique peut prendre plusieurs formes. En effet, le consentement est une notion fondamentale en droit, étudiée en de nombreux champs disciplinaires : droit des contrats, droit de la famille, droit pénal, droit médical, droit social, droit administratif, etc. La notion de consentement remplit cependant des fonctions différentes. Dans le domaine contractuel, le consentement est central car la rencontre des consentements entérine la rencontre des volontés, fondement du contrat. Dans le domaine de la responsabilité, le consentement a une fonction différente, mais revêt tout de même « une place importante en matière de responsabilité, notamment pénale, puisque le droit lui reconnaît le pouvoir de transformer l'illicite en licite »[94]. Dans d'autres domaines comme le droit médical et la protection des données à caractère personnel, le consentement va aussi jouer un rôle important, celui de la légitimation des soins ou des traitements de données : le consentement a alors pour fonction de pérenniser le « lien de confiance »[95] entre les différents acteurs. Dans le domaine

---

[92] *Ibidem.*

[93] Cette philosophie volontariste est notamment héritée des travaux de Emmanuel Kant, apercevant dans la volonté individuelle l'expression d'une législation universelle, qu'il appellera loi morale et dont la source se situe dans l'autonomie de la volonté. KANT Emmanuel, *Critique de la raison pratique,* Paris, Edition Félix Alcan, 1888, traduit de l'allemand par François PICAVET, p. 85-90 ; GOYARD-FABRE Simone, « La signification du contrat dans la « Doctrine du Droit » de Kant, *Revue de Métaphysique et de Morale*, 1973, n°2, pp. 189-217. Si elle est contestée par certains auteurs, l'influence d'Emmanuel Kant et de ses disciples dans la place accordée à la volonté individuelle en droit civil reste tout de même globalement reconnue par la doctrine. V. par exemple BUFFELAN-LANORE Yvaine, LARRIBAU-TERNEYRE Virginie, *Droit civil. Les* obligations, Paris, Sirey, 2020, 17e éd., p. 281 ; CABRILLAC Rémy, *Droit des obligations*, Paris, Dalloz, 2020, 14e éd., p. 21 ; PORCHY-SIMON Stéphanie, *Droit des obligations 2022*, Paris, Dalloz, 2021, 14e éd., p. 32.

[94] LAZARO Christophe, LE METAYER Daniel, « Le consentement au traitement des données personnelles. Perspective comparative sur l'autonomie du sujet », *RJTUM*, 48-3, 2014, pp. 774-775.

[95] STOEKLÉ Henri-Corto *et al.*, « Vers un consentement éclairé dynamique », *Med Sci (Paris)*, Vol. 33, No 2, 2017, pp. 188-192.

de la protection des données à caractère personnel, le consentement a la double fonction de fonder la légalité du traitement de données à caractère personnel et de permettre à la personne concernée d'exercer un contrôle sur ses données à caractère personnel.

B. Le consentement RGPD

39. Le RGPD envisage le consentement comme une source de légalité du traitement de données à caractère personnel. L'article 6 du RGPD confère ainsi au consentement le pouvoir de transformation de l'illicite en licite sur le traitement de données à caractère personnel. Le consentement n'est pas la seule source de légalité du traitement, puisque l'article 6 établit cinq autres sources de licéité : l'exécution du contrat, le respect d'une obligation légale, la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement et la nécessité aux fins des intérêts légitimes poursuivis par le responsable de traitement ou le tiers[96]. La manifestation de volonté de la personne concernée est donc la source de licéité du traitement de ses données à caractère personnel.

40. En même temps, le consentement est envisagé au prisme du contrôle exercé par la personne concernée sur ses données à caractère personnel. Le RGPD a ainsi mis en place une démarche visant à s'assurer de la réalité du consentement, cherchant ainsi à s'assurer du caractère protecteur de celui-ci. Le choix sémantique montre le souci du législateur national et européen[97] vis-à-vis de la réalité du consentement : le règlement s'efforce de garantir une « véritable liberté de choix »[98], prohibe les situations où « il est improbable que le consentement ait été donné librement »[99], octroie aux personnes concernées un droit à l'erreur à travers le retrait du consentement, et s'intéresse à la perception biaisée des enfants qui ne sont pas « pleinement [conscients] des risques inhérents au traitement »[100]. Se retrouvent ainsi toutes les dimensions du consentement-approbation sus-étudiées.

---

[96] 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) (RGPD), article 6.
[97] Les évolutions du consentement dans le RGPD sont largement héritées des lois nationales de transposition de la directive 95/46/CE : par exemple, l'Espagne, le Luxembourg et la Suède exigeaient que le consentement soit univoque et les dispositions de la loi allemande avaient pour conséquence que le consentement devait être spécifique. EDENBERG Elizabeth, JONES Meg Leta, « Analyzing the legal roots and moral core of digital consent », *New Media & Society*, 2019, Vol. 21, Issue 8, p. 1809.
[98] RGPD, 27 avril 2016, considérant 42.
[99] RGPD, 27 avril 2016, considérant 43.
[100] RGPD, 27 avril 2016, considérant 65.

41. Premièrement, l'affranchissement de tout lien d'autorité entre l'émetteur du consentement et son destinataire se traduit par la définition du consentement comme un consentement libre. Le RGPD s'assure ainsi que le consentement de la personne concernée ne soit pas sollicité lorsqu'il « existe un déséquilibre manifeste entre la personne concernée et le responsable de traitement » [101], et que ce consentement soit accompagné, ou du moins adapté, lorsqu'il s'agit de publics vulnérables[102]. La création intentionnelle d'un lien d'autorité entre la personne concernée et le responsable de traitement invalide explicitement le consentement. En effet, le consentement arraché par la ruse est neutralisé par les exigences de consentement spécifique et univoque, interdisant le consentement résultant du silence, de l'inactivité ou encore le consentement conditionné à l'acceptation d'autres dispositions. L'égalité entre la personne concernée et le responsable de traitement est aussi protégée par l'absence de « rébellion » de la personne concernée, qui peut refuser et retirer son consentement sans subir aucun préjudice[103].

42. Deuxièmement, le législateur envisage le consentement RGPD comme le résultat d'une réflexion de la personne concernée sur l'objet du consentement : le traitement de ses données à caractère personnel. Ainsi, la personne concernée est informée du traitement des données à caractère personnel proposé avant l'émission de son consentement. L'information de la personne concernée sur le traitement de ses données à caractère personnel est d'ailleurs si importante dans le RGPD qu'elle fait l'objet d'un droit préalable à l'émission du consentement (le droit à l'information) et d'un droit postérieur à l'émission de son consentement (le droit d'accès).

43. Le consentement est ainsi envisagé comme particulièrement protecteur de la personne concernée, le législateur cherchant à faire accéder à la personne concernée une égalité de pouvoir suffisante avec le responsable de traitement pour que son consentement corresponde réellement à la manifestation de sa volonté. Or, s'il est vrai que le consentement est une notion juridique incontournable, le recours à cette notion fait encore débat tant elle est paradoxale[104]. En matière de données à caractère personnel, force est de constater que l'opportunité de fonder la protection des données à caractère personnel sur le consentement ne fait pas l'objet d'un

---

[101] RGPD, 27 avril 2016, considérant 43.
[102] RGPD, 27 avril 2016, article 8.
[103] RGPD, 27 avril 2016, considérant 42.
[104] Le paradoxe se définit dans le langage courant comme une « proposition qui, contradictoirement, mettant la lumière sur un point de vue pré-logique ou irrationnel, prend le contrepied des certitudes logiques, de la vraisemblance ». « Paradoxe », CNRTL.fr, Lexicographie, disponible sur https://www.cnrtl.fr/definition/paradoxe (consulté en novembre 2020).

consensus. En effet, « alors que les uns considèrent que les règles en matière de consentement placent les individus et leur choix au centre de la réglementation en matière de protection des données personnelles, les autres se demandent s'il est vraiment réaliste de faire du consentement un mode de légitimation des traitements dans un contexte tel que celui des environnements numériques contemporains » [105]. Certaines critiques du consentement comme expression de la volonté de l'individu vont encore plus loin puisque certains auteurs considèrent que la fonction du consentement n'est pas l'approbation, mais l'obligation. Par exemple, il a pu être affirmé que « juridiquement, le consentement ne *libère* pas, mais *oblige* » [106], une critique mettant en exergue l'engagement consécutif au consentement.

44. Ainsi, le consentement peut être appréhendé soit comme une notion protectrice de la personne concernée, soit comme une notion illusoire qui est, au mieux inutile, au pire asservissante. L'étude du consentement trouve en cette question tout son intérêt.

Section 2 – Intérêt de l'étude

45. L'étude de la place du consentement dans le RGPD trouve son intérêt dans la question de savoir si la personne concernée est effectivement protégée par l'évolution du consentement dans la protection des données à caractère personnel. Cette interrogation trouve son sens dans les changements de paradigmes de la protection des données à caractère personnel initiés par le RGPD.

46. En effet, le RGPD recentre la protection des données à caractère personnel sur la personne concernée et sur sa capacité d'exercer un contrôle sur le traitement de ses données à caractère personnel. Dans ce cadre, le consentement constitue un prisme d'étude privilégié de l'objectif d'*empowerment* poursuivi par le Règlement (A). En recentrant la protection des données à caractère personnel sur la personne concernée, le RGPD s'éloigne du système bureaucratique d'autorisation administrative qu'il avait institué sous le régime de la directive 95/46/CE. La nouvelle liberté accordée aux responsables de traitement des moyens de leur conformité aux principes de protection des données à caractère personnel, à travers le paradigme de la *compliance* entraîne des changements dans l'appréhension par le responsable de traitement de la notion de consentement (B).

---

[105] LAZARO Christophe, LE METAYER Daniel, « Le consentement … », *op. cit.*, p. 801.
[106] FABRE-MAGNANT Muriel, *L'institution de la liberté*, Paris, PUF, 2018, p.56.

§1 – Le changement de paradigme de la protection des personnes concernées (empowerment)

47. La notion d'*empowerment* a fait son entrée dans le milieu de recherche anglophone à la fin des années 1970, dans diverses disciplines parmi lesquelles la santé publique, le service social ou encore le développement communautaire[107]. La mise en place d'un paradigme d'*empowerment* (notion parfois retrouvée dans le milieu francophone sous la forme d'« empouvoirement ») est selon certains auteurs la traduction logique de la transformation de l'exploitation des données à caractère personnel, d'un modèle vertical et centralisé à un modèle horizontal et décentralisé[108]. Pour d'autres, la logique d'*empowerement* est le fruit de la conciliation entre les intérêts des personnes concernées et celles des responsables de traitement[109]. Le développement de la notion a prospéré grâce au « désir de participation des sujets sociaux », mise en avant à la fois par la culture et par le développement d'internet, notamment des réseaux sociaux[110]. La notion d'*empowerment* est d'une part libératrice puisqu'il vise la participation des personnes, pour les rendre actrices de leur protection et autonomes[111]. D'autre part, l'*empowerment* peut également se révéler une « arme de domination » lorsque la notion crée un devoir d'agir centré sur la survalorisation des capacités des individus[112]. La notion d'*empowerement* a été également présentée comme une notion centrale - voire une fin – du développement numérique, identifié comme « le vecteur d'un pouvoir d'agir du citoyen, à la fois individuel et collectif » à travers « la promesse d'une émancipation de l'individu par le numérique »[113].

48. La définition de la notion d'*empowerment* n'est pas aisée dans la mesure où la notion est polysémique, pouvant tout aussi bien désigner un état qu'un processus, une démarche individuelle qu'une démarche collective, sociétale ou politique. Dans le domaine juridique, l'*empowerment* est tout de même globalement défini par l'action de « donner le pouvoir d'agir à un maximum d'usagers en les informant de leurs droits et en les invitant à être actifs et à

---

[107] CALVÈS Anne-Emmanuèle, « «Empowerment »: généalogie …», *op. cit.*, p. 735.
[108] SWIRE Peter, « Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment », *North Carolina Law Review*, 2012, vol. 90, n°5, pp. 1408-1409.
[109] VERHENNEMAN Griet, *The Patient, Data Protection and Changing Healthcare Models*, 1e edition, Bruxelles, Intersentia, 2021, p. 129.
[110] BERNARD Françoise, « Imaginaire, participation, engagement et *empowerment*. Des notions pour penser la relation entre risques et changements », *Communication et organisation*, 2014, n°45, pp. 87-98.
[111] PORTAL Brigitte, « De l'*empowerment* anglo-saxon au développement du pouvoir d'agir européen », *Le Sociographe* », 2016, n°55, p. 84.
[112] *Ibidem.*
[113] CNNum, *Ambition numérique. Pour une politique française et européenne de la transition numérique*, Rapport remis au Premier ministre, juin 2015, p. 23.

participer »[114]. La notion d'*empowerment* peut également se définir par ses qualités : l'individu a accès au pouvoir de prendre des décisions, a accès à l'information et aux ressources lui permettant d'exercer ce pouvoir, a accès à un panel d'option afin d'exercer son choix, possède la capacité de s'imposer, a le sentiment que son choix peut faire la différence, est capable de mener un raisonnement critique[115]. La notion d'*empowerment* peut enfin se définir en opposition avec la notion de paternalisme, laquelle se définit par une démarche ayant pour objectif d'atteindre le bien-être des individus sans que le consentement ou l'opposition du sujet ne soit une considération pertinente pour le décideur[116].

49. Le cadre juridique de la protection des données à caractère personnel au sein de l'Union européenne a fait l'objet d'une évolution substantielle quant à son paradigme. La directive 95/46/CE mettait initialement en place un système de protection des données à caractère personnel dont la pierre angulaire était le contrôle par les autorités de contrôle des traitements de données à caractère personnel mis en place par les responsables de traitement. La protection des données à caractère personnel était alors principalement centrée sur le respect des dispositions de la directive par les responsables de traitement.

50. L'approche de la directive était cependant ancrée dans la situation technologique des années 1990, dont les usages et capacités ont rapidement évoluées ces deux dernières décennies. La Commission constatait alors, dans son analyse d'impact relative à la proposition de RGPD, que « les données personnelles peuvent aujourd'hui être traitées plus facilement et à une échelle sans précédent tant par les entreprises privées que par les autorités publiques, ce qui augmente les risques pour les droits des individus et remet en question leur capacité à garder le contrôle de leurs propres données »[117]. Ce constat a poussé la Commission européenne à adopter une démarche relevant de l'*empowerment*, ayant pour objectif de redonner le contrôle de leurs données à caractère personnel aux personnes concernées.

---

[114] FERRAND-BECHMANN Dan, « Une clé pour davantage de démocratie et de participation : l'empowerment ou le pouvoir d'agir », *Juris Associations*, 2008, n°383, p. 22.
[115] CHAMBERLIN Judi, « A Working Definition of Empowerment », *Psychiatric Rehabilitation Journal*, 1997, volume 20, n°4, p. 45.
[116] CHIAPPERINO Luca, *From Consent to Choice: The Ethics of Empowerment-Based Reforms*, Thèse pour l'obtention du grade de docteur en Fondations et Éthique des Sciences Vivantes sous la direction de TESTA Giuseppe, MINUCCI Saviero et TENGLAND Per-Anders, European School of Molecular Medicine, p. 68.
[117] Commission européenne, *Impact Assessment*, Commission staff Working Paper Accompanying the document 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) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC/2012/0072 final.

51. L'*empowerment* sous-entend une approche plus positive de la protection des données à caractère personnel, à travers notamment le droit à l'autodétermination informationnelle, droit reconnu par la Cour constitutionnelle allemande dès 1983[118]. L'autodétermination informationnelle a été définie comme « le pouvoir de l'individu de déterminer quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui »[119]. L'autodétermination implique ainsi de conférer des droits subjectifs aux individus, comme le droit d'accès à ses données à caractère personnel, tout en définissant des limites au droit de traiter des données à caractère personnel, comme ave les principes de limitation des finalités ou de minimisation des données[120].

52. Une telle approche s'est traduite au sein du RGPD par le contrôle offert aux individus sur les données à caractère personnel les concernant[121], qui constitue l'un des objectifs du Règlement[122]. Le consentement libre et éclairé constitue un des outils privilégiés pour la mise en place d'une démarche d'*empowerment*[123], afin que les décisions concernant les données à caractère personnel des personnes concernées soient prises par les personnes concernées elles-mêmes. La démarche du RGPD a notamment été de conférer aux personnes concernées le contrôle sur le traitement de leurs données à caractère personnel, en établissant des garanties ayant pour objectif d'éviter que le contrôle de la personne concernée devienne illusoire[124]. La recherche porte donc sur le consentement sous le prisme de l'*empowerment*, sur la capacité de la notion à placer la personne concernée en situation de pouvoir concernant ses données à caractère personnel. Une telle capacité est à contextualiser dans le cadre du RGPD dont le second changement de paradigme a attrait à sa démarche de *compliance*.

---

[118] DEBIÈS Élise, « Big data de santé et autodétermination informationnelles : quelle articulation possible pour une innovation protectrice des données personnelles ? », *Revue française d'administration publique*, 2018, n°167, p. 570.

[119] BACHERT-PERETTI Audrey, « La protection constitutionnelle des données personnelles : les limites de l'office du Conseil constitutionnel face à la révolution numérique », *Revue française de droit constitutionnel*, 2019/2, n°118, p. 276.

[120] Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *L'autodétermination informationnelle à l'ère de l'Internet. Éléments de réflexion sur la Convention n°108 destinés au travail futur du Comité consultatif*, Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, 2004, T-PD 04 final.

[121] DE TERWANGNE Cécile, ROSIER Karen (dir.), *op. cit.*, pp. 161-162.

[122] RGPD, 27 avril 2016, considérant 7.

[123] PRADES Jean-Luc, « L'imagination participative. Empowerment, pouvoir d'agir et actepouvoir », *Sciences & Actions sociales*, 2015, n°2, pp. 198-216.

[124] Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices sur le consentement au sens du règlement 2016/679*, adoptées le 28 novembre 2017, Version révisée et adoptée le 10 avril 2018, WP 259 rev. 01. p. 3.

§2 – Le changement de paradigme du cadre législatif relatif a la protection des données à caractère personnel (compliance)

53. La compliance est « une démarche permanente, une logique organisationnelle »[125] afin d'atteindre non pas la simple conformité à des règles préétablies, mais la réalisation de buts « monumentaux »[126]. La compliance organise un nouveau rapport entre le droit et ses sujets, mêlant contrainte et organisation, mais surtout détachant le droit « du passage nécessaire par l'État et son organisation administrative »[127]. La compliance innove également en instaurant des mécanismes de prévention en amont des infractions, en intégrant en son sein une dose de pédagogie, d'éthique, mais également la participation des entreprises à la conformité de leurs activités[128]. En effet, la démarche de compliance suppose que l'entreprise soit « capable d'internaliser des objectifs sociétaux plus larges que la seule poursuite de ses intérêts économiques »[129]. Dès lors, la compliance peut se définir comme « une action proactive qui vise à organiser et mettre en œuvre les procédures et moyens nécessaires au respect de la réglementation par l'entreprise »[130]. Ainsi, la compliance entraîne le renforcement de la responsabilité du destinataire du droit qu'elle recouvre[131] (voire son *accountability*[132]). Les acteurs du numérique sont donc invités à jouer « un rôle davantage proactif »[133], notamment en matière de protection des données à caractère personnel.

54. Le RGPD a enclenché la mutation de la protection des données à caractère personnel d'une légalité classique aux dispositions législative à une construction commune de la protection des données à caractère personnel par la *compliance*. Le législateur européen envisage en effet le RGPD comme un outil au service du « but monumental », énoncé par le

---

[125] MARIN Jean-Claude, « La compliance, un progrès », *in* BORGA Nicolas, MARIN Jean-Claude, RODA Jean-Christophe (dir.), *Compliance : Entreprise, Régulateur et Juge*, Paris, Dalloz, 2018, p. 16.
[126] FRISON-ROCHE Marie-Anne, « L'aventure de la *compliance* », *D.*, 2020, p. 1805.
[127] FRISON-ROCHE Marie-Anne, « Le droit de la régulation », *D.*, 2001, p. 610.
[128] DONNEDIEU DE VABRES-TRANIÉ Loraine, « L'entreprise citoyenne : vices et vertus de la compliance », *Gazette du Palais*, 2021, Hors-Série n°2, p. 33.
[129] DONNEDIEU DE VABRES-TRANIÉ Loraine, « L'entreprise citoyenne : vices et vertus de la compliance », *Gazette du Palais*, 2021, Hors-Série n°2, p. 33.
[130] LENAERTS Koen, « Le juge de l'Union européenne dans une Europe de la compliance » *in* FRISON ROCHE Marie-Anne, *Pour une Europe de la compliance*, Paris, Dalloz, 2019, p. 1.
[131] LENAERTS Koen, « Le juge de l'Union européenne dans une Europe de la compliance » *in* FRISON ROCHE Marie-Anne, *Pour une Europe de la compliance*, Paris, Dalloz, 2019, p. 2.
[132] L'*accountability* est une notion dépassant la simple responsabilité en ajoutant aux entreprises une « obligation de rendre compte » dans une perspective de bonne gouvernance. L'*accountability* présuppose par exemple une transparence plus importante des processus décisionnels envers les citoyens. NDIOR Valère, *La participation d'entités privées aux activités des institutions économiques internationales*, Thèse pour l'obtention du grande de docteur en droit sous la direction de COSNAR Michel, Université Cergy-Pontoise, 2013, 450 pages.
[133] JACQUEMIN Zoé, « Les sanctions civiles comme outils de régulation de l'activité numérique », *in* CASTETS-RENARD Céline *et al.* (dir.), *Enjeux internationaux des activités numériques*, 1e édition, Bruxelles, Larcier, 2020, p. 180.

considérant 4 : « le traitement des données à caractère personnel devrait être conçu pour servir l'humanité »[134]. Les responsables de traitement soumis à l'application du RGPD sont dès lors tenus de choisir les moyens appropriés afin de réaliser cet objectif au sein de leur activité, moyens qu'ils devront documenter pour prouver leur conformité au Règlement, leur responsabilité étant engagée pour l'ensemble des traitements de données à caractère personnel qu'ils mettent en place[135]. Le responsable de traitement n'est dès lors non plus simple sujet de l'obligation de protection des données à caractère personnel, mais en devient un véritable acteur : le responsable de traitement est soumis à une obligation de transparence accrue, doit mettre en place des mesures techniques et organisationnelles pertinentes et adaptées à sa situation et aux traitements de données à caractère personnel mis en place, et est encouragé à mettre en place des processus et règles internes à travers par exemple l'adoption de codes de conduite.

55. La démarche de *compliance* mise en place par le Règlement s'intéresse également à l'anticipation des risques, à travers la protection *ex ante* des personnes concernées et la prévention précoce des potentielles effractions. Pour se faire, le RGPD crée à la charge des responsables de traitement des obligations d'anticipation et prévention des risques à travers les différents mécanismes que sont les analyses d'impact, les obligations de vie privée dès la conception (*privacy by design*) et par défaut (*privacy by default*) ou encore l'obligation de prouver que la personne concernée a donné son consentement.

56. L'évolution de la notion de consentement est dès lors intrinsèquement liée à ce changement de paradigme. En raison de son obligation de *compliance* au RGPD, le responsable de traitement ne peut plus se suffire d'un simple respect de conditions formelles lorsqu'il demande le consentement de la personne concernée. Au contraire, le responsable de traitement se voit attribuer la responsabilité de créer les conditions optimales permettant à la personne concernée de donner un consentement valide. Cette situation peut mener à des conflits d'intérêt important, la qualité du consentement pouvant varier selon son « coût de production »[136] pour les entreprises dont le revenu dépend de ses traitements de données à caractère personnel. Le cas des entreprises publicitaires est particulièrement parlant : la demande de consentement constitue un risque pour l'entreprise parce qu'elle détourne l'attention de la personne concernée

[134] RGPD, 27 avril 2016, considérant 4.
[135] Commission européenne, COM(2020) 264 final, *op. cit.*, p. 1.
[136] WOODS Daniel W., BÖHME Rainer, « The Commidification of Consent », *Computer & Security*, avril 2022, volume 115, disponible sur https://www.sciencedirect.com/science/article/pii/S0167404822000049 (consulté en avril 2022).

de la publicité délivrée et qu'elle ne contient aucune garantie que la personne concernée acceptera le traitement de ses données à caractère personnel[137]. D'un autre côté, le respect de la protection des données à caractère personnel, et par extension, le respect du consentement de la personne concernée, peut être envisagé comme un avantage concurrentiel au profit des responsables de traitement[138].

57. Ainsi, l'étude du consentement dans le RGPD se justifie par son renforcement dans le cadre de la nouvelle relation entre le responsable de traitement, acteur de sa conformité, et la personne concernée, actrice de sa protection.

Section 3 – Méthodologie adoptée

58. L'étude de la protection européenne des données à caractère personnel présente plusieurs particularités ayant eu des conséquences sur la sélection des sources étudiées. Le RGPD est tout d'abord un instrument législatif particulièrement jeune, adopté en 2016 et mis en œuvre depuis 2018. La définition des contours des obligations du règlement nécessite ainsi non seulement l'étude des textes et de la jurisprudence portant sur ses dispositions depuis 2018, mais également l'analyse de textes et jurisprudences antérieures à son adoption. Le RGPD est également un instrument d'harmonisation de la protection des données à caractère personnel dans l'ensemble des États membres de l'Union européenne et des États ayant souhaité être liés par le règlement. De ce fait, l'étude de la jurisprudence, des éléments d'interprétation proposés par les autorités de contrôle et la doctrine font l'objet d'une recherche dans l'ensemble des systèmes juridiques pertinent pour autant que la barrière de la langue ait pu permettre cet effort[139]. Enfin, la protection des données à caractère personnel est un système de protection

---

[137] *Ibidem.*

[138] D'après la Commission européenne, « les entreprises se félicitent en général du principe de responsabilité prévu par le règlement, qui représente une évolution par rapport à l'ancienne approche ex ante, qui était fastidieuse (suppression des exigences de notification, modularité des obligations et souplesse du principe de la protection des données dès la conception et par défaut permettant une concurrence sur la base de solutions respectueuses de la vie privée. Commission européenne, *Les règles en matière de protection des données comme instrument pour créer un climat de confiance dans l'UE et au-delà – bilan* », Communication de la Commission au Parlement européen et au Conseil, Bruxelles, 24 juillet 2019, COM(2019) 374 final. D'après la Tribune, en 2016, 43% des responsables de traitement français considéraient la conformité au RGPD comme un avantage concurrentiel. La Tribune, « Protection des données : les entreprises européennes mal préparées », *LaTribune.fr*, 18 octobre 2016, disponible sur https://www.latribune.fr/technos-medias/internet/la-reglementation-europeenne-sur-les-donnees-mal-comprise-par-les-entreprises-608575.html (consulté en avril 2022). Par ailleurs, la CNIL encourage les entreprises innovantes à faire du respect du RGPD un avantage concurrentiel. CNIL, « Start-up : comment faire de votre conformité RGPD un avantage concurrentiel ? », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/startup-comment-faire-de-votre-conformite-rgpd-un-avantage-concurrentiel (consulté en avril 2022).

[139] La recherche privilégie les sources francophones, anglophones et hispanophones. De manière subsidiaire des sources utilisant une autre langue ont pu être utilisées lorsqu'aucune autre source n'était accessible. Dans cette situation, l'utilisation de moteurs de traduction a été nécessaire.

accordant des compétences importantes aux autorités de contrôle, ce qui entraîne une multiplication des instruments interprétatifs du RGPD. Ces instruments interprétatifs ont été utiles à la fois pour déterminer l'application nationale de certains principes, mais également l'interprétation proposée au niveau de l'Union européenne par le Comité européen de la protection des données (EDPB). Dès lors, l'étude s'est appuyée sur des sources européennes et internes de valeurs différentes : les traités internationaux et européens, les règlements et directives, les textes législatifs et réglementaires, la jurisprudence européenne et nationale, les décisions, déclarations, recommandations et autres textes pertinents des autorités de contrôle et de l'EDPB et la doctrine.

59. La thèse s'inscrit dans un double prisme, à la fois théorique et pratique. D'un point de vue pratique, l'étude se veut une clarification des éléments relatifs au consentement dans la protection européenne des données à caractère personnel, à travers la décortication minutieuse des différents éléments relatifs à ses qualités. Du fait de sa construction autour de la notion de *compliance*, le RGPD ne peut en effet devenir un instrument juridique obscur pour les responsables de traitement chargés de leur propre conformité. L'étude a donc vocation à répondre, clarifier, et systématiser les aspects relatifs au consentement dans le RGPD, et en déterminer les aspects encore mal saisis par la protection des données à caractère personnel. D'un point de vue théorique, l'étude souhaite dresser un premier bilan de l'application du RGPD, quatre ans après son entrée en vigueur. Ce premier bilan se déroule dans un contexte d'effort législatif important de la part de la Commission européenne, enrichissant le cadre établi par le RGPD de propositions législatives visant à le préciser et compléter. Enfin, l'étude se veut une contribution au débat doctrinal relatif aux données à caractère personnel à travers une démarche prospective. La protection des données à caractère personnel n'est pas une matière figée dans le temps, mais un domaine à bâtir, afin d'en explorer les futurs possibles à travers une réflexion critique[140].

60. Enfin, l'étude délivre une analyse juridique qui se nourrit de pluridisciplinarité. À cet égard, elle mobilise l'ensemble des champs disciplinaires permettant de préciser les contours des dispositions et enjeux du RGPD.

61. L'étude fait tout d'abord appel à des précisions scientifiques relevant du fonctionnement de l'humain (aspects neurologiques, psychologiques) afin d'évaluer l'adéquation du règlement avec les capacités de la personne concernée. Cette approche se justifie à deux égards.

[140] BARRAUD Boris, *La prospective juridique*, Paris, L'Harmattan, 2020, p. 11.

Premièrement, les dispositions relatives au consentement sont pour certaines « élaborées en connaissance savante par le droit », par exemple les dispositions relatives à une protection plus stricte des données à caractère personnel des enfants du fait de la différence de structure cognitive de ceux-ci avec les adultes[141]. Deuxièmement, en incorporant la participation de la personne concernée dans la protection de ses données à caractère personnel, le droit ne peut se permettre d'ignorer le « halo psychologique » entourant la réalité de celle-ci, formant un spectre allant de l'adhésion au rejet, en passant par l'enthousiasme, l'ennui ou encore la frustration[142].

62. L'étude fait également appel à d'autres champs disciplinaires comme l'économie, la gestion, la science politique, ou encore des aspects sociologiques afin de comprendre, expliquer et s'impliquer dans le débat social contemporain qui entoure le sujet des données à caractère personnel[143]. En effet, le droit a pour finalité de faciliter « la coordination des actions des individus en société », et n'est « accepté que dans la mesure où il remplit bien sa mission sociale »[144]. Or, cette mission sociale nécessite, pour être comprise et acquise, l'analyse d'enjeux sociétaux étudiés en détail par les chercheurs en sciences sociales, et prises en compte par le législateur dans l'édiction des normes[145]. L'approche pluridisciplinaire se justifie donc par le constat que « les données économiques, les pratiques sociales, les croyances partagées, la réalité juridique sont des considérations qui soutiennent bien souvent les réformes législatives, l'activité administrative, les interprétations jurisprudentielles, les constructions doctrinales »[146]. En atteste par exemple la démarche guidant la légistique de la Commission européenne, à travers l'évaluation de ses propositions législatives au regard de leur efficacité pour atteindre les objectifs fixés, de leur impact économique sur les parties prenantes, de leur impact social et de leur incidence sur les droits fondamentaux[147].

---

[141] PETARD Jean-Pierre, « Connaissance du droit et psychologie », *Revue juridique de l'Ouest*, 1989, pp. 104-105

[142] Pour une illustration des liens entre le halo psychologique du sujet et le droit, v. l'étude proposée par Jean Carbonnier sur la réception du droit de la filiation par la population protestante. CARBONNIER Jean, « L'amour sans la loi : Réflexions de psychologie sociale sur le droit de la filiation, en mare de l'histoire du protestantisme français », pp. 47-75.

[143] AUDIT Mathias *et al.*, « Pour une recherche juridique critique, engagée et ouverte », *D.* 2010, p. 1505.

[144] MACKAAY Ejan, « Droit et économie – autonomie et fertilisation », *in* SCHWEITZER Serge, FLOURY Loïc (dir.), *Droit et économie. Des divergences aux convergences*, Dalloz, 2019, p. 15.

[145] *Idem*, p. 16.

[146] FENOUILLET Dominique, « Avant-propos », *in* FENOUILLET Dominique, *L'argument sociologique en droit. Pluriel et singularité*, Dalloz, 2015, p. 4.

[147] D'autres considérations comme l'impact environnemental peuvent également être prises en compte par la Commission. V. par exemple, Commission européenne, COM(2012) 11 final, *op. cit.*, §2.

Section 4 – problématique et plan

63. L'étude du consentement dans le RGPD s'inscrit donc dans un débat doctrinal qui n'est pas tranché, ni dans sa dimension théorique ni dans sa dimension pratique. La question ne paraît pas non plus tranchée par ailleurs par le législateur européen dont la protection du consentement oscille entre d'une part, la volonté maintes fois proclamée d'octroyer aux personnes concernées le contrôle de leurs données à caractère personnel et ce faisant, améliorer leur confiance vis-à-vis du marché numérique européen[148] et d'autre part, l'absence de régulation d'activités numériques jugées indésirables et très attentatoires à la protection des données à caractère personnel[149].

64. De plus, même l'attitude de la personne concernée vis-à-vis de la protection de ses données à caractère personnel paraît *a priori* paradoxale. La littérature juridique et économique abonde d'études mettant en lumière le paradoxe de la vie privée (*privacy paradox*) : la volonté autoproclamée des individus en matière de protection de la vie privée et de leurs données à caractère personnel ne correspondrait à leur attitude en matière de gestion de leurs données à caractère personnel et des risques associés aux traitements qu'ils acceptent[150]. La question du consentement se complexifierait alors : si le consentement cherche à traduire la manifestation de la volonté de la personne concernée, cette dernière serait-elle constituée de sa volonté autoproclamée ou de la volonté révélée par son comportement ? Cependant, la présente étude propose de se positionner sur un autre point de vue : celui proposé par Daniel J. Solove. En effet, selon cet auteur, le paradoxe de la vie privée n'en est pas un : les personnes concernées n'ont pas un comportement contraire aux valeurs qu'ils revendiquent[151]. Au contraire, la résignation serait un comportement rationnel face au manque de ressource des personnes

---

[148] *Idem*, §1 ; Commission européenne, COM(2020) 66 final, *op. cit.*, p. 30 ; Commission européenne, COM(2020) 264 final, *op. cit.*, p. 2 ; Commission européenne, « La Commission propose des mesures pour stimuler le partage des données et soutenir les espaces européens de données », *Communiqué de presse*, Bruxelles, 25 novembre 2020, disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_2102 (consulté en janvier 2022).

[149] NETTER Emmanuel, « E-privacy ou la poursuite de la guerre contre la publicité ciblée par d'autres moyens », *Dalloz IP/IT*, 2021, p. 226.

[150] La notion de *privacy paradox* a été formulée pour la première fois en 2007. NORBERG Patricia A., HORNE Daniel R. HORNE David A., « The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviours », *The Journal of Consumer Affairs*, 2007, Vol. 41, n°1, pp. 100-126. La littérature scientifique confrontant la volonté proclamée des individus en matière de protection de la vie privée en la matière a cependant commencé à apparaître dès le début des années 2000, v. par exemple SPIEKERMANN Sarah, GROSSKLAGS Jens, BERENDT Bettina, « Stated Privacy Preferences versus Actual Behavious in EC Environments : a Reality Check », *in* BUHL Hans Ulrich, KREYER Nina, STECK Werner (dir.), *e-Finance*, Berlin, Springer, 2001, pp. 129-147. Pour une analyse d'ensemble de la littérature scientifique relative au *privacy paradox*, v. GERBER Nina, GERBER Paul, VOLKAMER Melanie, « Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior », *Computer & Security*, 2018, Volume 77, pp. 226-261.

[151] SOLOVE Daniel J., « The Myth of the Privacy Paradox », *George Washington Law Review*, 2021, Volume 89, Issue 1, pp. 1-51.

concernées quant à la gestion de leurs données à caractère personnel[152]. La question n'est alors plus de savoir quelle est la volonté réelle de la personne concernée, mais de s'intéresser aux raisons pour lesquelles les personnes concernées ne sont pas aptes à exprimer leur volonté en matière de protection de la vie privée à travers le mécanisme de consentement.

65. Il ne s'agit pas pour autant de rejeter la notion de consentement en matière de protection des données à caractère personnel. Au contraire, lorsque les conditions permettant l'expression de la volonté réelle de la personne concernée sont réunies, le consentement permet à la personne concernée de contrôler le traitement de ses données à caractère personnel selon ses propres valeurs, convictions et opinions. Le consentement doit en effet atteindre un certain seuil de qualité (ci-après désigné « *gold standard* »[153]) afin que la réalité du consentement soit garantie à la fois vis-à-vis de la personne concernée et au regard de l'environnement dans lequel évolue cette personne.

66. La définition du *gold standard* n'est pas une notion unanimement définie par la doctrine. Deux standards ont cependant attiré notre attention. Premièrement, selon Elizabeth Edenberg et Meg Leta Jones, la racine morale du consentement nécessite la satisfaction de cinq critères :

> « (1) clear delineation of the background conditions for permissible and impermissible uses of one's data ; (2) a defined scope of action ; (3) relevant information provided to the consentee ; (4) freedom to choose among a set of viable options; and (5) the consentee should be treated fairly and should not be required to sacrifice other important rights »[154].

Généraux, ces critères replacent la personne concernée au centre de la protection des données à caractère personnel, en insistant sur la capacité d'anticipation des conséquences du consentement, l'information délivrée à la personne concernée, le lien entre la liberté du consentement et la variété de choix offerte à la personne concernée et la relation entre le consentement et la protection des droits fondamentaux.

67. Neil Richards et Woodrow Hartzog ont proposé une définition plus pratique du *gold standard* en matière de consentement numérique, celui-ci étant valide :

---

[152] *Idem*, p. 5.
[153] L'expression est notamment utilisée en ce qui concerne le seuil de qualité que doit atteindre le consentement en matière médicale. V. par exemple BROSMAN Terenia, PERRY Michael, « « Informed » consent in adult patients: can we achieve a gold standard? », *British Journal of Oral and Maxillofacial Surgery*, Volume 47, Issue 3, avril 2009, pp. 186-190 ; MOULTON Ben *et al.*, « From informed consent to informed request: do we need a new gold standard ? », *Journal of the Royal Society of Medicine*, 2013, Volume 106, Issue 10.
[154] EDENBERG Elizabeth, JONES Meg Leta, *op. cit.*, p. 1816.

> « when we are asked to choose *infrequently*, when the potential harms that result from the consent are *easy to imagine*, and when we have the correct *incentives to consent* consciously and seriously »[155]

Plus pratiques, ces critères situent la question du consentement dans le contexte dans lequel il est émis. Ainsi, la personne concernée n'émettrait un consentement valide que si la demande de consentement ne constitue pas une nuisance, si elle peut anticiper les risques relatifs à l'émission de son consentement et si la demande de consentement est construite de telle façon qu'elle encourage la personne concernée à opérer une réflexion interne avant l'émission du consentement.

68. Ces *gold standards* visent à sortir la personne concernée de son « incapacité » à donner un consentement libre et éclairé afin qu'elle puisse accéder par la connaissance, le choix, la pratique et la défense de ses intérêts à une position de pouvoir satisfaisante pour considérer sa relation avec le responsable de traitement comme une relation dépourvue de contrainte et de lien d'autorité. Il a été étudié précédemment que l'ambition du RGPD est similaire à travers la définition du consentement par l'énumération de ses critères de validité. Cependant, confronté aux deux *gold standards* présentés, le consentement RGPD ne semble satisfaire que partiellement les critères moraux et pratique visant à garantir un consentement qui soit valide.

69. Pourtant, le consentement a le potentiel de devenir un outil privilégié du contrôle exercé par les personnes concernées sur leurs données à caractère personnel, en tant qu'expression de la volonté et de la dignité de la personne concernée. **Néanmoins, malgré l'effort du législateur européen, le RGPD présente des lacunes empêchant la personne concernée d'accéder à un pouvoir suffisamment équivalent à celui du responsable de traitement pour réellement refléter la manifestation de sa volonté**. Ainsi, le RGPD est le résultat d'un renforcement incomplet du consentement (Partie 1) dont les limites altèrent sa validité au profit d'un consentement illusoire (Partie 2).

[155] RICHARDS Neil, HARTZOG Woodrow, « The Pathologies of Digital Consent », *Washington University Law Review*, 2019, Volume 96, p. 1465.

PARTIE 1 – LE RENFORCEMENT INCOMPLET DE LA RÉALITÉ DU CONSENTEMENT

70. La réception du RGPD dans l'univers médiatique a accordé une place privilégiée au consentement, tantôt qualifié de « révolution »[156] ou de « nouvelle ère »[157] ou encore présenté comme l'expression d'une volonté collective enfin exaucée[158]. Pourtant, le RGPD n'est pas le premier instrument de protection des données à caractère personnel à prévoir le consentement comme base légale pouvant fonder un traitement des données à caractère personnel. L'innovation du RGPD ne se trouve donc pas dans la reconnaissance du consentement comme base légale.

71. En effet, si le consentement était absent de la version initiale de la Loi informatique et libertés en dehors des traitements qui « font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales des personnes »[159], la question du consentement avait pourtant déjà été abordée dans les débats précédant son adoption comme le démontre le texte de l'article 10 de la déclaration des libertés publiée en juin 1975 par le parti communiste français :

> « Il est interdit de recueillir des renseignements sur la vie privée d'une personne sans son consentement, en dehors des cas exceptionnels expressément prévus par la loi. De tels renseignements ne doivent en aucun cas être utilisés à d'autres fins que celles que l'intéressé a acceptées ou que la loi a prévues »[160].

Ces discussions avaient alors abouti à la proposition de l'amendement n°4 lors des débats parlementaires préalables à l'adoption de la loi informatique et libertés dans sa version de 1978 :

> « Il est interdit de recueillir des renseignements sur la vie privée d'une personne sans son consentement, en dehors des cas exceptionnels expressément prévus par la loi »[161].

---

[156] Le Temps, « Le RGPD, la révolution du consentement », *letemps.ch*, 11 février 2018, disponible sur https://www.letemps.ch/societe/rgpd-revolution-consentement (consulté en mai 2022) ;
[157] Les Échos, « La nouvelle ère du consentement numérique », *lesechos.fr*, 29 mai 2018, disponible sur https://www.lesechos.fr/idees-debats/cercle/la-nouvelle-ere-du-consentement-numerique-132946 (consulté en mai 2022).
[158] ZDNet, « Le RGPD exige (enfin) un consentement éclairé », *zdnet.fr*, 7 décembre 2017, disponible sur https://www.zdnet.fr/actualites/le-rgpd-exige-enfin-un-consentement-eclaire-39861032.htm (consulté en mai 2022).
[159] Article 31, Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Journal Officiel de la République Française, Loi et décrets, n°006, 7 janvier 1978, p. 229.
[160] VILLA Lucien, Journal Officiel de la République Française (JORF) n°79 A.N., 5 octobre 1977, p. 5787.
[161] JORF 5 octobre 1977 (séance du 4 octobre 1977), p. 5792, disponible sur http://archives.assemblee-nationale.fr/5/cri/1977-1978-ordinaire1/002.pdf (consulté en janvier 2021).

72. Rejetée lors du vote parlementaire, cette proposition aurait institué le recueil du consentement en régime « par défaut » d'une collecte de données à caractère personnel. Néanmoins, le parlement n'a en réalité pas rejeté la notion même du consentement, mais plus particulièrement le champ d'application, alors perçu comme trop large, de la proposition : non seulement la notion de « renseignements sur la vie privée » faisait l'objet d'une maladresse de langage difficile à interpréter pour le juriste, mais le garde des Sceaux avait également regretté une rédaction trop générale pouvant aboutir à restreindre d'autres libertés fondamentales comme la liberté de la presse. En effet, cette formulation aurait pu conduire à interdire aux journalistes de publier certaines informations[162].

73. Il faudra ainsi attendre la directive 95/46/CE et sa transposition par la loi informatique et libertés pour que le consentement en tant que base légale de traitement de données à caractère personnel apparaisse dans le paysage juridique français. La directive 95/46/CE envisageait en effet déjà le consentement comme base légale du traitement[163], exigeant que celui-ci soit le résultat d'une « manifestation de volonté, libre, spécifique et informée »[164]. Elle faisait dès lors déjà apparaître la nécessité d'obtenir un consentement valable pour fonder un traitement de données à caractère personnel. Pour le juriste non averti, le RGPD ne serait *a priori* pas novateur en matière de consentement, et ne s'inscrirait finalement que dans la continuité avec la directive en vigueur précédant son adoption.

74. Cependant, l'innovation du RGPD en matière de consentement se situe bien au niveau des critères attestant de sa validité, le règlement traduisant les efforts du législateur européen visant à renforcer les dispositions relatives au consentement afin que celui-ci corresponde effectivement à la manifestation de volonté de l'individu. En effet, l'objectif du législateur est de « confier aux individus la responsabilité de la collecte et de l'utilisation de leurs données à caractère personnel »[165]. Dans ce cadre, le mécanisme du consentement se rattache à la « théorie de contrôle de la vie privée » (*control theories of privacy*)[166], théorisée par de nombreux auteurs[167]. Ainsi, la vie privée ne serait, selon Charles Fried, « pas simplement une absence

---

[162] *Ibidem.*
[163] Directive 95/46/CE du 24 octobre 1995, considérant 30, Article 7.
[164] *Ibidem*, article 2(h).
[165] REIDENBERG, Joel R *et al.*, « Privacy Harms and the Effectiveness of the Notice and Choice Framework », *TPRC Conference Paper*, 2014, disponible sur SSRN.
[166] TAVANI Herman T. « Philosophical theories of privacy: Implications for an adequate online privacy policy », *Metaphilosophy*, 38.1, 2007, pp. 1-22.
[167] FRIED Charles, « Privacy: A Rational Context », *in* ERMANN David *et al.* (dir.), *Computers, Ethics and Society*, New York, Oxford University Press, 1990, pp. 50-63 ; MILLER Arthur, *The Assault on Privacy*, Cambridge, Harvard University Press, 1971 ; BEARDSLEY Elizabeth, « Privacy: Autonomy and Selective

d'information sur nous dans l'esprit des autres, mais plutôt un contrôle des informations que nous avons sur nous-même » [168]. Cette notion de « contrôle » se retrouve d'ailleurs très rapidement dans le texte du RGPD, puisqu'il est nettement affirmé, dès le septième considérant, que « les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant »[169]. La notion de « contrôle » des données à caractère personnel est par ailleurs régulièrement rappelée par la Commission européenne comme un objectif du RGPD[170], ce qui a récemment été reconfirmé lors du déploiement d'applications de traçage dans le cadre de la pandémie de COVID-19[171].

75. De plus, le consentement répond également à un objectif plus général. Il s'agit, d'une part, de préserver l'autonomie des individus et, d'autre part, de permettre une flexibilité du régime de protection des données pour les entreprises et une harmonisation des régimes juridiques dans l'Union européenne[172]. Le consentement semble donc permettre de répondre exactement à l'objectif annoncé du RGPD : « [protéger] les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel »[173] tout en veillant à ce que « la libre circulation des données à caractère personnel au sein de l'Union [ne soit] ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel »[174]. Ce double objectif a été réaffirmé dans une Communication de la Commission évaluant les premières années d'application du RGPD. Cette dernière s'est ainsi félicité que le RGPD ait « renforcé les garanties apportées en matière de protection des données » et, en même temps, que le RGPD ait créé « une égalité des conditions de concurrence pour toutes les entreprises exerçant des activités sur le marché de l'UE, indépendamment de leur lieu d'établissement, et [qu'il ait] garanti la libre circulation des données dans l'UE, renforçant de la sorte le marché intérieur »[175].

Disclosure », *in* PENNOCK J. Roland, CHAPMAN, John W. (dir.), *Nomos XIII: Privacy*, New York, Atherton Press, 1971, pp. 56-70 ; RACHELS James, « Why Privacy is Important », *Philosophy and Public Affairs*, n°4, 1975, pp. 323-333 ; WEINSTEIN Michael A., « The Uses of Privacy in Good Life», *in* PENNOCK J. Roland, CHAPMAN, John W. (dir.), *Nomos XIII: Privacy*, New York, Atherton Press, 1971, pp. 88-104.

[168] FRIED Charles, *op cit.*, pp. 50-63

[169] RGPD, 27 avril 2016, Considérant 7.

[170] Voir par exemple Commission européenne, *Une meilleure protection et de nouvelles perspectives – Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018*, Communication de la Commission au Parlement européen et au Conseil, Bruxelles, 24 janvier 2018, COM(2018) 43 final, p. 3 ; Commission européenne, COM(2020) 264 final, *op. cit.*, p. 2.

[171] Commission européenne, *Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données*, Communication de la Commission, 17 avril 2020, 2020/C-124, p. 4.

[172] LAZARO Christophe, LE MÉTAYER Daniel, *op. cit.*, p. 771.

[173] RGPD, 27 avril 2016, Article 1 (2).

[174] RGPD, 27 avril 2016, Article 1 (3).

[175] Commission européenne, COM(2020) 264 final, *op. cit.*, p. 1.

76. Il apparaît alors que ce modèle est prometteur, puisqu'il permettrait d'empêcher une régulation excessive d'activités économiques tout à fait légitimes[176]. En effet, selon une doctrine majoritairement américaine et largement partagée sur le continent européen, « des restrictions rigides résultant d'une régulation excessive peuvent entraver l'innovation et la concurrence, mais les mécanismes fondés sur l'autonomie de l'utilisateur empêchent » une telle entrave[177]. Dans cette optique, le consentement trouve une place privilégiée dans la mesure où le « consentement égalise les volontés »[178]. Appliqué au cadre de la protection des données à caractère personnel, cela signifie qu'en acceptant une offre, la personne concernée élève sa volonté au niveau de celle de l'offrant (le responsable de traitement). Conséquence directe de ce constat, le consentement engage la personne concernée puisqu'il ne pourra pas estimer que les conséquences négatives de l'acte auquel il a consenti sont exclusivement le fait d'un tiers[179]. Ce modèle correspond aussi à une certaine vision du droit à la vie privée, celle d'Alan Westin. En effet, en 1967, ce dernier définissait le droit à la vie privée (« *privacy* ») comme « le droit accordé aux individus, groupes ou institutions de déterminer pour eux-mêmes quand, comment et dans quelles mesures les informations les concernant sont communiquées aux autres »[180]. Appliquée à l'environnement numérique, cette vision du droit à la vie privée implique un droit de la personne concernée au contrôle de l'utilisation de ses données à caractère personnel[181].

77. Ainsi, de nombreux modèles législatifs se concentrent sur la capacité de choix de la personne concernée ou de l'utilisateur du service concerné. L'Union européenne n'est, de ce fait, pas la seule entité à considérer le consentement comme un modèle usuel, voire privilégié de la protection des données à caractère personnel. Déjà en 1980, les lignes directrices de l'OCDE liaient la collecte et l'utilisation des données à caractère personnel au consentement de la personne concernée. En Asie, l'*APEC Privacy Framework* érige le choix – par extension, le consentement – en véritable principe gouvernant la protection des données à caractère personnel[182]. Le modèle est aussi apprécié outre-Atlantique. En effet, en 2012, la *Federal Trade Commission* (FTC) recommandait déjà au législateur américain « [d']offrir un mécanisme de

---

[176] REIDENBERG, Joel R *et al.*, *op. cit.*
[177] *Ibidem*.
[178] BOARINI Serge, *op. cit.*, p. 48.
[179] *Idem*, p. 47.
[180] « *the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others* » [traduction libre]. WESTIN Alan F., « Privacy and Freedom », *Wash. & Lee L. Rev.*, n°25, p. 166.
[181] SCHWARTZ Paul M., « Privacy and Democracy in Cyberspace », *Vanderbilt Law* Review, vol. 52, 1999, pp. 1609-1999 ; FRIED Charles, « Privacy: A Rational Context », *op. cit.*, pp. 50-63 ; FROOMKIN A. Michael, « The Death of Privacy ? », *Stanford Law Review*, n°52, 2000, pp. 1461-1548.
[182] APEC Privacy Framework, §20.

choix simplifié qui donne aux consommateurs un contrôle plus significatif, et qui améliore la transparence de leurs pratiques en matière de traitement de données »[183]. En Australie, la notion de consentement a aussi connu un succès, bien que cette notion soit plus large que la notion européenne dans la mesure où le consentement est défini comme un consentement explicite ou implicite[184]. En effet, *l'Australian Privacy Act* conditionne l'utilisation de certaines bases légales à l'impossibilité de recueillir le consentement : ce sera par exemple le cas de la collecte de données de santé dans le cadre de recherches relevant de la santé publique[185]. De plus, la collecte de données à caractère personnel sensibles est conditionnée à la collecte du consentement. Si tel n'est pas le cas, la collecte fait l'objet d'un régime dérogatoire[186].

78. Enfin, il faut noter qu'en Europe, certaines théories vont plus loin dans le développement de la notion de consentement, en érigeant le choix (et par extension le consentement), non plus comme un outil de la protection des données à caractère personnel, mais comme son but[187]. En 1983, la Cour constitutionnelle allemande définit pour la première fois l'autodétermination informationnelle comme « le pouvoir de l'individu de décider lui-même, sur la base du concept d'autodétermination, quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui »[188]. Cette notion a été admise au niveau européen par le biais de la Cour européenne des droits de l'homme (CEDH), qui a affirmé en 2017 que « l'article 8 de la Convention consacre donc le droit à une forme d'autodétermination informationnelle, qui autorise les personnes à invoquer leur droit à la vie privée en ce qui concerne des données qui, bien que neutres, sont collectées et diffusées à la collectivité, selon des formes ou modalités telles que leurs droits au titre de l'article 8 peuvent être mis en jeu »[189]. Cependant, cette approche, bien qu'elle soit, dans la suite de nos propos,

---

[183] « *offer simplified choice mechanisms that give consumers more meaningful control, and increase the transparency of their data practices*" » [traduction libre]. Federal Trade Commission (FTC*), Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers*, 2012, disponible sur http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commissionreport-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (consulté en février 2021).

[184] Australian Privacy Act, Part II, Division 1, Section 6 (1).

[185] *Idem*, Part II, Division II, Section 16B.

[186] *Idem*, Schedule 1, Part 2, Section 3, 3.3.

[187] CATE Fred H., « Protecting Privacy in Health Research: The Limits of Individual Choice », *California Law Review*, Vol. 98, No 6, 2010, pp. 1765-1803.

[188] POULLET Yves, ROUVROY Antoinette, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in* BENYEKHLEF Karim, TRUDEL Pierre (dir.), *État de droit et Virtualité*, Montréal, Thémis, 2009, p. 159.

[189] CEDH, Grande Chambre, 27 juin 2017, *Satakunnan Markkinapörssi et Satamedia Oy c. Finlande*, req. n°913/13.

utilement confrontée à la notion de consentement, n'est pas reprise dans le droit européen de la protection des données à caractère personnel[190].

79. En effet, l'article 4, alinéa 11, du RGPD définit le consentement comme « toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Le RGPD fait ainsi le choix, dans cette définition, de regrouper les caractéristiques propres au consentement – « libre » et « éclairé » – et les dispositions garantissant l'effectivité de ces caractéristiques – « spécifique » et « univoque ». En effet, lorsque le caractère libre et éclairé se rapporte à la qualification du consentement, le caractère spécifique et équivoque se rapporte aux modalités de recueil du consentement. Ainsi, un consentement univoque permet à la personne concernée d'être informée sur les traitements la concernant (consentement éclairé), et de ce fait, d'effectuer expressément ce choix (consentement libre). De même, un consentement spécifique permet à la personne concernée de s'informer de chacune des finalités du traitement (consentement éclairé) et de pouvoir choisir s'il consent au traitement pour chacune des finalités, indépendamment des autres (consentement libre). Le lien entre consentement spécifique et éclairé avait d'ailleurs déjà été relevé par le G29 lors de son avis de 2011 relatif à la définition du consentement :

> « Pour être spécifique, le consentement doit être intelligible. Il doit mentionner, de façon claire et précise, l'étendue et les conséquences du traitement des données […]. Un « consentement spécifique » est dès lors intrinsèquement lié au fait que le consentement doit être informé. Il existe une obligation de « détail » du consentement »[191].

Le lien entre consentement univoque et consentement libre avait aussi été souligné, de manière plus subtile, par le G29 lors d'une contribution de 2009 :

> « La complexité des pratiques de collecte des données, des modèles commerciaux, des relations entre fournisseurs et des applications technologiques dépasse, bien souvent, la capacité ou la volonté d'une personne de décider, par un choix actif, de contrôler l'utilisation et le partage d'informations »[192].

---

[190] En particulier, aucune mention de l'autodétermination informationnelle ne sera présente dans le Règlement général sur la protection des données (RGPD).

[191] Groupe de travail « Article 29 » sur la protection des données, *Avis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187.

[192] Groupe de travail « Article 29 » sur la protection des données, *L'avenir de la protection de la vie privée – Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel*, 1er décembre 2009, WP 168.

80. Plan – Ainsi, la Partie 1 se concentrera sur les caractéristiques attachées au consentement plutôt qu'à celles se rapportant aux modalités de son recueil, même si celles-ci se retrouveront au sein des développements. L'étude s'intéressera donc aux efforts européens renforçant le consentement éclairé par une obligation d'information exigeante (Titre 1) puis aux mécanismes de protection assurant le consentement libre par la protection du choix de la personne concernée (Titre 2).

TITRE 1- LE RENFORCEMENT DU CONSENTEMENT ÉCLAIRÉ : UNE OBLIGATION D'INFORMATION EXIGEANTE

82. Le caractère éclairé du consentement a été largement étudié en sciences humaines, sociales et juridiques : notion classique de droit des contrats, elle apparaît très tôt dans les études de philosophie. En effet, dès l'antiquité, les philosophes se sont emparés de cette notion et en ont notamment dégagé deux aspects qui s'appliquent encore de manière pertinente à la question du consentement au traitement de ses données à caractère personnel.

83. En premier lieu, garantir un consentement éclairé permet de protéger le consentement des personnes concernées afin qu'ils ne s'engagent pas dans des actes auxquels ils n'auraient pas consenti s'ils avaient pu en saisir tous les enjeux. Le consentement non, peu ou mal éclairé serait alors invalide. À ce propos, Aristote affirmait que « semblent non consentis les actes qui s'accomplissent […] par ignorance »[193]. Il ajoutait à cette affirmation une distinction bienvenue entre les actes accomplis « dans l'ignorance » et « par ignorance » : quand les premiers relevaient de sa propre méchanceté (par exemple, l'ivresse) et rendaient la personne responsable de ses actes, les seconds résultaient quant à eux d'un manque d'information qui ne pouvait lui être reproché[194]. Dès lors, le consentement obtenu par ignorance ne pourrait être validé par le droit puisqu'aucune faute ne pourrait être imputée à l'émetteur du consentement. Ce dernier doit donc être protégé des manœuvres visant à obtenir son consentement de manière trompeuse ou frauduleuse.

84. En deuxième lieu, le consentement éclairé implique une démarche de transparence et de bonne foi de l'offrant. À ce propos, Cicéron avait affirmé que taire une information constituait bien une manœuvre opérée en vue de son profit. En effet, au sein d'un débat romancé entre Antipater et Diogène, Antipater déclarait que « cacher quelque chose en pareil cas, ce n'est pas seulement ne pas dire, c'est vouloir, parce qu'on y a profit, que ceux qui ont intérêt à savoir, ignorent »[195]. Dans cette vision, taire équivaut à tromper : un consentement non éclairé est le résultat d'une manœuvre contraire à l'éthique. Le consentement éclairé nécessite donc, de la part de la personne cherchant à obtenir le consentement d'une autre personne, le respect d'une obligation d'information et de transparence. Cette obligation d'information va par ailleurs plus loin que la simple tromperie (la délivrance d'informations fausses ou trompeuses), car elle

[193] ARISTOTE, *Éthique à Nicomaque*, Les classiques de la philosophie, édition 1992, p. 131.
[194] *Idem*, p. 133.
[195] CICERON, *De officiis*, Livre III, traduit par Charles APPUHN, Cicéron, Des devoirs. Paris, Garnier, 1933.

impose que toute information permettant à l'émetteur du consentement de faire un choix en toute connaissance de cause soit portée à sa connaissance.

85. Cette dualité est également présente en termes sémantiques puisque le terme « éclairer » signifie, au sens figuré, l'action de « rendre clair, compréhensible, intelligible »[196] quelque chose. Ainsi, le caractère « clair, compréhensible, intelligible » de l'information permet à son récepteur de prendre une décision en toute connaissance de cause, tandis que l'action de « rendre » implique une action positive de la part de l'émetteur de l'information. Cette action positive est d'ailleurs évaluée du point de vue du résultat, l'étymologie du terme éclairer révélant la volonté de « faire comprendre, éclairer »[197].

86. La dualité des enjeux attachés au consentement éclairé entraîne des conséquences juridiques. La transparence présente ainsi également une nature mixte, puisque selon la formule de François Vialla, « l'information est à la fois « fin et moyen » »[198]. L'information est une finalité au regard du responsable de traitement, la transparence constituant une obligation à sa charge. L'information est également un moyen puisqu'il s'agit d'un instrument permettant d'obtenir un niveau de compréhension suffisant pour que la personne concernée puisse donner son consentement. C'est pourquoi, concernant la protection des données à caractère personnel, l'information est à la fois un droit de la personne concernée et un devoir du responsable de traitement.

87. L'étude philosophique, sémantique et juridique du terme « éclairer » révèle une particularité importante du consentement éclairé : le sujet est la base de référence de l'évaluation de la clarté, de la compréhensibilité et de l'intelligibilité de l'objet du consentement. Par cette définition, le juriste retrouve les enseignements de Thomas d'Aquin selon lequel « *consensus voluntatis est actus qui praesupponit actum intellectus* »[199] : le consentement de la personne concernée n'est pas un « acte passif »,[200] mais un réel acte de volonté nécessitant un acte intellectuel. Par conséquent, la validité du consentement est conditionnée par l'obligation de l'entreprise de rendre compréhensibles par le sujet tous les éléments attachés à son objet. Cette particularité n'est encore une fois pas propre à la protection des données à caractère personnel puisque l'information est systématiquement envisagée au

---

[196] « Eclairer », CNRTL.fr, Lexicographie, disponible sur https://www.cnrtl.fr/definition/éclairer
[197] *Ibidem.*
[198] VIALLA François, « Enjeux et logique de l'information comme préalable au consentement », *in* AFDS (dir.), *Consentement et santé,* Paris, Dalloz, 2014, p. 36.
[199] « L'acte de volonté présuppose un acte intellectuel ». D'AQUIN THOMAS, *Summa* Theologica, Tomus Octavus, 1860, p. 84.
[200] VIALLA François, *op. cit.* , p. 36.

niveau juridique du point de vue du destinataire : l'information du salarié, l'information du consommateur, ou encore l'information des administrés par exemple[201]. Consacrée par les articles 4 et 7 du RGPD, l'obligation d'obtenir un consentement éclairé est renforcée par l'article 13 du même règlement, qui consacre une obligation d'information générale à la collecte de données à caractère personnel auprès de la personne concernée. Pour cause, « le consentement et l'information se manifestent comme deux droits étroitement liés. L'exercice de l'un dépend de la correcte compréhension préalable de l'autre »[202]. La jurisprudence des autorités de contrôle illustre ce lien. Dans sa décision de 2018 contre la société Google LLC., la CNIL affirme que le « caractère éclairé doit être examiné à la lumière des développements précédents concernant le défaut de transparence et d'information des utilisateurs lors de la création de leur compte », car « les manquements précédemment identifiés ont nécessairement une incidence sur l'information délivrée aux utilisateurs pour assurer le caractère éclairé du consentement »[203]. Bien qu'elle examine séparément la question de la conformité à l'article 13 et la question du consentement éclairé, la CNIL ne se fonde que sur les conclusions déjà dressées sur la non-conformité à l'obligation d'information pour conclure à l'inexistence du consentement éclairé[204].

88. Le renforcement de la transparence paraît *a priori* être une révolution dans le cadre de la protection des données à caractère personnel. Or, tel n'a pas été le cas : la transparence telle qu'envisagée par le RGPD est la traduction d'une évolution historique de l'importance accordée à l'information de la partie faible. Initialement, l'obligation d'information n'avait été envisagée que dans sa nature de fin. En effet, l'article 3 de la loi informatique et libertés dans sa version de 1978 – loi pour laquelle la notion de consentement était circonscrite aux traitements de données présentant un caractère sensible – disposait alors :

> « Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés »[205].

89. Si, historiquement, l'obligation d'information remonte au moins à la loi des XII Tables à Rome[206], l'obligation d'information a été remise en exergue au milieu du XXe siècle par « un

---

[201] DABOSVILLE Benjamin, *L'information du salarié. Contribution à l'étude de l'obligation d'informer*, Paris, Dalloz, Nouvelle Bibliothèque de Thèses, volume 123, 2013, p. 12.
[202] PEREZ-RUBIO Lourdes Blanco, « La liberté personnelle de consentement : fondement éthique et juridique », *in Des liens et des droits, Mélanges en l'honneur de Jean-Pierre Laborde*, Paris, Dalloz, 2015, p. 800.
[203] CNIL, Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.
[204] *Ibidem.*
[205] Loi n°78-17 du 6 janvier 1978, Article 3.
[206] BERNHEIM-DEVAUX Sabine, « Le droit de la consommation, entre protection du consommateur et régulation du marché », *Revue Juridique de l'Ouest*, 2013, p. 46.

courant de pensée plus attentif aux faibles, plus soucieux de réduire les inégalités »[207], qui a eu pour conséquence de modifier « l'équilibre en faveur de celui dont la capacité réelle de s'informer apparaît limitée »[208]. L'obligation d'information se comprenait alors, de la plume même de ses contemporains, comme « l'une des manifestations de cet esprit de solidarité […] par réaction contre l'individualisme excessif du XIXe siècle »[209]. L'obligation d'information a d'ailleurs connu un succès considérable en droit de la consommation à partir des années 1960, le législateur prenant conscience du déséquilibre intellectuel (au sens d'informationnel) entre le consommateur et le professionnel[210]. La redécouverte de l'obligation d'information a alors eu des conséquences sur l'appréhension de la notion de consentement puisque la logique de ce dernier « a, dans certains champs du droit, connu une évolution particulière puisqu'elle s'est vue agrémentée d'une exigence préalable d'information comme dans le droit de la consommation ou dans le droit médical et de l'expérimentation sur les êtres humains »[211].

90. Dans l'ensemble, le consentement éclairé fait principalement l'objet d'une consécration législative. Cependant, dans certaines matières particulièrement sensibles, il a pu faire l'objet de consécrations plus fortes. En droit médical, le consentement s'est élevé à un niveau constitutionnel, voire universel puisque, héritage de la Seconde Guerre mondiale, « la logique du consentement informé a […] été développée à la suite du procès de Nuremberg ayant révélé les atrocités commises pendant la guerre sur certains prisonniers des camps de concentration »[212]. Dans le domaine médical, l'obligation d'information préalable au recueil du consentement éclairé a été consacrée au nom de la dignité humaine :

> « L'obligation médicale d'information ressortit à la protection de la dignité de la personne humaine. Elle est le corollaire, ou plutôt le préalable de l'obligation de recueillir le consentement du patient, obligation qui sans elle n'aurait pas de sens. Quelle valeur aurait un consentement qui ne serait pas éclairé ? »[213]

En ce sens, les Cours suprêmes nationales se sont attachées à élever le droit à l'information en matière médicale à un niveau supralégislatif. En France, il faudra attendre 2001 pour que la première chambre civile de la Cour de cassation lie expressément l'information médicale à un principe constitutionnel en affirmant que l'obligation d'information du médecin

---

[207] TERRÉ François, SIMLER Philippe, LEQUETTE Yves, *Les obligations*, 10 éd., Dalloz, 2009, n°259, p. 268.
[208] *Ibidem.*
[209] DE JUGLART Michel, « L'obligation de renseignements dans les contrats », *RTD civ.* 1945.1 et s.
[210] BERNHEIM-DEVAUX Sabine, « Le droit de la consommation, entre protection du consommateur et régulation du marché », *Revue Juridique de l'Ouest*, 2013, p. 46
[211] LAZARO Christophe, LE MÉTAYER Daniel, *op. cit.*, p. 775.
[212] LAZARO Christophe, LE MÉTAYER Daniel, *op. cit.*, p. 777.
[213] CHABAS François, « L'obligation médicale d'information en danger », JCP 2000. I. 212.

envers son patient « trouve son fondement dans l'exigence du respect du principe constitutionnel de sauvegarde de la dignité de la personne »[214]. Ce mouvement est aussi présent à l'étranger, comme le montre l'exemple espagnol où le tribunal suprême espagnol a fait du consentement éclairé un « droit humain fondamental, précisément l'un des derniers apports réalisés dans la théorie des droits humains, une conséquence nécessaire ou une explication des droits classiques à la vie, à l'intégrité physique et à la liberté de conscience »[215].

91. Le consentement éclairé a aussi une importance toute particulière en droit de la consommation, ce qui est d'autant plus important pour la protection des données à caractère personnel dans la mesure où celle-ci est aussi parfois envisagée sous le prisme de la protection du consommateur. Ce point de vue est très présent dans le droit américain pour lequel l'ensemble de la protection des données à caractère personnel face aux acteurs privés est contrôlé par la *Federal Trade Commission* (FTC), qui est une commission s'intéressant au droit de la concurrence et de la consommation. Cette commission assimile la personne concernée à un consommateur dont le consentement éclairé doit être protégé par le droit de la consommation. Ainsi, après avoir étudié les législations américaine, canadienne et européenne, la *Federal Trade Commission* a considéré que « le principe le plus fondamental est l'information préalable »[216], dans la mesure où sans information, le consommateur n'était pas capable de prendre une décision informée sur le traitement de ses données à caractère personnel.

92. L'obligation d'information a aussi été consacrée en économie en tant que préalable indispensable au bon fonctionnement du marché. Par exemple, la crise de 2008 a notamment mis l'accent sur la nécessité d'une plus grande transparence dans le domaine bancaire, car il a été démontré que non seulement « les banques qui ne peuvent pas communiquer efficacement sur leur situation financière peuvent être amenées à choisir un monitoring plus faible »[217], mais aussi « les détenteurs de dette subordonnée pourraient ne pas être capables d'évaluer correctement le risque de la banque en raison d'un manque d'information ou de l'opacité bancaire » [218].

---

[214] Cass, Civ. 1e, 9 octobre 2001, n°00-14.

[215] « *El consentimiento informado constituye un derecho humano fundamental, precisamente una de las últimas aportaciones realizada en la teoría de los derechos humanos, consecuencia necesaria o explicación de los clásicos derechos a la vida, a la integridad física y a la libertad de conciencia* ». Tribunal Supremo, Sala de lo Civil, 12/01/2001, *Jose Manuel Martinez-Pereda Rodriguez*, n°3688/1995.

[216] « *the most fundamental principal is notice* ». Federal Trade Commission, *Privacy Online: A report to Congress*, 1998, available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf

[217] DISTINGUIN Isabelle, « Discipline de marché par la dette subordonnée : Impact de l'opacité bancaire et des politiques de renflouement des banques », *Revue Économique*, vol. 70, no. 2, 2019, pp. 207-228, disponible sur www.jstor.org/stable/26632000 (consulté en octobre 2020).

[218] *Ibidem.*

93. En matière de protection des données à caractère personnel, il a été énoncé que « sans politiques de protection des données, les entreprises détiennent l'ensemble de l'information et les consommateurs aucune, ce qui entraîne une asymétrie de l'information [qui est] l'une des causes potentielles d'une défaillance du marché »[219]. Ainsi, l'obligation d'information est importante pour le bon fonctionnement du marché, et ce, à deux égards. Premièrement, l'obligation d'information permet aux produits et services d'être correctement évalués sur le marché[220]. Deuxièmement, l'obligation d'information rétablit la confiance entre les parties puisqu'elle permet aux consommateurs d'évaluer les risques du produit qu'ils achèteront, et par extension, les personnes concernées pourront évaluer les risques inhérents au choix qu'ils ont à effectuer[221]. Cette dernière affirmation est importante pour l'économie numérique, car il a été démontré que « la loyauté d'un individu envers un site internet est étroitement liée au niveau de confiance » [222] que l'individu octroie au site internet.

94. Derrière la notion de consentement éclairé se trouve la volonté de recueillir un consentement valable et suffisamment informé pour que la personne concernée ait un réel contrôle sur ses données à caractère personnel. Une telle volonté implique que la personne concernée soit en mesure de comprendre les conséquences de ses choix sur sa propre protection[223]. Cependant, le législateur souhaitant garantir un consentement éclairé se retrouve confronté à la pratique, la collecte des données à caractère personnel étant une activité très lucrative. C'est ainsi que le bilan que la FTC dresse de la législation américaine en 2010 a fatalement trouvé un écho au sein de l'Union européenne : « les individus manquent souvent d'une information complète sur les conséquences complètes de la divulgation de leurs informations ainsi que sur les mécanismes permettant de s'assurer que leurs informations sont divulguées de la manière qu'ils souhaitent »[224]. En 2011, l'Eurobaromètre a démontré que les efforts en termes d'information devaient se poursuivre. En effet, bien que 49% des personnes ayant répondu à ce sondage aient affirmé qu'ils se sentaient suffisamment informés par les

---

[219] « Without privacy policies, companies have all of the information about their own practices and consumers have none, leading to an information asymmetry. Information asymmetries are one potential cause of market failure. ». MCDONALD Aleecia, FAITH CRANOR Lorrie, « The Cost of Reading Privacy Policies », *I/S: A Journal of Law and Policy for the Information Society*, 2008, p. 5.

[220] « an individual's loyalty to a web site is closely linked to the levels of trust ». *Ibidem.*

[221] *Ibidem.*

[222] BENNETT Colin J., RAAB Charles D., *The governance of privacy: Policy instruments in global perspective*. Routledge, 2017, pp. 611-612.

[223] REIDENBERG, Joel R *et al.*, *op. cit.*

[224] « individuals often lack complete information about the consequences of information disclosure as well as mechanisms for ensuring that their information is disclosed only in the way they desire ». *Ibidem.*

réseaux sociaux, 46% d'entre eux ont affirmé le contraire[225]. La France faisait partie des pays les plus sceptiques quant à l'information délivrée par les réseaux sociaux quant à l'exploitation de leurs données à caractère personnel puisque 61% des Français ayant répondu à ce sondage ont affirmé de pas être suffisamment informés contre 35% exprimant l'opinion contraire[226].

95. La seule obligation d'informer les personnes concernées de l'utilisation de leurs données à caractère personnel à travers une politique de confidentialité n'est donc pas suffisante : l'absence de précision a d'ailleurs été regrettée sous le règne de la directive 95/46/CE, mais aussi à propos d'autres législations ayant une obligation similairement vague. La faible effectivité de ces mesures a nourri les opposants à la protection des données à caractère personnel, qui finalement ont mis en exergue les principales pistes d'amélioration attendues pour garantir aux individus une information utile à la prise de décision. Par exemple, le praticien Kent Walker[227], en discutant du coût du droit à la vie privée (*privacy*) adressait de nombreuses critiques aux politiques de confidentialité : excessives tant dans leur longueur que dans leur complexité, contenant souvent des considérations peu pertinentes pour la majorité des personnes concernées, opaques, non comparables et peu flexibles pour les entreprises[228]. Les législateurs européens ont constaté l'ensemble des difficultés rencontrées sous l'égide de la directive 95/46/CE[229] et ont, à travers le RGPD, voulu renforcer le consentement éclairé aussi bien au niveau des exigences de forme que de fond.

96. Ce constat désormais dressé, le problème a été étudié lors de l'analyse d'impact accompagnant la proposition de Règlement sur la protection des données (RGPD). En effet, pour répondre au problème résultant des difficultés pour les individus d'exercer leur droit à la protection des données à caractère personnel de manière effective, l'analyse d'impact a proposé des idées d'amendements renforçant la responsabilité des responsables de traitements, dont l'obligation pour le responsable de traitement de fournir un certain nombre d'informations obligatoires à la personne concernée d'une manière intelligible, à travers l'utilisation d'un

---

[225] Commission européenne, « Attitudes on Data Protection and Electronic Identity in the European Union », *Rapport*, Special Eurobarometer 359, juin 2011.
[226] *Ibidem*.
[227] En 2001, encore vice-président d'eBay. Aujourd'hui, vice-président aux affaires générales et chef des affaires juridiques de Google.
[228] WALKER Kent, « The Costs of Privacy », *Harvard Journal of Law and Public Policy*, vol. 25, 2001, p. 87
[229] Pour ne citer qu'un exemple, lors des débats en première lecture, le député européen Carl Schlyter rappelait que « si vous allez lire toutes les clauses du contrat sur les applications, programmes et autres que vous utilisez, cela vous prend 180 heures par an » [traduction libre]. Parlement européen, *Protection of individuals with regard to the processing of personal data – processing of personal data for the purpose of crime prevention (debate)*, Strasbourg, 11 mars 2014, CRE 11/03/2014 – 13, 2012/0011 (COD).

vocabulaire clair et simple[230]. L'obligation d'information se voit donc revêtue de deux obligations, différentes dans leurs effets, bien que similaires dans le contenu.

97. D'une part, l'obligation d'information permet à la personne concernée d'être avertie de tout traitement de données à caractère personnel, peu importe la base légale choisie pour fonder ce traitement. Ainsi, même en dehors de tout consentement, le traitement sera conforme au RGPD uniquement dans la mesure où la personne concernée aura eu une connaissance suffisamment complète de celui-ci. Par conséquent, la personne concernée aura la possibilité de contester un tel traitement, par exemple si elle estime que le traitement n'est pas nécessaire à l'exécution d'un contrat ou à l'exercice d'une mission de service public. Cette obligation a aussi comme objectif d'interdire les traitements de données à caractère personnel à l'insu de la personne concernée, un objectif d'autant plus important que les technologies de captation, potentiellement « invisibles » sont de plus en plus développées : vidéosurveillance, vidéoprotection, reconnaissance faciale, reconnaissance vocale, etc. Sur internet, cette obligation aura notamment permis de rendre visible l'utilisation de plus en plus généralisée du dépôt de *cookies* sur le terminal des personnes concernées[231]. Un manquement à l'obligation d'information sera ainsi qualifié de « manquement aux obligations de transparence et d'information telles que prévues par les articles 12 et 13 »[232] du RGPD.

98. D'autre part, la qualité de l'obligation permettra de juger de la validité ou non du consentement, qui se doit d'être éclairé. Dans ce cadre, l'obligation d'information n'est pas uniquement une obligation à la charge du responsable de traitement, mais également une condition nécessaire à la validation de la base légale du traitement. Ainsi, un manquement à l'obligation d'information sera non seulement un manquement aux articles 12 et 13 du RGPD, mais entraînera également un défaut de base légale au sens de l'article 6 du RGPD, dans la mesure où le manquement invalidera le consentement.

99. Ainsi, le consentement éclairé est garanti par le droit à la transparence, dont l'effectivité va dépendre à la fois de considérations relatives à la forme de l'information et au fond. Dans ce cadre, les obligations de forme permettent de renforcer l'accessibilité à l'information (Chapitre 1) et des obligations de fond permettent de délivrer suffisamment d'information pour que

---

[230] Commission européenne, *Impact Assessment*, SEC/2012/0072 final, *op. cit.*

[231] NETTER Emmanuel, « Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls », *in* NETTER Emmanuel (dir.), *Regards sur le nouveau droit des données personnelles*, CEPRISCA, Collection Colloques, pp. 19-20, disponible sur HAL : https://hal.archives-ouvertes.fr/hal-02357967/document (consulté en janvier 2021).

[232] CNIL, Délibération de la formation restreinte du 21 janvier 2019, *op. cit.*

l’individu soit en mesure d’une part de faire un choix éclairé et d’autre part d’exercer ses droits s’il estime qu’il a été lésé (Chapitre 2).

CHAPITRE 1 – LES CONDITIONS FORMELLES ATTACHÉES À L'OBLIGATION D'INFORMATION

100. La volonté du législateur européen d'améliorer les conditions formelles attachées à l'obligation d'information de la personne concernée afin que celle-ci accède réellement à l'information découle du bilan de l'application de la directive 95/46/CE. De nombreuses critiques se sont en effet élevées contre le mécanisme du consentement, du fait que les utilisateurs ne remarquaient pas, ne lisaient pas ou ne comprenaient pas les politiques de confidentialité des différents services qu'ils utilisaient en ligne[233]. Saisi par la sphère académique, le sujet a fait l'objet de nombreuses études cherchant l'explication du phénomène.

101. Le manque d'accessibilité des informations destinées à la personne concernée a alors été mis en exergue. Notamment, deux chercheurs américains ont, en 2004, analysé soixante-quatre politiques de confidentialités d'entreprises américaines afin d'en déterminer leur niveau de lisibilité[234] selon le *Flesch Reading Ease Score*[235]. Leurs résultats ont montré un manque d'accessibilité de l'information puisque seulement 6% des politiques de confidentialité étudiées étaient suffisamment accessibles pour une personne ayant un niveau de lycée ou moins tandis que 54% étaient accessibles à une population ayant l'équivalent de quatorze années d'études et 13% étaient accessibles à une population ayant fait des études après le master[236]. Si l'évaluation de la capacité de compréhension selon le niveau d'étude doit être maniée avec précaution dans la mesure où elle se fonde sur des données sociologiques américaines et des données linguistiques de langue anglaise, l'étude nous fournit toutefois une indication pertinente quant à la difficulté de lecture des politiques de protection des données à caractère personnel.

102. Le RGPD s'inscrit dans ce double constat puisqu'il va, d'une part, améliorer la délivrance de l'information (Section 1) et d'autre part, chercher à adapter l'information au public cible (Section 2).

---

[233] REIDENBERG, Joel R *et al.*, *op. cit.*

[234] JENSEN Carlos, POTTS Colin, « Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices », *in* DYKSTRA-ERICKSON Elizabeth, TSCHELIGI Manfred (dir.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 471-478.

[235] Le *Flesh Reading Ease Score* est une formule mathématique proposée par Rudolf Flesh, qui permet d'évaluer la lisibilité d'un texte en anglais. La formule prend en compte le nombre de mots, le nombre de syllabes, le nombre de phrases, le nombre moyen de syllabes par mot et le nombre moyen de mots par phrase. FLESCH Rudolf, « How to Write Plain English. Chapter 2: Let's Start With the Formula », disponible sur https://web.archive.org/web/20160712094308/http://www.mang.canterbury.ac.nz/writing_guide/writing/flesch.shtml (consulté en octobre 2020).

[236] JENSEN Carlos, POTTS Colin, *op. cit.*, pp. 471-478.

Section 1 – L'amélioration de la délivrance de l'information

103. La transparence est largement louée pour ses vertus permettant aux acteurs externes d'une entreprise (consommateurs, investisseurs, organisations non gouvernementales (ONGs)) de se mobiliser, instaurant ainsi une relation de confiance avec l'entreprise s'essayant à l'exercice de la transparence[237]. En matière de protection des données à caractère personnel, la confiance des personnes concernées semble directement dépendre de la protection et du contrôle perçus par les personnes concernées sur leurs données à caractère personnel[238]. Fortement intégrée à la stratégie déployée par la Commission européenne en matière de maché numérique européen[239], l'objectif de confiance a conduit le législateur européen à pleinement intégrer la transparence au sein du RGPD.

104. Le RGPD envisage la transparence sous le paradigme de l'*empowerement* : la transparence vise à octroyer à la personne concernée le pouvoir d'exercer un contrôle sur ses données à caractère personnel, notamment lorsqu'elle émet ou non son consentement. La délivrance de l'information prend alors toute son importance, puisque la personne concernée ne peut exercer un tel contrôle que si elle est capable de comprendre l'information ainsi délivrée. Ainsi, la transparence transcende sa nature d'obligation à la charge du responsable de traitement pour devenir un droit au profit de la personne concernée (§1).

105. L'objectif de garantir à la personne concernée le contrôle de ses données à caractère personnel à travers la transparence de leur traitement devient dès lors un objectif à atteindre pour le responsable de traitement, dans une logique de *compliance.* En effet, le responsable de traitement est responsable de la mise en pratique de l'exigence d'accessibilité de l'information (§2).

---

[237] MARES Radu, « Corporate transparency laws : A hollow victory ? », *Netherlands Quartely of Human Rights*, 2018, Volule 36, Issue 3, p. 193.

[238] Par exemple, la Commission européenne affirme que « la confiance dans le monde en ligne suppose aussi d'aider les consommateurs à exercer un meilleur contrôle sur leurs propres données et leur identité et à assumer une responsabilité accrue à cet égard ». Commission européenne, *Façonner l'avenir numérique de l'Europe*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Bruxelles, 19 février 2020, COM(2020) 67 final, p. 12.

[239] Commission européenne, COM(2020) 66 final, *op. cit.* p. 30 ; Commission européenne, COM(2012) 11 final, *op. cit.*, §1 ; Commission européenne, COM(2020) 264 final, *op.cit.*, p. 2 ; Commission européenne, « La Commission propose des mesures pour stimuler le partage des données et soutenir les espaces européens de données », *op. cit.*

§1 – Le renforcement des modalités d'accès à l'information : d'une obligation de transparence à un droit à l'information

106. L'adjectif « accessible » se définit couramment comme ce « dont l'accès est possible ou facile »[240]. Le terme « accessibilité » désigne quant à lui les démarches visant à rendre plus facile – ou moins difficile – l'accès à certains objets. Par exemple, le terme « accessibilité » est fréquemment employé pour désigner les procédés mis en place dans l'objectif de garantir plus simplement l'accès aux lieux, équipements et fonctions des personnes en situation de handicap. Ainsi, la démarche d'accessibilité présuppose l'identification d'une difficulté d'accès ainsi que la définition et la mise en place de correctif permettant de pallier la difficulté.

107. Lorsqu'il s'agit de protection et surtout d'accès à l'information, le caractère accessible signifie généralement la facilité de l'accès. Plusieurs textes viennent d'ailleurs préciser le caractère « facilement accessible » de l'information[241]. En matière de protection des données à caractère personnel, le caractère facile de l'accès à l'information est mis en exergue de façon très explicite par le considérant 39[242] et par l'article 12 du RGPD qui requière une information « concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples »[243]. La loi informatique et libertés procède à un renvoi aux articles 12 et 14 du règlement quant aux conditions d'exercice du « droit à l'information », tout en précisant que l'information collectée auprès d'un mineur de moins de quinze ans doit faire l'objet d'une information « dans un langage clair et facilement accessible »[244]. Ainsi, le responsable de traitement est tenu de rendre la délivrance de l'information accessible à la personne concernée, à la fois dans son choix du moyen de délivrance d'information (A) que dans son implémentation (B).

A. L'exigence d'accessibilité centrée sur la personne concernée

108. Le renforcement des dispositions relatives à la transparence en matière de protection des données à caractère personnel est la conséquence du recentrage de la protection sur la personne concernée. La personne concernée devient le destinataire des informations relatives au

---

[240] CNRTL, « Accessible », *CNRTL.fr*, Lexicographie, disponible sur https://www.cnrtl.fr/definition/accessible

[241] Ministère de la santé, de la famille et des personnes handicapées, Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, Journal officiel du 17 mars 2004, n°65, pp. 5206-5209.

[242] Le considérant 39 dispose : « Le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre et formulées en des termes clairs et simples »[242]. RGPD, 27 avril 2016, considérant 39.

[243] RGPD, 27 avril 2016, article 12(1).

[244] Loi n°78-17 du 6 janvier 1978, article 48 tel que modifié par l'article 9 de la loi n°2021-998 du 30 juillet 2021.

traitement de ses données à caractère personnel, dont elle doit être capable de s'emparer pour exercer un contrôle sur ces traitements.

109. L'exigence d'accessibilité contenue dans le RGPD peut dès lors se comprendre comme la traduction du passage d'un régime centré sur l'autorisation administrative à un régime centré sur la personne concernée (1). Cependant, la personne concernée reste la personne vulnérable dans sa relation avec le responsable de traitement : ce dernier se voit donc imposer un cahier des charges poursuivant l'objectif de sortir effectivement la personne réelle de l'asymétrie d'information qu'elle détient sur le traitement de ses données à caractère personnel. Pour se faire, le législateur européen a dessiné un cahier des charges de l'obligation de transparence, dont le référentiel d'évaluation est la personne concernée (2).

1. *L'accessibilité, traduction d'un régime d'autorisation administrative à un régime centré sur la personne concernée*

110. L'exigence d'accessibilité de l'information apparaît dans les lignes directrices régissant la protection de la vie privée, traditionnellement considérées comme le premier instrument international en matière de protection des données[245]. Le principe de transparence inscrit en son 1.2 disposait notamment qu'il « devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel des activités »[246]. Le verbe « procurer » impliquait alors pour la personne concernée de « faire en sorte »[247] d'avoir ces informations à sa disposition, et donc d'adopter une démarche active vis-à-vis de l'information. La même philosophie semble parcourir la Convention 108 du Conseil de l'Europe, dans sa version originale, qui disposait que « toute personne doit pouvoir connaître l'existence d'un fichier automatisé de données à caractère personnel, et ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier »[248]. L'utilisation du verbe pouvoir plutôt que de devoir présume de la nécessité pour la personne concernée d'être capable de trouver facilement l'information si elle la cherche.

111. En 1995, la directive 95/46/CE crée à la charge du responsable du traitement une obligation quant à l'identité du responsable de traitement, les finalités du traitement et des informations supplémentaires si « ces informations sont nécessaires pour assurer à l'égard de

[245] OCDE, *op. cit.*
[246] OCDE, *op. cit.*
[247] CNRTL, « Procurer », *CNRTL.fr*, Lexicographie, disponible sur https://www.cnrtl.fr/definition/procurer
[248] Convention 108, 28 janvier 1981, Article 8(a).

la personne concernée un traitement loyal des données »[249]. L'information devient ainsi une obligation à la charge du responsable du traitement, mais ses modalités quant à son accessibilité par la personne concernée ne sont pas prises en compte. L'information n'est pas encore considérée comme un droit à l'information de la personne concernée. Tout juste, la Cour de justice considère que l'exigence d'information « est une condition nécessaire à l'exercice par ces personnes de leur droit d'accès et rectification des données traitées »[250].

112. La nature hybride obligation-droit du principe de transparence apparaît dans les discussions officielles dans les années 2000. Les Résolutions de Sydney et de Madrid de la Conférence des commissaires à la protection des données sont symptomatiques de cette transition. Ces résolutions viennent dessiner le contour de ce qui sera plus tard le principe de transparence, à travers l'obligation d'information « de façon adéquate »[251] c'est-à-dire « dans une forme intelligible, utilisant un langage clair et simple »[252]. En 2010, la Commission européenne regrettera, dans sa communication relative à l'approche de la protection des données à caractère au sein de l'Union européenne, que « les dispositions applicables relatives aux informations à communiquer à la personne concernée sont insuffisantes », entraînant l'apparition de politiques de confidentialités difficilement accessibles et peu transparentes[253]. La Commission révèle à cette occasion sa volonté de renforcer le principe de transparence à travers « un accès aisé à l'information, qui doit être facile à comprendre et l'utilisation d'un langage clair et simple »[254], initiative saluée par le Parlement européen[255] et le Contrôleur européen de la protection des données[256]. Ces réflexions aboutissent finalement à la proposition de Règlement sur la protection des données de la Commission européenne, dont l'étude d'impact affirme que l'un des objectifs du RGPD est d'accroître la transparence des traitements

---

[249] Directive 95/46/CE, 24 octobre 1995, articles 10 et 11.
[250] CJUE, 3e ch., 1e octobre 2015, *Smaranda Bara e.a.*, C-201/14, §33 ; Conclusions de l'avocat général M. Pedro RUZ VILLALÓN, *Smaranda Bara e.a.*, C-201/14, présentées le 9 juillet 2015, §74.
[251] Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), *Résolution sur des normes internationales de vie privée*, Madrid, 4-6 novembre 2009, 31e Conférence, point 2(a)
[252] [252] Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), *Résolution sur des normes internationales de vie privée*, Madrid, 4-6 novembre 2009, 31e Conférence, article 10(5) ; Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), *Resolution on improving the communication of data protection and privacy information practices*, Sydney, 12 septembre 2003, points 2 et 5.
[253] Commission européenne, COM(2010) 609 final, *op. cit.*, §2.1.2.
[254] *Ibidem.*
[255] Parlement européen, *Rapport sur une approche globale de la protection des données à caractère personnel dans l'Union européenne*, Commission des libertés civiles, de la justice et des affaires intérieures, 22 juin 2011, A7-0244/2011, p. 9.
[256] EDPS, *Avis du contrôleur européen des données sur la communication de la Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée – « Une approche globale de la protection des données à caractère personnel dans l'Union européenne »*, 2011/C, 181/01, point 73.

de données à caractère personnel dans la perspective de donner le pouvoir aux personnes concernées sur leurs données à caractère personnel[257].

2. L'accessibilité, obligation évaluée du point de vue de la personne concernée

113. Le RGPD désormais adopté, le principe de transparence « trône aujourd'hui en majesté »[258]. Intégré à la démarche de *compliance,* le principe de transparence dépasse la simple délivrance d'informations déterminées à la personne concernée au profit du « souci d'être en conformité, à l'instar d'un remodelage intégral d'un parcours utilisateur pour garantir une parfaite transparence […] ayant aussi pour objectif de faire en sorte que cette information est également accessible, claire, simple et concise »[259]. Intégré à la démarche d'*empowerment,* le principe de transparence reconnaît la vulnérabilité de la personne concernée et propose d'évaluer l'accessibilité de l'information du point de vue de la personne concernée, qui « doit être aidée, accompagnée pour traduire ce qui se joue derrière chaque finalité »[260]. La prise en compte de la « faiblesse intrinsèque » de la personne concernée se justifie ainsi au regard de l'asymétrie d'information entre la personne concernée et le responsable de traitement, notamment face aux techniques commerciales agressives ou suggestives mises en place sur le marché intérieur[261]. Ainsi, l'obligation d'information est considérablement étoffée, le législateur ne se contentant plus d'une simple délivrance de l'information par le responsable de traitement, mais veillant au contraire à ce que la personne en soit effectivement la destinataire et puisse en prendre connaissance[262] .

114. Dès lors, le RGPD a considérablement étoffé l'obligation d'information en assignant au responsable de traitement un cahier des charges plus précis : désormais, l'information doit être délivrée « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples »[263]. Le texte du RGPD est cependant neutre quant aux modalités de délivrance de l'information, l'article 12 se bornant à mentionner que « les informations sont

---

[257] Commission européenne, *Impact Assessment*, SEC/2012/0072 final, *op. cit.*, p. 43.
[258] NETTER Emmanuel, « À quoi sert le principe de transparence en droit des données personnelles ? », *Dalloz IP/IT*, novembre 2020, n°11, p. 611.
[259] PERRAY Romain, « Les outils de la conformité au RGPD : des outils de valorisation », *Revue des affaires européennes*, 2021/1, p. 45.
[260] EYNARD Jessica, « RGPD « empouvoirement » individuel : promesse tenue ou espoir déçu ? », *Revue des affaires européennes*, 2021/1, p. 20.
[261] Cour de cassation italienne, Cass Civ., Sec. I, 2 juillet 2018, *Newsletter, e-mail pubblicitarie e consenso,* 17278/2018.
[262] BRUNEAU Laurent, *Contribution à l'étude des fondements de la protection du contractant,* Thèse pour l'obtention du grade de docteur en droit sous la direction de ROZÈS Louis, 2005, Université des sciences sociales de Toulouse, p. 392.
[263] RGPD, 27 avril 2016, Article 12(1).

fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique »[264]. Si la forme de délivrance de l'information reste généralement libre, cette information doit tout de même présenter des caractéristiques visant à garantir l'accessibilité de l'information par la personne concernée. Le responsable de traitement doit dès lors veiller à activement délivrer l'information à la personne concernée, sur le même canal que celui utilisé pour collecter ses données à caractère personnel et de manière lisible.

115. L'exigence de délivrance active de l'information à la personne concernée signifie que celle-ci doit avoir accès à l'information sans avoir à fournir d'efforts préalables. Le G29 rappelle dans ses lignes directrices relatives à la transparence que « la personne concernée ne devrait pas à rechercher les informations, mais devrait pouvoir tout de suite y accéder »[265]. Ainsi, l'information doit être directement communiquée à la personne concernée à l'aide d'un canal adapté. Selon le G29, le terme « fournir » l'information à la personne concernée signifie que « le responsable de traitement doit prendre des mesures concrètes pour fournir les informations en question à la personne concernée ou pour diriger activement la personne concernée vers l'emplacement desdites informations »[266]. Notamment, l'emplacement et l'accès à l'information doivent être clairement indiqués tout au long de la navigation de la personne concernée sur le site internet : le G29 considère en effet qu'un lien vers la politique de protection des données « doit être clairement visible sur chaque page [du site internet] sous un terme communément utilisé »[267]. Le G29 prohibe toute manipulation du texte visant à rendre moins visible les textes ou liens vers la politique de protection des données à caractère personnel à travers, par exemple, un choix de mise en page ou de couleur inopportun[268].

116. La délivrance de l'information doit aussi répondre à des exigences de lisibilité, qui s'étendent au-delà du contenu de l'information. En effet, le responsable de traitement se doit d'utiliser un canal d'information permettant une lecture la plus lisible possible de l'information. Comme le rappellent Aurélie Banck et Catherine Schultis,

> « Le défi de l'information dans le cadre du RGPD réside dans son caractère lisible. Il faut adresser le bon message au bon moment et utiliser, pour se faire, l'ensemble des canaux (« pop-

[264] RGPD, 27 avril 2016, Article 12(1).
[265] Groupe de travail « Article 29 », *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679,* adoptées le 29 novembre 2017, version révisée et adoptée le 11 avril 2018, WP260 rev. 01, p. 21.
[266] *Ibidem.*
[267] *Idem*, p. 8.
[268] *Idem*, p. 9.

> up » et page dédiée dans l'espace client, page du site Web, voir site dédié, charte, *privacy notice,* etc.) et des modes de communication disponibles (collective et individuelle) »[269].

Cette exigence se justifie aisément par les études attribuant la raison pour laquelle les personnes concernées ne lisent pas les politiques de protection des données à caractère personnel à l'absence de lisibilité de ces dernières (par exemple, à cause du format utilisé ou de la taille de la police)[270].

117. L'exigence de lisibilité peut aboutir à un contrôle très pragmatique du moyen de délivrance choisi par le responsable de traitement. Par exemple, le Règlement dispose que si le responsable de traitement choisit de communiquer les informations relatives au traitement de données à caractère personnel grâce à un document accompagné d'icônes, ces dernières devront être lisibles par machines si elles sont présentées par voie électronique[271]. Les autorités de contrôle exerceront un contrôle *in concreto* aussi bien sur la forme choisie par le responsable de traitement pour délivrer l'information que sur l'exécution de celle-ci. C'est ainsi que le Conseil d'État et la CNIL ont tous deux condamné la société Google non pas sur la forme choisie pour délivrer l'information (l'information multiniveaux), mais sur l'exécution de celle-ci aboutissant à un éparpillement trop complexe de l'information[272] : la personne concernée n'avait pas un accès immédiat à l'information. En effet, le caractère immédiat de l'accès à l'information a été pensé pour encourager les personnes concernées à lire l'information qui leur est délivrée à propos du traitement de leurs données à caractère personnel. Le caractère immédiat de l'accès à l'information englobe aussi bien l'accessibilité au canal d'information que l'accessibilité de l'information au sein du canal.

118. De plus, en sus d'un canal d'information accessible, la personne concernée doit être capable d'accéder rapidement à l'information au sein même du canal. En effet, il a été suffisamment démontré que « si le coût de lecture des politiques de protection de la vie privée est trop élevé, les personnes concernées sont peu susceptibles de lire ces politiques »[273]. Dans le cas de la protection des données à caractère personnel, ce coût est principalement évalué en

---

[269] BANCK Aurélie, SCHULTIS Catherine, *Vade-mecum de la protection des données personnelles pour le secteur bancaire et financier,* RB édition, Les essentiels de la banque et de la finance, 2018, p. 59.
[270] MILNE George R., CULNAN Mary J., « Strategies for Reducing Online Privacy Risks: Why Consumer Read (or Don't Read) Online Privacy Notices », *Journal of Interactive Marketing*¸2004, 18(3), p. 24.
[271] Article 12(7) du RGPD.
[272] CNIL, « La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société Google LLC », disponible sur https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la (consulté en septembre 2020) ; CE, 10e et 9e chambres réunies, 19 juin 2020, n°430810, *Société Google LLC*, cons. 23.
[273] « *If the cost for reading privacy policies is too high, people are unlikely to read policies* », MCDONALD Aleecia, FAITH CRANOR Lorrie, *op. cit.*, p. 548.

termes de temps. De nombreuses études ont démontré que la raison principale pour laquelle les personnes concernées ne lisaient pas les politiques de protection des données à caractère personnel était que ces politiques étaient trop longues et que leur lecture était par conséquent trop chronophage[274]. L'étude désormais célèbre de Aleecia M. McDonald et Lorrie Faith Cranor[275] avait à ce propos démontré que si un internaute américain lisait les politiques de protection des données de chaque nouveau site qu'il visitait, il devrait y consacrer une moyenne de quarante minutes par jour, ce qui représente un investissement bien trop lourd à la charge de la personne concernée.

119. Conscient de ces difficultés, le Groupe de travail « Article 29 » a proposé une interprétation du RGPD visant à remédier au coût trop élevé de la lecture des données à caractère personnel :

> « L'exigence que la fourniture d'informations aux personnes concernées et que les communications qui leur sont adressées soient réalisées d'une manière « concise et transparente » signifie que les responsables du traitement devraient présenter les informations/communications de façon efficace et succincte afin d'éviter de noyer d'informations les personnes concernées »[276].

Ainsi, le Groupe de travail « Article 29 » insiste sur le fait que l'obligation d'information des personnes concernées est une obligation de résultat que ce soit dans la délivrance de l'information à la personne concernée que dans l'accessibilité de ces informations à la personne concernée. Cette obligation s'applique tout au long de la relation entre la personne concernée et le responsable de traitement.

120. L'ensemble des critères érigés par le RGPD et les autorités de contrôle, ainsi que l'appréciation *in concreto* de ces critères, protègent ainsi la personne concernée contre des pratiques auparavant dénoncées comme incompatibles avec le consentement éclairé. Par exemple, la pratique consistant à inclure la politique de la confidentialité au sein des conditions générales d'utilisation noyait la personne concernée dans un flux d'information excessif. Dès lors, il n'aurait pas été raisonnable de présupposer que la personne concernée ait pu parcourir et comprendre l'ensemble de ces informations, et donc ait pu émettre un consentement éclairé. Ainsi, l'accessibilité de l'information a pour objectif de centrer la protection des données à caractère personnel sur la personne concernée, afin que celle-ci puisse exercer un contrôle réel sur le traitement de ses données à caractère personnel. L'accessibilité de l'information constitue

---

[274] Voir par exemple MILNE George R., CULNAN Mary J., *op. cit*, pp. 15-29.
[275] MCDONALD Aleecia, FAITH CRANOR Lorrie, *op. cit.*, pp. 543-568.
[276] Groupe de travail « Article 29 », WP260 rev. 01, *op. cit.*, p. 7.

dès lors une avancée importante du RGPD pour assurer la réalité du consentement, non seulement au moment de sa collecte, mais durant toute la durée du traitement de données à caractère personnel.

B. Une exigence présente durant toute la durée du traitement

121. Le principe de transparence connaît son apogée lors de la collecte des données à caractère personnel de la personne concernée. En effet, la collecte constitue un moment privilégié du principe de transparence, permettant à la personne concernée d'accepter ou refuser la collecte de ses données dans le cadre du traitement de données à caractère personnel envisagé. Cependant, ni le consentement ni les traitements de données à caractère personnel ne sont définitifs : le consentement peut être retiré, le traitement de données à caractère personnel peut faire l'objet de traitements fondés sur d'autres bases juridiques que le consentement, etc. Dès lors, il apparaît indispensable que le principe de transparence soit respecté par le responsable de traitement pendant toute la durée du traitement.

122. Premièrement, l'information doit apparaître dès le début du traitement. Lorsque les données ont été collectées auprès de la personne concernée, le responsable du traitement doit lui fournir les informations « au moment où les données sont obtenues »[277]. Plus particulièrement, pour le consentement, l'information de la personne concernée doit se faire avant l'expression de son consentement afin que ce dernier soit éclairé[278]. Lorsque les données ne sont pas collectées auprès de la personne concernée, l'article 14 dispose que le responsable de traitement fournit les informations « dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées »[279]. Cette hypothèse ne devrait *a priori* pas se présenter en matière de consentement puisque le consentement conditionne la mise en œuvre ou non du traitement.

123. Deuxièmement, il peut arriver que le responsable de traitement modifie sa politique de protection des données à caractère personnel durant la mise en place du traitement auquel la personne concernée a consenti. En cas de modification de la politique de confidentialité de l'entreprise, l'obligation d'obtenir un consentement éclairé ne se limite pas à changer sa politique de confidentialité et d'avertir la personne concernée de ce changement. En effet, la

---

[277] RGPD, 27 avril 2016, Article 13(1) ; CNIL, Délibération de la formation restreinte n°SAN-2020-013 du 7 décembre 2020 concernant la société Amazon Europe Core, §97 et §102
[278] CJUE, 2e ch., 11 novembre 2020, *Orange Romãnia*, C-61/19, §73-74.
[279] RGPD, 27 avril 2016, Article 14(3)(a)

jurisprudence de la CNIL semble impliquer qu'il existe une obligation pour l'entreprise de mettre en exergue ces changements dans la nouvelle politique de confidentialité. Dans l'affaire Google de 2012, la CNIL avait relevé qu'un des changements essentiels de sa nouvelle politique de confidentialité n'apparaissait « qu'au milieu des règles de confidentialité, dans le dernier tiers de la rubrique intitulée Comment nous utilisons les données que nous collectons »[280]. Ainsi, la CNIL avait jugé que cette pratique ne permettait pas de considérer que le consentement à ces changements était valide, car « cette information, alors qu'elle a trait à une modification de la politique de confidentialité de la société, n'est donc pas accessible aux utilisateurs en première intention »[281].

124. Enfin, le principe de transparence implique également un effort du responsable de traitement tout au long de sa relation avec la personne concernée. Ainsi, le principe de transparence s'applique également en matière d'exercice des droits de la personne concernée, comme le dispose l'article 12(4) :

> « Si le responsable du traitement ne donne pas suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel ».

L'autorité de protection des données belge (APD) a précisé la signification du principe de transparence en matière de demandes de référencement et d'effacement. Premièrement, la personne concernée doit être informée des éléments de refus à la demande de droit, même lorsque ces motifs ont été déclarés à l'autorité de protection des données[282]. En l'espèce, un résident belge a adressé à Google une demande de déréférencement, considérant que les contenus visés étaient des contenus attentatoires à son honneur et à sa réputation[283]. Google refuse la demande, en répondant dans les termes suivants : « après examen de l'équilibre entre les intérêts et les droits associés au contenu en question, y compris des facteurs tels que votre rôle dans la vie publique, Google a décidé de ne pas bloquer »[284]. L'APD considère que le motif de refus est « lacunaire » puisqu'il ne permet pas de connaître ou comprendre « complètement »

---

[280] CNIL, Délibération de la formation restreinte n°2013-420 du 3 janvier 2014 prononçant une sanction pécuniaire à l'encontre de la société X.
[281] *Ibidem.*
[282] APD, 17 septembre 2019, décision quant au fond 8/2019 ; DELFORGE Antoine *et al.*, « Chronique de jurisprudence 2018-2020. Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information », *Revue de Droit des Technologies de l'Information (RTDI)*, 2021/1-2, n°82, p. 66.
[283] APD, 14 juillet 2020, décision quant au fond 37/2020.
[284] *Idem*, §165.

la motivation de Google[285]. Ainsi, la réponse négative à une demande de déréférencement doit faire l'objet d'une réponse précise quant au motif de refus, dans une forme compréhensible[286].

125. Les modalités d'accessibilité de l'information ne répondent ainsi pas à un cahier des charges précis quant à la forme de l'accessibilité, mais sont exigeantes en matière de résultat vis-à-vis de la personne concernée. Cette flexibilité a permis aux responsables de traitement d'adapter en pratique la délivrance de l'information au traitement concerné.

§2 – Les pratiques d'accessibilité de l'information

126. Si l'accessibilité à l'information est une obligation de résultat à la charge des responsables de traitement, cette obligation de résultat varie selon les différents traitements de données et le contexte dans lequel ces traitements ont lieu. L'article 12(1) dispose en effet que « le responsable du traitement prend des mesures appropriées pour fournir toute information […] d'une façon concise, transparente, compréhensible et aisément accessible ». L'emploi de termes légaux généraux tels que « mesures appropriées » a certes pu être une difficulté pour les entreprises peu habituées au jargon juridique[287]. Cette formulation permet cependant aux acteurs privés d'adapter l'information au traitement mis en place. Le responsable de traitement est donc invité, voire incité, à fournir des outils adaptés et facilement utilisables de délivrance de l'information, permettant aux personnes concernées de comprendre leurs droits et leurs choix[288].

127. Il n'est pas surprenant que les politiques de protection des données à caractère personnel constituent le média le plus utilisé pour remplir les obligations des articles 12, 13 et 14 du RGPD sur internet, puisque ces politiques permettent de centraliser l'ensemble des mentions d'informations obligatoirement délivrées à la personne concernée tout en ne déployant pas ou très peu de moyens techniques. Ces politiques de protection des données à caractère personnel sont devenues « *de facto,* des tableaux de transparence »[289]. Cependant, des modalités d'accessibilité ont été dégagées en matière de politiques de protection des données à caractère

---

[285] *Idem*, §165.
[286] *Idem*, §165.
[287] AYALA-RIVERA Vanessa, PASQUALE Liliana, « The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements », *2018 IEEE 26th International Requirements Engineering Conference (RE)*, Banff, AB, 2018, pp. 136-146.
[288] Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), *Proposed Resolution on Improving the Communication of Data Protection and Privacy Information Practices*, 25th International Conference of Data Protection & Privacy Commissioners, Sydney, 12 septembre 2003.
[289] TESFAY Welderufael B. *et al*., « PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation », *Fourth ACM International Workshop on Security and Privacy Analytics – IWSPA '18,* Proceedings, p. 15.

personnel afin d'éviter les dérives consistant à noyer la personne concernée dans l'information délivrée (A).

128. En plus des politiques de protection des données à caractère personnel, un responsable de traitement peut utiliser d'autres moyens technologiques de délivrance de l'information, permettant au responsable de traitement soit d'optimiser l'accès à l'information sur les traitements de données à caractère personnel, soit d'adapter l'information aux caractéristiques propres du traitement (B).

A. Les modalités d'accessibilité propres aux politiques de protection des données à caractère personnel

129. Avantageuses du fait qu'elles nécessitent peu de compétences techniques et qu'elles permettent de centraliser l'ensemble des mentions d'informations devant être délivrées à la personne concernée au titre des articles 13 et 14 du RGPD, les politiques de protection des données à caractère personnel sont cependant encadrées et contrôlées par les autorités de contrôle, afin de permettre à la personne concernée de disposer d'un accès effectif à l'information.

130. Pour ce faire, la politique de protection des données à caractère personnel doit, en premier lieu, être isolée de toute autre information légale. Le G29 considère que les informations sur les traitements de données à caractère personnel doivent être « clairement différenciées des autres informations non liées à la vie privée telles que des clauses contractuelles ou des modalités d'utilisation générale »[290]. Par conséquent, la première modalité d'accessibilité propre aux politiques de protection des données à caractère personnel est la création d'un document uniquement dédié à l'information sur les traitements de données à caractère personnel et aux mesures de protection des données qui y sont attachées.

131. De plus, pour répondre à l'ensemble de ces exigences, une des pratiques recommandées par les autorités de protection des données à caractère personnel[291] et répandues au sein des acteurs privés est l'information multiniveaux (ou multistrates). En effet, l'information multiniveaux est pensée pour résoudre le « conflit inhérent entre, d'une part, l'exigence de communiquer aux personnes concernées les informations complètes qui sont requises au titre du RGPD et, d'autre part, l'exigence de le faire de manière concise, transparente,

[290] Groupe de travail « Article 29 », WP260 rev. 01, *op. cit.*, p. 7.
[291] *Ibidem*, p. 7 ; Groupe de travail « Article 29 », *Opinion on More Harmonised Information Provisions*, version proposée le 25 novembre 2004 pour discussion et adoption, 11987/04/EN, WP 100, p. 6.

compréhensible et aisément accessible »[292]. Le fait que l'information multiniveaux ait pour but de remplir l'obligation d'information de la personne concernée en rendant l'information aisément accessible a été rappelé très récemment par la CNIL lors de son avis sur le projet de décret relatif à l'application « StopCovid »[293]. L'information multiniveaux propose une information en plusieurs étapes : une information concise est délivrée en premier lieu, dans une version raccourcie à l'essentiel (« *short notice* »)[294], afin de demander le consentement de la personne concernée. Puis, si cette dernière souhaite avoir plus de détails ou accéder à l'entière politique de confidentialité de l'entreprise, il lui faudra activer un lien prévu à cet effet.

132. Pour identifier les informations essentielles que le responsable de traitement doit fournir en premier lieu à la personne concernée, il est possible de se référer aux opinions des différentes autorités de contrôle. En 2003, lors de la conférence internationale des commissaires à la protection des données (« *International Conference of Data Protection & Privacy Commissionners* »), la résolution incitant les responsables de traitement à délivrer une information multiniveau invitait ces derniers à fournir en premier lieu les informations les plus importantes à savoir pour les personnes concernées ainsi que les informations que les personnes concernées voudraient probablement le plus savoir. À ce titre, le responsable de traitement doit renseigner l'identité et les coordonnées du responsable de traitement, les données collectées, les moyens de collecte des données et les finalités du traitement concernées, les éventuels transferts de données à une personne tierce et ses coordonnées, les choix offerts à la personne concernée en ce qui concerne la gestion de ses données à caractère personnel, les droits d'accès, de modification, de limitation et d'effacement des données, et les coordonnées de l'autorité de contrôle compétente[295]. Un des objectifs de cette conférence était de permettre, par la suite, de standardiser les différentes politiques de protection des données à caractère personnel dans leur version limitée à l'essentiel dans un format qui serait compatible avec l'ensemble des différentes lois nationales de protection des données à caractère personnel[296]. La liste des informations à fournir en premier niveau a d'ailleurs été inspirée d'une recommandation du

[292] Groupe de travail « Article 29 », WP260 rev. 01, *op. cit.*, p. 21.
[293] CNIL, Délibération n°2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » (demande d'avis n°20008032).
[294] Groupe de travail « Article 29 », WP 100, *op. cit.*, p. 8.
[295] Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), 12 septembre 2003, *op. cit.*
[296] *Ibidem.*

Groupe de travail « Article 29 » sur les exigences minimales pour la collecte de données à caractère personnel en ligne au sein de l'Union européenne[297].

133. Après l'adoption du RGPD en 2016, le G29 a publié des préconisations similaires, mais adaptées aux dispositions du règlement nouvellement adopté dans ses lignes directrices relatives à la transparence. Dans ce texte, le G29 invite les responsables de traitement à fournir en premier niveau les informations mentionnées au considérant 39 du RGPD, soit les informations sur l'identité du responsable de traitement, les finalités du traitement, le droit d'accès aux données à caractère personnel ainsi que toutes autres informations visant à assurer un traitement loyal et transparent des données à caractère personnel vis-à-vis des personnes concernées[298]. En plus de ces informations, le responsable de traitement devra identifier les traitements qui auront la plus forte incidence sur la personne concernée et « tout traitement qui pourrait la surprendre »[299] afin d'informer la personne concernée dès le premier niveau d'information des conséquences que ces traitements pourraient avoir sur elle[300]. Ainsi, le contenu du premier niveau d'information dépendra des traitements concernés, et l'identification de certaines informations essentielles au premier niveau d'information sera à la charge du responsable de traitement.

134. Concernant les niveaux suivants d'information, une proposition d'avis du G29 en 2004 avait proposé de créer jusqu'à trois niveaux d'information : la version raccourcie à l'essentielle, la version condensée et la version complète de la politique de protection des données[301]. Le deuxième niveau contiendrait les informations délivrées au titre des obligations européennes (à l'époque de la rédaction, la directive 95/46/CE) et le troisième niveau inclurait également les informations délivrées au titre des obligations nationales[302]. À l'heure de l'harmonisation de l'ensemble des dispositions européennes de protection des données souhaitée par le RGPD, cette distinction semble désormais obsolète. Le responsable de traitement doit désormais décider des informations à délivrer à chacun de ces niveaux en fonction des traitements des données, mais aussi de la lisibilité de l'information délivrée.

135. La pratique de l'information multiniveaux est bénéfique à plusieurs égards. Premièrement, elle permet de concilier droit à l'information sur la collecte de ses données à

---

[297] Groupe de travail « Article 29 », *Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union*, adoptee le 17 mai 2001, 5020/01/EN/Final WP43, pp. 4-6.
[298] RGPD, 27 avril 2016, considérant 39 ; Groupe de travail « Article 29 », WP260 rev. 01, *op. cit.*, p. 22.
[299] *Ibidem*, pp. 22-23.
[300] *Ibidem*, p. 23.
[301] Groupe de travail « Article 29 », WP 100, *op. cit.*, pp. 8-9.
[302] *Idem.*

caractère personnel et activités économiques sur internet puisqu'elle permet de ne pas entraver la navigation par de longues politiques de confidentialités tout en laissant à la personne concernée la possibilité d'accéder aux détails de la collecte de ses données à caractère personnel. Deuxièmement, cette pratique permet de rendre plus claire la politique de confidentialité, et de présenter une politique de confidentialité en plusieurs niveaux de détails. Ces différents niveaux de détails permettent à la personne concernée de cerner la globalité des traitements attachés à la collecte de ses données à caractère personnel sans pour autant sacrifier la description détaillée de ceux-ci. Cette raison explique pourquoi la pratique a été validée[303] et même encouragée[304] par la CNIL. Enfin, elle permet d'améliorer la lisibilité des politiques de protection des données sur des formats où l'espace, voire le temps, de la communication des informations est limitée, comme sur un smartphone[305].

136. Cependant, l'abus d'une telle pratique doit être prohibé puisque, si l'information multiniveaux permet de simplifier la réception de l'information, une utilisation malveillante d'un tel procédé peut au contraire brouiller la clarté de l'information délivrée. La pratique est dès lors soumise au contrôle *in concreto* des autorités de contrôle. En effet, en 2018, la CNIL a condamné Google sur ce fondement, relevant que non seulement les données étaient « excessivement disséminées dans plusieurs documents »,[306] mais qu'il était aussi nécessaire d'activer plusieurs liens et boutons afin d'accéder à des informations complémentaires[307]. L'autorisation et l'encouragement de délivrance d'une information multiniveaux doivent donc être lus en adéquation avec l'objectif de délivrance d'une information claire et le caractère immédiat de la délivrance de l'information. Ainsi, la CNIL a condamné Google sur le fondement d'un manque d'accessibilité du fait de « l'architecture générale de l'information »[308]. Cet arrêt résume bien l'obligation d'accessibilité d'information – et l'obligation d'informer de bonne foi qui en découle. En effet, la CNIL a invoqué deux fondements principaux dans sa condamnation. Premièrement, l'information n'était pas regroupée au sein d'un document unique puisque les données étaient « excessivement

[303] CNIL, Délibération de la formation restreinte n°2013-420 du 3 janvier 2014 prononçant une sanction pécuniaire à l'encontre de la société X.
[304] CNIL, « Google's new privacy policy : incomplete information and uncontrolled combination of data across services » *Communiqué de presse*, 16 octobre 2012, disponible sur https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20121016_press_release_google_privacy_cnil_en.pdf
[305] Groupe de travail « Article 29 », WP 100, *op. cit.*, pp. 7-8.
[306] CNIL, « La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de Google LLC », CNIL.fr, janvier 2019, disponible sur https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la (consulté en novembre 2020).
[307] *Idem.*
[308] *Idem.*

disséminées dans plusieurs documents »[309] et il était ainsi nécessaire d'activer plusieurs liens et boutons afin d'accéder à des informations complémentaires[310]. Deuxièmement, l'information n'était « accessible qu'après plusieurs étapes, impliquant parfois jusqu'à cinq ou six actions »[311]. La CNIL démontre bien qu'il ne suffit pas que l'information existe, mais qu'il faut encore qu'elle soit délivrée de bonne foi – et qu'elle soit, par conséquent, facilement accessible à la personne concernée. Les autorités de contrôle et les autorités judiciaires procèdent ensuite à un contrôle *in concreto* de la bonne foi de l'entreprise, introduisant une dose de subjectivation importante dans l'appréciation de l'accessibilité de l'information.

137. À la suite de l'élévation du conflit de Google devant le Conseil d'État, la juridiction administrative suprême a validé la solution de la CNIL. Rejetant les arguments de Google interprétant la délibération de la CNIL comme l'exigence qu'une « information exhaustive soit livrée dès le premier niveau d'information »[312], le Conseil d'État considère à son tour qu'une information abusivement éparpillée nuit à l'accessibilité et à la clarté de celle-ci pour les personnes concernées[313].

Cette interprétation est en accord avec l'interprétation proposée par le G29. En effet, celui-ci a anticipé les possibles abus de cette pratique et a précisé dans ses lignes directrices relatives à l'obligation de transparence :

> « Il convient de noter que les avis/déclarations sur la protection de la vie privée à différents niveaux ne sont pas simplement des pages imbriquées nécessitant que l'utilisateur effectue plusieurs clics avant d'accéder aux informations pertinentes. La mise en page et l'organisation du premier niveau de l'avis ou de la déclaration sur la protection de la vie privée devraient être telles que la personne concernée bénéficie d'un aperçu clair des informations qui lui sont accessibles sur le traitement de ses données à caractère personnel et du lieu ainsi que de la façon de trouver ces informations détaillées parmi les niveaux de l'avis ou de la déclaration sur la protection de la vie privée »[314].

138. Les modalités d'accessibilité de l'information ont donc été précisées à plusieurs reprises en ce qui concerne les politiques de protection des données, à travers une interprétation uniforme des autorités de contrôles et des juridictions. Les autorités de contrôle se sont aussi

---

[309] *Idem.*
[310] *Idem.*
[311] *Idem.*
[312] CE, 10e et 9e chambres réunies, 19 juin 2020, n°430810, *Société Google LLC*, cons. 23.
[313] *Idem.*
[314] Groupe de travail « Article 29 », WP260 rev. 01, *op. cit.*, p. 22.

intéressées aux autres moyens d'accessibilité de l'information relative à la protection des données à caractère personnel.

B. Les autres moyens d'accessibilité de l'information

139. L'information multiniveaux n'est évidemment pas le seul moyen de délivrance de l'information que les responsables de traitement peuvent proposer aux personnes concernées. En effet, le développement des « technologies permettant la transparence » (*Transparency-Enhancing Technologies ou TETs)* a pour objectif de « fournir à la personne concernée une visibilité claire des aspects relatifs à la protection de ses données à caractère personnel et de sa vie privée »[315]. Le Groupe de travail « Article 29 » a en effet aussi mentionné dans ses lignes directrices sur la transparence les notifications de type « push », permettant d'afficher l'information « en temps réel » et les notifications de type « pull », comme les tableaux de bord ou les tutoriels[316]. Ces deux technologies diffèrent dans leur forme et utilité.

140. Les technologies de type « push » sont les technologies permettant à un serveur de délivrer une information sur le serveur de l'utilisateur[317], sans que ce dernier n'ait émis la moindre requête[318] : c'est le cas, par exemple, des notifications qui peuvent apparaître sur le navigateur de recherche lors de la navigation sur internet. Cette technologie présente des caractéristiques intéressantes quant à l'exécution de l'obligation d'information. En effet, par l'action de « pousser » l'information sur le terminal de l'utilisateur, le responsable de traitement va pouvoir choisir à quel moment la personne concernée recevra cette information. Dès lors, le responsable de traitement pourra demander le consentement « en temps réel » de la personne concernée, permettant à cette dernière de choisir quand et si elle consent. D'après Eve Maler, ces notifications permettent à la personne concernée de garder le contrôle de ses données, tout en incitant les responsables des données à conserver une relation « sur un pied d'égalité » lors de leurs demandes d'accès aux données à caractère personnel[319]. Le Groupe « Article 29 » a

---

[315] HANSEN Marit, « User-Controlled Identity Management: the Key to the Future of Privacy? », *International Journal of Intellectual Property Management*, 2(4), p. 337.
[316] Groupe de travail « Article 29 », WP260 rev. 01, *op. cit.*, pp. 23-24.
[317] Google, « Web Push Notifications: Timely, Relevant, and Precise », *Google.com*, Web fundamentals, 12 février 2019, disponible sur https://developers.google.com/web/fundamentals/push-notifications (consulté en janvier 2021).
[318] YUHAS Katherine, « Subscribe Here For More: Analyzing the Video Privacy Protection Act in the Mobile Era », *Southern Illinois University Law Journal*, 2008, 42(2), p. 389.
[319] MALER Eve, « Extending the Power of Consent with User-Managed Access: A Standard Architecture for Asynchronous, Centralizable, Internet-Scalable Consent », *2015 IEEE Security and Privacy Workshops*, San Jose, CA, 2015, pp. 175-179.

également validé la technique des notifications « en temps réel » [320] (*just-in-time notice*), car, non seulement cette technologie permet de fournir les informations « au moment où leur lecture est la plus pertinente pour la personne concernée », mais elle permet également de fournir une information plus facilement assimilable par la personne concernée,[321] et ce, à deux titres. Premièrement, la notification « en temps réel » permet de fournir à la personne concernée une information contextualisée quand une politique de protection des données à caractère personnel fournira une information sortie de son contexte[322]. Deuxièmement, scinder l'information permet de fournir une explication plus synthétique, encourageant la personne concernée à la lecture de l'information.

141. En introduisant la subjectivation du contrôle de l'accès à l'information du point de vue de la personne concernée, le RGPD encourage implicitement les responsables de traitement à contextualiser l'information et la scinder de telle sorte que la personne concernée possède toutes les cartes en main pour contrôler le sort de ses données à caractère personnel. Plus que le respect de la lettre du RGPD à travers des politiques de confidentialité, le législateur européen a encouragé les responsables de traitement à penser la transparence non plus comme lieu de centralisation des informations aux fins de satisfaction d'une obligation légale, mais comme une transparence intégrée au parcours utilisateur (ou *experience map*) de la personne concernée. En encourageant de telles initiatives, les autorités de contrôle cherchent à inciter les responsables du traitement à respecter l'esprit du RGPD, au-delà de la simple lettre. Penser la transparence à travers les notifications « push » relève de l'esprit du RGPD, car un tel effort nécessite d'utiliser des ressources juridiques, techniques, marketing[323], etc. Le respect du RGPD s'étend en dehors de la simple conformité afin de devenir une valeur de l'organisation, centrée sur la capacité de la personne concernée de se saisir de l'information délivrée avant de consentir ou non au traitement de ses données à caractère personnel.

142. Les notifications « pull » sont des méthodes qui ont pour objet de centraliser certaines informations afin d'en faciliter l'accès par les utilisateurs[324]. En matière d'information sur la protection des données à caractère personnel, c'est donc la personne concernée qui va initier la

---

[320] Dans la version française, le texte du Groupe de travail « Article 29 » mentionne des notifications à « flux tendus ». Nous considérons que la traduction de *just-in-time notice* par notification à « flux tendus » est peu appropriée dans la mesure où elle reprend des termes consacrés en Gestion de la chaîne logistique (ou *Supply Chain Management*) tandis que les termes « notification en temps réel » est davantage utilisé en matière informatique.
[321] Groupe de travail « Article 29 », WP260 rev. 01, *op. cit.*, p. 24.
[322] *Ibidem.*
[323] Notamment, la mobilisation de compétences d'*user experience design* ou *UX design*.
[324] Groupe de travail « Article 29 », WP260 rev. 01, *op. cit*, p. 24.

requête d'information[325]. Parmi les notifications « pull », le Groupe de travail « Article 29 » insiste plus particulièrement sur les tableaux de bord sur la protection de la vie privée qui sont « un lieu unique depuis lequel les personnes concernées peuvent visualiser les informations relatives à la confidentialité et gérer leurs préférences en permettant ou en empêchant que leurs données soient utilisées de certaines façons par le service en question »[326]. Un tableau de bord sur la protection de la vie privée, contrairement à une simple politique de protection des données à caractère personnel, implique pour le responsable de traitement de mettre en œuvre des moyens technologiques plus importants afin de répondre à trois objectifs : fournir à la personne concernée des outils de contrôle de ses données traitées par un responsable de traitement, permettre à la personne concernée de vérifier la conformité des traitements de ses données à caractère personnel avec la législation en vigueur et enfin, sensibiliser les personnes concernées à la nature et au volume de ses données à caractère personnel traitées par un responsable de traitement[327]. Au niveau de l'obligation légale de transparence et de garantie du consentement éclairé, une telle technologie peut répondre à la double contrainte inhérente à l'obligation d'information : informer suffisamment la personne concernée sans la noyer sous un volume trop important d'informations[328].

143. Comme toute technologie créée dans l'objectif de remplir une obligation prévue dans le RGPD, et plus largement de protéger le consentement éclairé des personnes concernées, le tableau de bord sur la protection de la vie privée doit répondre à un cahier des charges inspiré des textes législatifs. Christoph Bier, Kay Kühne et Jürgen Beyerer ont, lors d'une communication au quatrième forum annuel sur la vie privée (*4th Annual Privacy Forum*) en 2016, proposé un cahier des charges du tableau sur la protection de la vie privée comportant treize points, dont huit sont inspirés de textes législatifs[329]. Ces spécifications peuvent être résumées de la manière suivante. Un tableau de bord sur la vie privée doit être accessible à toute personne concernée sans contraintes formelles ou techniques[330]. À l'intérieur de ce tableau de

---

[325] WU Heng *et al.*, « The Role of Push_Pull Technology in Privacy Calculus: The Case of Location Based Services », *Journal of Management of Information Systems*, 2009, 26:3, p. 137.
[326] Groupe de travail « Article 29 », WP260 rev. 01, *op. cit.*, p. 24.
[327] ZIMMERMANN Christian *et al.*, « Privacy Dashboards: Reconciling data-driven business models and privacy », *2014 Ninth International Conference on Availability, Reliability and Security*, Fribourg, 2014, p. 158.
[328] Privacy Patterns, "Privacy Dashboard", *Privacypatters.org*, disponible sur https://privacypatterns.org/patterns/Privacy-dashboard
[329] BIER Christoph *et al.*, « Privacy Insight: The Next Generation Privacy Dashboard » *in* SCHIFFNER Stefan *et al.* (dir.), *Privacy Technologies and Policy*, 4th Annual Privacy Forum, AFP 2016, Frankfurt/Main, Germany, September 7-8 2016, Proccedings, Springer, pp. 135-152.
[330] BIER Christoph *et al.*, *op. cit.*, pp. 135-152; RASCHKE Philip *et al.*, « Designing a GDPR-Compliant and Usable Privacy Dashboard » *in* KOSTA Eleni *et al.* (dir.), *Privacy and Identity Management. The Smart Revolution*, 12th Annual IFI Summer School on Privacy and Identity Management, Ispra, Italy, September 4-8, 2017, Revised Selected Papers, Springer, p. 226.

bord, la personne concernée doit avoir accès à l'ensemble des données collectées, leurs sources et les finalités pour lesquels elles sont traitées, dans un format téléchargeable dans un format lisible[331]. Ainsi, la personne concernée doit être capable de visualiser l'ensemble des flux de données internes au traitement et des responsables de traitement et avoir les moyens de demander la modification, l'effacement ou la limitation de ses données[332].

144. La valeur des tableaux de bord de la vie privée semble être assez valorisée dans la recherche sur les technologies et la protection de la vie privée. Christian Zimmermann et son équipe de chercheurs vont jusqu'à considérer que cette technologie « a le potentiel unique de réconcilier les entreprises dont l'économie est fondée sur le traitement de données à caractère personnel et la protection de la vie privée »[333]. Plus modestement, les tableaux de bord de la vie privée présentent l'avantage principal de permettre à la personne concernée de visualiser concrètement et de contrôler plus facilement le traitement de ses données à caractère personnel. En facilitant la gestion des données à caractère personnel par la personne concernée, les tableaux de bord de la vie privée peuvent permettre, selon certains chercheurs, d'inciter les personnes concernées à prendre des décisions plus adéquates et plus performantes en matière de protection des données à caractère personnel[334]. En effet, les tableaux de bord de la vie privée présentent l'avantage indéniable de placer la personne concernée en contrôle de ses données à caractère personnel en lui fournissant un outil centralisé permettant de facilement comprendre, visualiser et contrôler le sort de ses données à caractère personnel. Il s'agit dès lors d'un outil respectant l'ensemble des objectifs du RGPD : la clarté, l'accessibilité et le contrôle. Cependant, en raison du coût élevé du tableau de bord de la vie privée par rapport à une politique de protection des données, il est probable que cette pratique n'apparaisse dans un premier temps que parmi les acteurs économiques dont le respect des données à caractère personnel ait la valeur d'avantage concurrentiel sur le marché. De plus, cette pratique ne peut se suffire à elle-même : puisque l'accès au tableau de bord répond à l'initiative de la personne concernée, l'information n'est plus « fournie » à cette dernière. L'utilisation d'un tableau de bord de la vie privée ne dispense donc pas le responsable de traitement de faire appel à des mécanismes d'information qui sont directement délivrés à la personne concernée.

---

[331] *Idem.*
[332] *Idem.*
[333] ZIMMERMANN Christian *et al., op. cit.*, pp. 152-157
[334] KARUNAGARAN Surya *et al.*, « Privacy Protection Dashboard: A Study of Individual Cloud-Storage Users Information Privacy Protection Responses », *ACM SIGMIS Conference on Computer and People Research – SIGMIS-CPR'17*, Proceedings, 2017, p. 181.

145. Les pratiques d'accessibilité de l'information sont ainsi diverses, et permettent de répondre à des situations variées en matière de protection des données à caractère personnel. Par exemple, un tableau de bord de la vie privée semble pertinent pour un acteur traitant de nombreuses données à caractère personnel pour des finalités diverses (ce qui est le cas de la publicité comportementale par exemple) tandis que les notifications « push » semblent être plus pertinentes pour les situations nécessitant un consentement contextuel intégré à l'expérience utilisateur (ce qui est le cas des applications mobiles, par exemple). Le responsable de traitement doit dès lors, en théorie, choisir le moyen de délivrance de l'information le plus adapté au besoin des personnes concernées. Il est d'ailleurs regrettable que les dispositions relatives à la transparence n'aient pas été rédigées d'une manière similaire aux dispositions relatives à la sécurité, en ce qui concerne les critères à prendre en compte pour choisir le canal d'information sur les traitements de données à caractère personnel. L'article 32 du RGPD exige en effet que le responsable de traitement choisisse les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque du traitement « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques »[335]. Une telle modulation de l'obligation pourrait être envisageable au niveau de l'obligation de transparence, cette obligation variant par exemple en fonction du coût de mise en œuvre du canal de délivrance de l'information, de la complexité de l'information et de l'état des recherches en matière de délivrance de l'information, etc. Une telle modulation de l'obligation de transparence pourrait également prendre en compte les enjeux liés à la capacité de compréhension de la personne concernée, qui varie selon ses caractéristiques.

146. Conclusion de section. – L'amélioration de la délivrance d'information a été atteinte à travers l'institution d'un réel droit à l'information, renforçant la simple obligation de transparence auparavant consacrée par les textes de protection des données à caractère personnel qui ont précédé le RGPD. L'évolution de l'obligation de transparence en droit à l'information a en effet permis d'ancrer l'interprétation des dispositions relatives à l'accessibilité dans le concret et la pratique quotidienne des responsables de traitement. L'accessibilité de l'information n'étant plus une obligation de moyen, mais une obligation de résultat, l'obligation de transparence n'est désormais satisfaite qui si la personne concernée a réellement les moyens de se saisir de l'information délivrée. Si les pratiques de délivrance de

[335] RGPD, 27 avril 2016, Article 32(1).

l’information ont encore peu évolué, faute d’incitants légaux, l’accès simplifié aux informations sur le traitement de leurs données à caractère personnel permet aux personnes concernées de consulter ces informations avant d’émettre leur consentement. La délivrance effective de l’information est ainsi un prérequis du consentement éclairé, mais pas une condition suffisante puisque la personne concernée doit également être capable de se saisir des informations ainsi délivrées.

Section 2 – L'adaptation de l'information aux personnes concernées

147. L'enjeu de la transparence en matière de consentement éclairé est de s'assurer que la personne concernée soit capable de comprendre l'information qui lui est délivrée. Or, cette prémisse au consentement éclairé était loin d'être satisfaite avant le RGPD. Notamment, les politiques de protection de la vie privée étaient dénoncées comme étant « verbeuses, difficiles à comprendre, trop longues à lire et sont souvent les éléments les moins lus de la plupart des sites web, alors même que les utilisateurs expriment des préoccupations croissantes quant aux pratiques de collecte »[336] de leurs données à caractère personnel.

148. Dans ce cadre, le législateur a innové en matière de transparence au sein du RGPD, en évaluant spontanément l'information délivrée à la personne concernée du point de vue de la personne concernée. Cette évaluation ne se limite pas à l'accès physique au contenu de l'information, mais s'étend également à l'accès intellectuel au contenu de l'information, soit à la capacité pour la personne concernée « moyenne » de se saisir et de comprendre l'information délivrée afin de prendre des décisions éclairées sur les traitements de ses données à caractère personnel (§1).

149. En adaptant l'information à la personne concernée, le législateur a désiré protéger la partie faible (la partie « ignorante ») face à la partie forte (la partie « connaisseuse »). Cependant, ce qui est accessible à la personne raisonnable moyenne ne l'est pas nécessairement pour les personnes concernées particulièrement vulnérables. Dans une logique de protection de la partie faible, le législateur a donc également désiré protéger les populations plus vulnérables (§2).

§1 – Les personnes concernées

150. La question de l'adaptation de l'information aux personnes concernées a été vastement étudiée par la recherche. Dès 1979, Franz J. Ingelfinger présente sa théorie selon laquelle « le problème avec le consentement éclairé est qu'il ne s'agit pas d'un consentement éduqué »[337]. L'auteur avait alors notamment mis en évidence l'inadaptation des obligations légales d'information lorsque cette information n'était pas en mesure d'être comprise par la personne

---

[336] "*Privacy policies are verbose, difficult to understand, take too long to read, and may be the least-read items on most websites even as user express growing concerns about information collection practices".* REINDERNBERG Joel R. *et al.*, « Disagreeable Privacy Policies: Mismatches between meaning and users' understanding », *Berkeley Technology Law Journal*, 2015, Vol. 30:1, p. 41.

[337] "*the trouble with informed consent is that it is not educated consent"* [traduction libre]. INGELFINGER Franz J., « Informed (but uneducated) consent », *in* HUMER James M., *Biomedical Ethics and the Law*, Springer US, 1979, XIV, p. 265.

concernée[338]. En 1980, une étude a été menée concernant le consentement éclairé à un traitement médical : les résultats ont montré que la capacité du patient de comprendre les buts et enjeux du traitement et de se rappeler au moins un des risques majeurs dépendait notamment du niveau d'études du patient.[339]. L'étude concluait alors que « les obstacles [au consentement] sont imposés par la difficulté de compréhension du contenu, du jargon juridique et d'autres connotations négatives contenues dans le document du consentement »[340]. Ce constat a conduit les chercheurs à réfléchir au renforcement de l'obligation d'information, notamment à une simplification du langage technique utilisé préalablement à l'exercice du consentement. Certains chercheurs sont allés jusqu'à revendiquer un « droit du patient à la compréhension »[341], « allant au-delà du simple devoir d'information imposé au médecin en vertu de la théorie du consentement »[342]. Ce qui a été démontré concernant le droit médical est aussi pertinent pour la protection des données à caractère personnel. En effet, l'étude précitée de Carlos Jensen et Colin Potts avait également démontré que la capacité de compréhension des politiques de protection des données variait avec le niveau d'études de la personne concernée[343].

151. S'il n'instaure pas un droit explicite de la personne concernée à la compréhension, le RGPD instaure tout de même une obligation à la charge du responsable de traitement de fournir une information compréhensible en matière de protection des données à caractère personnel : cette obligation est d'ailleurs renouvelée à cinq reprises au sein du texte du règlement[344]. Encore faut-il, pour évaluer la compréhensibilité d'une information, identifier le destinataire de l'information, c'est-à-dire la personne concernée. Il n'est jamais question, dans le texte du RGPD, de parler de « personne concernée raisonnable », mais il est possible, pour plusieurs raisons, de penser que cette fiction juridique, importée du droit anglo-saxon[345], est utile et nécessaire à l'interprétation du RGPD.

---

[338] *Idem.*
[339] CASSILETH, Barrie R. *et al.* « Informed Consent – Why are its Goals Imperfectly Realized ? », *New England Journal of Medecine,* 1980, 302(16), p. 899.
[340] « *barriers are imposed by the difficulty of the material and the legalistic and other negative connotations of the consent document* » [traduction libre]. *Idem.*
[341] CALMAN Kenneth C. « Communication of Risk: Choice, Consent and Trust », *The Lancet,* 360, p. 166 ; voir également HOLZEM Julie, « Les limites du consentement éclairé », *AJDA*, 2016, p. 364.
[342] LAZARO Christophe, LE METAYER Daniel, *op. cit.*, p. 771.
[343] JENSEN Carlos, POTTS Colin, *op. cit.*, pp. 471-478.
[344] RGPD, 27 avril 2016, considérant 42, considérant 60, article 7 (2), article 12 et article 12 (7).
[345] Le standard du raisonnable, s'il est importé du droit anglo-saxon, a tout de même eu un succès tout particulier en France avec le remplacement du « bon père de famille » par la « personne raisonnable » par la réforme des obligations de 2016. Voir notamment MARTIAL-BRAZ Nathalie, « L'objectivation des méthodes d'interprétation : la référence à la « personne raisonnable » et l'interprétation *in favorem* », *Revue des contrats,* 2015, n° 1, p. 193.

152. Premièrement, s'il n'est jamais question de « personne concernée raisonnable », le RGPD octroie des éléments de raisonnabilité à la personne concernée. Par exemple, le responsable de traitement devra mettre en balance ses intérêts légitimes avec les droits fondamentaux de la personne concernée en tenant compte des attentes raisonnables de celle-ci[346]. Les attentes raisonnables de la personne concernée doivent également être prises en compte pour évaluer la compatibilité d'une finalité autre que celle pour laquelle les données ont été collectées avec la finalité initiale[347]. Deuxièmement, une partie de la doctrine utilise déjà la fiction de la « personne concernée raisonnable » pour évaluer des notions telles que les données manifestement rendues publiques[348] ou encore le niveau de complexité de l'information compréhensible par la personne concernée[349].

153. Par conséquent, l'évaluation de la compréhensibilité et de la clarté d'une information s'effectue *in concreto* dans la mesure où « la personne raisonnable incarne la règle de droit calibrée à la situation »[350] : l'autorité de contrôle ou l'institution juridictionnelle chargée de déterminer la conformité ou non d'une information avec le RGPD se verra dès lors dotée d'un pouvoir de contrôle plein. Quant au responsable de traitement, l'utilisation de la fiction de la « personne concernée raisonnable » a un effet équivalent à une obligation générale de bonne foi dans la délivrance de l'information à la personne concernée[351].

154. Dès lors, pour être compatible avec le principe de transparence énoncé dans le RGPD, le responsable de traitement devra accorder une attention particulière à l'effort d'adaptation de la langue et du langage utilisé pour délivrer l'information à la personne concernée (A). Cependant, si la personne concernée n'est pas identifiée dans le texte du RGPD, il est possible de se demander si la personne concernée répond à la fiction traditionnellement utilisée dans le droit de la « personne raisonnable » ou si la notion prend en compte les particularités de personnes plus vulnérables comme les personnes en situation de handicap (B).

---

[346] RGPD, 27 avril 2016, considérant 47.
[347] RGPD, 27 avril 2016, considérant 50.
[348] DOVE Edward, CHEN Jiahong, « What Does it Mean for a Data Subject to Make their Personal Data "Manifestly Public"? An Analysis of GDPR Article 9(2)(e) », *Edinburgh School of Law research Paper,* 2020, vol. 18, p. 14.
[349] MCGRUER Jonathan, « Emerging Privacy Legislation in the International Landscape: Strategy and Analysis for Compliance », *Washington Journal of Law, Technology & Arts,* Hiver 2020, Vol. 15, Issue 2, p. 133.
[350] VINEY François, « L'expansion du « raisonnable » dans la réforme du droit des obligations : un usage déraisonnable ? », *D.*, 2016, p. 1940.
[351] LAISNEY Louis-Jérôme, « Pour en finir avec le « raisonnable » ! », *AJ contrat*, 2017, p. 6.

A. L'adaptation du langage

155. Adapter le langage à la capacité de compréhension de la personne concernée nécessite une réflexion sur ce qui relève du compréhensible et ce qui relève du complexe pour la personne concernée moyenne. Si certaines composantes peuvent relever de l'évidence, comme le fait d'éviter d'utiliser du jargon et des acronymes juridiques ou techniques, l'adaptation du langage de l'information délivrée à la personne concernée ne fait pas l'objet d'une définition précise, et semble plutôt relever de l'application concrète, de l'impression générale de compréhension à la suite de la lecture du texte étudié.

156. Des éléments précisant le niveau d'adaptation de langage que doit mettre en place le responsable de traitement peuvent être trouvés dans les sciences cognitives. En effet, il peut être considéré que le nœud du problème de l'adaptation de l'information au public concerné soit la cognition. Dans l'ouvrage de Claudette Fortin et Robert Rousseau, la cognition est définie comme « l'ensemble des activités mentales impliquées dans nos relations avec l'environnement : la perception d'une stimulation, sa mémorisation, son rappel, la résolution de problème ou la prise de décision »[352]. Les sciences cognitives se sont dès lors intéressées au processus cognitif aboutissant à la lisibilité et à la compréhension d'un texte.

157. Notamment, Walter Kintsch, chercheur américain en psychologie, a beaucoup travaillé sur le processus de compréhension de texte[353]. Ainsi, d'après Walter Kintsch, la compréhension d'un discours est un processus qui se déroule en deux phases : la phase de construction et la phase d'intégration (selon le modèle Construction-Intégration)[354]. Pendant la phase de construction, le processus de compréhension du discours va faire appel à la connaissance du sujet, connaissance qui sera peu structurée dans un réseau associatif dont les nœuds correspondent aux concepts et propositions extraites du discours[355]. Ces nœuds seront interconnectés selon les interconnexions qui seront positives ou négatives[356]. Le lecteur va donc extraire des propositions et concepts à partir du texte qu'il traite et ces extraits « vont servir d'indices de récupération d'autres propositions [en permettant] l'activation de leurs plus

---

[352] FORTIN Claudette, ROUSSEAU Robert, *Psychologie cognitive : une approche de traitement de l'information*, Québec, Presses de l'Université du Québec, 2016, p. 1.
[353] DENHIÈRE Guy *et al.*, « Psychologie cognitive et compréhension de texte : une démarche théorique et expérimentale », *in* PORHIEL Sylvie, KLINGER MAESTRALI Dominique (dir.), *L'unité texte*, Pleyben : Perspective, 2004, p. 75.
[354] LEBRETON Olivier, *Adaptation du modèle de la Construction-Intégration de Kintsch à la compréhension des énoncés et à la résolution des problèmes arithmétiques complexes*, Thèse pour l'obtention du grade de docteur en psychologie cognitive sous la direction de HAMON Jean-François, Université de la Réunion, 2011, pp. 81-82.
[355] KINTSCH Walter, « The Role of Knowledge in Discourse Comprehension: A Construction-Intergration Model », *Psychological Review*, 1988, vol. 95, n°2, pp. 163-182.
[356] *Ibidem.*

proches voisins dans le réseau de connaissance du lecteur »[357]. Ces propositions vont être liées les unes avec les autres grâce à des connexions positives ou négatives. La phase d'intégration va ensuite permettre la stabilisation du réseau associatif en renforçant la signification appropriée et en inhibant les propositions contradictoires[358]. Il faut également noter que la structuration des propositions au sein d'une phrase a également un effet sur la compréhension du texte puisque, selon une étude expliquée par Olivier Lebreton :

> « Kintsch et Keenan (1973) ont construit des phrases comportant approximativement le même nombre de mots (+- 16). Ces phrases se différenciaient, en revanche, par le nombre de propositions. Ce nombre variait entre 4 et 8. Les sujets devaient d'une part, appuyer sur le bouton aussi vite que possible après la lecture de chaque phrase (reading time) et d'autre part, les rappeler aussi bien que possible juste après. L'analyse des protocoles a montré que plus le nombre de propositions rappelées était élevé et plus le temps d'encodage était lui aussi élevé »[359].

158. Dès lors, la structure de l'information joue un rôle important dans la capacité de la personne concernée de comprendre l'information et de s'en approprier la substance. Le législateur européen semble en avoir été conscient puisque l'article 12 du RGPD requiert du responsable de traitement la délivrance d'une information « compréhensible et aisément accessible, en des termes clairs et simples »[360]. La simplicité du vocabulaire utilisé doit ainsi s'accompagner d'une structure grammaticale simple, permettant à la personne concernée une lecture plus rapide et plus efficace de l'information qui lui est délivrée. Le législateur a même permis aux responsables de traitement d'aller plus loin dans la recherche de la simplicité de l'information, évoquant la possibilité d'utiliser des icônes accompagnant les informations fournies « afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu »[361].

159. Le souci de rendre les informations concernant les traitements de données à caractère personnel s'est manifesté dès les négociations ayant abouti à l'adoption du RGPD. En effet, la plupart des amendements proposaient, à l'instar du texte adopté, une liste de caractéristiques à atteindre par le responsable de traitement. Il est à cet égard intéressant de mentionner que

---

[357] LEBRETON Olivier, *op. cit.*, p 82.
[358] BLANC Nathalie, BROUILLET David, *Mémoire et compréhension*, Clamecy, 2003, 190 p. ; Olivier Lebreton, *op. cit.*, p 89.
[359] LEBRETON Olivier, *op. cit.* p 51. L'étude décrite est rapportée dans l'article KINTSCH Walter, KEENAN Janice, « Reading rate and retention as function of the number of propositions in the base structure of sentences », *Cognitive Psychology*, 1973, Vol. 5(3), pp. 257-274.
[360] RGPD, 27 avril 2016, Article 12 § 1.
[361] RGPD, 27 avril 2016, Considérant 60.

certains députés ont voulu rendre abstrait le niveau de compréhension à atteindre à travers la figure du consommateur moyen informé, attentif et capable de compréhension[362], constituant une formule plus exigeante que celle de la personne concernée raisonnable susmentionnée. En effet, la notion de « consommateur moyen informé, attentif et capable de compréhension » fait peser sur la personne concernée une présomption de connaissance générale des mécanismes de protection des données à caractère personnel ou encore du fonctionnement des outils numériques. Une telle interprétation aurait empêché de protéger les personnes concernées face à des outils innovants encore mal compris, ou encore des catégories de personnes concernées présentant des difficultés face aux outils numériques. Ainsi, le rejet de cet amendement constitue un indice de la volonté des parlementaires de protéger la personne concernée d'une information difficile à comprendre plutôt que de faire peser sur la personne concernée une charge de compréhension.

160. La question du niveau de langage à utiliser pour informer la personne concernée sur le traitement de données à caractère personnel a été analysée par le G29. Dans ses lignes directrices sur le consentement, le G29 fournit certaines indications sur comment fournir les informations requises par le RGPD :

> « Un message devrait être facilement compréhensible pour l'homme de rue et pas uniquement pour les avocats. Les responsables du traitement ne peuvent pas utiliser de longues politiques de confidentialité difficiles à comprendre ou des énoncés riches en jargon juridique »[363].

Dans ce cadre, la CNIL recommande d'adopter les mesures suivantes :

> « Utiliser un vocabulaire simple, faire des phrases courtes et employer un style direct ; éviter les termes juridiques ou techniques, les termes abstraits ou ambigus et les formules telles que « nous pourrions utiliser vos données », « une possible utilisation de vos données », « quelques données vous concernant sont utilisées »[364].

La CNIL a, en 2020, renouvelé son invitation à délivrer une « information compréhensible par le plus grand nombre, dans des termes clairs et simples » à propos de l'application StopCovid envisagée par le gouvernement français[365].

---

[362] « *an average informed, attentive and understanding average consumer* ». TICĂU Silvia-Andriana, Bernd LANGE, Amendement 1114 proposé à l'article 11, paragraphe 2 du RGPD.
[363] Groupe de travail « Article 29 », WP 260 rev. 01, *op. cit.*, p. 16.
[364] CNIL, « Conformité RGPD : comment informer les personnes et assurer la transparence ? », CNIL.fr, 26 juillet 2019, disponible sur https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence
[365] CNIL, Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » (demande d'avis n° 20006919).

161. Ainsi, ces recommandations correspondent aux données dégagées par les sciences cognitives sur la compréhension du discours. D'une part, l'information fournie par le responsable de traitement ne doit pas faire appel à des connaissances étendues de l'individu puisque le « jargon juridique », les « termes techniques » doivent être éliminés au profit d'un « vocabulaire simple ». D'autre part, le nombre de propositions par phrase doit être limité dans la mesure où les recommandations invitent le responsable de traitement à employer des « phrases courtes » afin de ne pas aboutir à de « longues politiques de confidentialité difficiles à comprendre ».

162. En 2019, le Tribunal de Grande Instance de Paris a annulé une clause de la politique de protection de la vie privée de l'entreprise Steam. Si le Tribunal a fondé sa décision sur l'article L. 211-1 du Code de la consommation exigeant du professionnel une information claire et compréhensible, les mêmes motifs font de la politique de protection de la vie privée de Steam une information non conforme au RGPD. En effet, le tribunal remarque que :

> « La simple lecture de la clause critiquée, qui fait référence aux « lois applicables sur le marketing par e-mail », montre qu'à l'évidence la clause n'est ni claire ni compréhensible. Elle sous-entend que l'utilisateur connaît parfaitement le code des postes et des communications électroniques et plus précisément son article L. 34-5, ce qui non seulement n'est pas le cas d'un « utilisateur moyen » voire d'un « juriste moyen » »[366].

163. L'adaptation du langage de l'information délivrée à la personne concernée comporte ainsi plusieurs éléments complémentaires, qui sont la structure grammaticale de l'information et l'utilisation d'un vocabulaire simple ne demandant pas à la personne concernée de posséder des connaissances supplémentaires pour comprendre l'information. Ce dernier élément n'implique pas uniquement l'utilisation d'un vocabulaire simple puisqu'une conséquence de la compréhensibilité de l'information sans faire appel à d'autres connaissances a également des conséquences sur le choix de langue opéré pour rédiger les politiques de confidentialité.

B. L'adaptation de la langue

164. Le RGPD, en tant que règlement européen, harmonise les dispositions européennes en matière d'obligation de transparence sur les traitements de données à caractère personnel. Cependant, en matière d'obligation d'informer, la diversité linguistique caractéristique de l'Union européenne peut constituer un obstacle. La Commission européenne est d'ailleurs consciente des difficultés issues du multilinguisme de l'Union européenne : en 2009, dans une

[366] TGI Paris, 17 septembre 2019, n° 16/01008.

Communication au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions relative au multilinguisme, la Commission débute en citant Amin Maalouf, selon lequel :

> « La diversité linguistique constitue pour l'Europe un défi. Mais c'est là, de notre point de vue, un défi salutaire ».[367]

165. Aujourd'hui, l'Union européenne compte vingt-quatre langues officielles. La première conséquence d'un multilinguisme aussi avancé est qu'il n'est pas raisonnable d'exiger d'un citoyen de l'Union européenne la maîtrise de l'ensemble des langues officielles de l'Union européenne. Dès lors, les traités et les documents officiels de l'Union européenne sont traduits dans l'ensemble des vingt-quatre langues officielles. Appliquée à la création du marché intérieur permettant la libre circulation des marchandises et des services, cette logique va aussi imprégner le droit influencé par la création du marché unique, notamment le droit de la consommation et le droit social. L'application de mesures d'adaptation au multilinguisme va d'ailleurs plus particulièrement toucher l'obligation d'information relative aux produits, services et relations de travail dans une démarche de protection. L'étude de l'exigence linguistique quant à l'obligation d'informer le consommateur sera utile pour dégager une philosophie linguistique générale (1) qui imprégnera l'obligation de transparence en matière de protection des données à caractère personnel (2).

1. Les exigences linguistiques dans l'obligation d'informer le consommateur

166. La création du marché intérieur permettant la libre circulation des marchandises et des personnes a ainsi dû faire l'objet de certaines adaptations quant aux exigences linguistiques liées à la présentation et à l'étiquetage des produits. En effet, l'information d'informer, pour être effective, doit être comprise par le destinataire de l'information.

167. Ainsi, l'exigence d'informer dans une langue que le destinataire de l'information comprend une règle bien établie en matière de droit de la consommation ou encore en droit du travail, dont l'interprétation a pu faire l'objet de certaines évolutions. En France, c'est la loi du 4 août 1994 qui impose de façon générale et obligatoire l'usage du français dans certains domaines, dont la publicité, l'audiovisuel, le travail ou encore l'enseignement[368]. Dès

---

[367] Commission européenne, *Multilinguisme : un atout pour l'Europe et un engagement* commun, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 18 septembre 2008, {SEC (2008) 2443} {SEC (2008) 2444} {SEC (2008) 2445}.

[368] FÉRAL-SCHUHL Christiane, « Chapitre 714 – Atteintes à l'ordre public », *in* FÉRAL-SCHUHL Christiane (dir.), *Cyberdroit : le droit à l'épreuve de l'Internet*, Dalloz, Collection Praxis, 2020-2021, p. 1612 ; L. n° 94-665, 4 août 1994 relative à l'emploi de la langue française, dite loi Toubon, *JO* 5 août 1994, p. 1392.

l'article 2, cette loi garantit la délivrance de certaines informations relatives à un produit en langue française. Une telle obligation, bien que plus légère dans son libellé, avait, quelques années plus tard, été édictée au niveau de l'Union européenne à travers la directive 97/4/CE qui a exigé « l'étiquetage des denrées alimentaires dans une langue facilement comprise par le consommateur »[369], permettant aux États membres d'imposer la rédaction de certaines informations dans une ou plusieurs langues officielles européennes selon les nécessités et réalités propres à leur population[370].

168. Cette disposition a fait l'objet d'une difficulté d'interprétation sur la possibilité ou non d'imposer l'étiquetage d'un produit dans la langue officielle ou dominante de l'État membre dans lequel la denrée alimentaire concernée était commercialisée. En effet, la Cour de Justice des Communautés européennes (CJCE) a refusé d'assimiler l'obligation d'utiliser « langue facilement compréhensible par les consommateurs » à l'emploi obligatoire de la langue sur une région déterminée en matière d'étiquetage des produits alimentaires[371]. La CJCE a ensuite clarifié sa jurisprudence en énumérant un certain nombre d'indices permettant de déterminer le caractère « facilement compréhensible par les consommateurs » d'une langue sur une région déterminée :

> « À cet égard, peuvent constituer des indices pertinents, sans être pour autant déterminants en soi, divers facteurs, tels que l'éventuelle similarité des mots dans différentes langues, la connaissance générale de plus d'une langue par la population concernée, ou l'existence de circonstances particulières telles qu'une vaste campagne d'information ou une large diffusion du produit, pourvu qu'il puisse être constaté que le consommateur est suffisamment informé »[372].

Dès lors, l'interprétation de la Cour de Justice voyait en la loi dite « Tourbon » une entrave à la libre circulation des marchandises et des prestations de service[373] : les exigences linguistiques devaient alors être soumises à un test de proportionnalité strict par rapport à l'objectif de compréhension de l'information par le consommateur pour ne pas constituer une mesure d'effet équivalent à des restrictions quantitatives à la libre circulation des marchandises[374].

---

[369] Directive 97/4/CE du Parlement européen et du Conseil, du 27 janvier 1997, modifiant la directive 79/112, *JO L. 43*, p. 21 ; CJCE, 12 septembre 2000, *Geoffroy et Casino France SNC*, C-366/98, §6.
[370] Directive 97/4/CE du 27 janvier 1997 ; CJCE, C-366/98, §6.
[371] CJCE, 18 juin 1991, *ASBL Piageme et BVBA* Peeters, C-369/89 ; Commission des communautés européennes, *Communication interprétative de la Commission concernant l'emploi des langues pour la commercialisation des denrées alimentaires suite à l'arrêt « Peeters »,* 10 novembre 1993, COM (92) 532 final ; CJCE, C-366/98.
[372] CJCE, 12 octobre 1995, *Groupement des producteurs, importateurs et agents généraux d'eaux minérales étrangères, VZW (Piageme) e. a.*, C-85/94, §30.
[373] MANGIAVILLANO Alexandre, « La clause Molière, une tartufferie ? », *D.*, 2017, p. 968.
[374] PIZZIO Jean-Pierre, « Exigences linguistiques en matière d'étiquetages des produits mis sur le marché », *D.*, 2000, p. 42.

169. Cette interprétation n'a pas fait l'unanimité parmi les juristes. Notamment, Jean-Marie Pontier a adressé à propos de l'interprétation des exigences linguistiques en matière d'étiquetage de denrées alimentaires deux critiques intéressantes à soulever. Premièrement, pour l'auteur, « la Cour a inversé le raisonnement de la directive »[375]. Cette objection est intéressante à soulever dans la mesure où la directive énonce dans son préambule que les réglementations relatives à l'étiquetage des denrées alimentaires doivent « être fondée[s], avant tout, sur l'impératif de l'information et de la protection des consommateurs »[376]. Dès lors, la solution de la Cour de justice confrontée au constat juste de Jean-Marie Pontier que « s'il est une langue que les Français sont en mesure de comprendre, c'est bien, *a priori,* le français » peuvent laisser à penser que les objectifs liés à la libre circulation des marchandises dans le marché intérieur prévalent sur les objectifs liés à la protection des consommateurs, et plus particulièrement, sur l'obligation de délivrer une information compréhensible pour le consommateur. Deuxièmement, l'auteur voit en cette solution « cette vaste hypocrisie qui consiste à donner de plus en plus la préférence à une langue, l'anglais, tout en continuant à affirmer officiellement l'égalité des langues »[377]. Dans cette hypothèse, l'effectivité de la protection du consommateur s'en trouve fortement réduite par les données relatives au niveau en langue anglaise de la population française. En effet, le récent constat de l'EF EPI plaçant la France comme un des pays de l'Union européenne ayant le plus mauvais niveau d'anglais (avec l'Espagne et l'Italie)[378] semble partagé par la population française elle-même d'après un sondage IPSOS de 2019, selon lequel :

> « Seulement 19 % des Français (et 21 % des actifs) jugent leur propre niveau d'anglais satisfaisant. La moitié d'entre eux (50 %) a à l'inverse un mauvais niveau voire ne parle pas du tout anglais »[379].

Ce constat n'est d'ailleurs pas spécifique à la population française. En effet, dans la recommandation du Conseil du 22 mai 2019 relative à une approche globale de l'enseignement et de l'apprentissage des langues, le Conseil de l'Union européenne a constaté que « près de la

---

[375] PONTIER Jean-Marie, « Le juge communautaire, la langue française et les consommateurs », *D.,* 2001, p. 1458.
[376] Directive 79/112/CEE du Conseil, du 18 décembre 1978, relative au rapprochement des législations des États membres concernant l'étiquetage et la présentation des denrées alimentaires destinées au consommateur final ainsi que la publicité faite à leur égard, Préambule.
[377] PONTIER Jean-Marie, 2001, *op. cit.*, p. 1458.
[378] EF EPI, *Un classement de 100 pays et régions par compétences en anglais,* édition 2020, disponible sur https://www.ef.com/cafr/epi/ (consulté en janvier 2021).
[379] VACAS Federico, BOISSON Laurène, « Les Français et l'anglais : seuls 21 % estiment avoir un niveau satisfaisant », *Ipsos.com,* 23 septembre 2019, disponible sur https://www.ipsos.com/fr-fr/les-francais-et-langlais-seuls-21-estiment-avoir-un-niveau-satisfaisant (consulté en janvier 2021).

moitié des Européens déclarent qu'ils ne sont pas capables de tenir une conversation dans une autre langue que leur langue première »[380].

170. Néanmoins, de tels constats semblent avoir été remis en cause par l'évolution du droit positif en matière de droit de la consommation, notamment par les efforts de regroupement et de construction d'outils juridiques européens cohérents et harmonisés de droit de la consommation aboutissant à l'adoption de règlements. Ainsi, aujourd'hui, l'article 15 du règlement 1169/2011 garantit la délivrance de l'information au consommateur dans une langue qu'il comprend d'une part, en créant à la charge de l'exploitant proposant des denrées alimentaires une obligation de délivrer ces informations « dans une langue facilement compréhensible par les consommateurs des États membres où la denrée est commercialisée », et d'autre part, en permettant aux États membres d'imposer la délivrance de l'information dans une ou plusieurs langues officielles de l'Union de leur choix. Le Code de la consommation français fonde d'ailleurs expressément son article R. 412-7 imposant l'étiquetage des denrées alimentaires en français sur l'article 15 du règlement 1169/2011. La jurisprudence sera peut-être amenée également à évoluer. Il est possible de voir un indice dans le fait que, en 2020, la CJUE a, dans une affaire portant sur l'étiquetage de produits cosmétiques, énoncé que l'exigence « selon laquelle les informations […] sont mentionnées dans la langue prescrite par la législation de l'État membre dans lequel le produit est mis à la disposition de l'utilisateur final, permet de garantir un niveau élevé de protection des consommateurs »[381].

171. Ainsi, la jurisprudence européenne ne consacre pas absolument le droit d'obtenir une information dans la langue de l'État dans lequel réside un consommateur. Cependant, le faisceau d'indices utilisé pour évaluer la capacité pour les résidents d'un État membre de comprendre l'information qui leur est délivré aboutit en pratique à l'utilisation des langues nationales communément parlées dans l'État membre concerné. En matière de protection des données à caractère personnel, les autorités de contrôle ont proposé une application plus sévère des exigences linguistiques, évalué en fonction de la région dans laquelle se situe la personne concernée cible du traitement de données à caractère personnel.

---

[380] Conseil de l'Union européenne, Recommandation du Conseil relative à une approche globale de l'enseignement et de l'apprentissage des langues, 22 mai 2019, 2019/C 189/03, considérant 7. Ce constat est fondé sur une étude de l'Eurobaromètre intitulé « Les Européens et leurs langues » menée sur l'année 2012.
[381] CJUE, 3e ch, 17 décembre 2020, *A.M. contre E.M.*, n° 667/19, §47.

2. Les exigences linguistiques applicables à l'obligation de transparence en matière de données à caractère personnel

172. Le RGPD n'indique pas directement que l'information délivrée à la personne concernée doit être rédigée dans une langue que cette dernière comprend. Néanmoins, l'article 12 du RGPD crée à la charge du responsable de traitement une obligation de fourniture d'une information « compréhensible », obligation qui présuppose l'utilisation d'une langue comprise par la personne concernée. Cette interprétation est conforme à celle du Groupe de travail « Article 29 » qui précise, dans ses lignes directrices relatives à la transparence qu'« une traduction dans une ou plusieurs langues devrait être fournie lorsque le responsable du traitement cible des personnes concernées parlant ces langues »[382]. Au sein du même document, le G29 expose les différents indices permettant de conclure qu'un responsable de traitement cible des personnes concernées parlant une langue déterminée : il s'agira notamment de la rédaction d'un site internet dans une certaine langue, l'offre d'options spécifiques à un État ou encore, la possibilité de payer des biens ou services dans la monnaie d'un État[383].

173. La question des exigences linguistiques quant à la rédaction des informations sur les traitements de données à caractère personnel a été posée devant l'autorité de protection des données belge (APD). Lors d'un audit d'un site internet d'actualités juridiques, le Service d'inspection a relevé une infraction matérialisée par le fait que les informations fournies quant aux traitements de données à caractère personnel « n'étaient disponibles qu'en néerlandais, alors qu'il ressort de la mention « Français » en haut à gauche que celles-ci (et par extension le site Internet https://Y) s'adressent également à des francophones »[384]. Selon l'APD, le RGPD prévoit la fourniture d'information dans la langue du « groupe cible »[385]. Plus tard, l'APD estime au cours de la même affaire que lorsqu'un traitement de données a pour « groupe cible » des personnes parlant des langages différents, il n'est pas possible de proposer, à leur égard, une information uniquement en langue anglaise[386]. À la suite du courrier du Service d'inspection informant le site internet du fait que les informations n'étaient pas fournies dans la langue du « groupe cible », des modifications à la politique de cookies avaient été apportées. Le Service d'inspection constatait alors que « les informations relatives aux cookies ne sont

[382] Groupe de travail « Article 29 », WP 260 rev. 01, *op. cit*, p. 11.
[383] *Ibidem*.
[384] APD, 17 décembre 2019, décision quant au fond 12/2019, note de bas de page n° 32.
[385] *Idem*, p. 23.
[386] *Idem*, p. 24.

désormais plus fournies qu'en anglais (ni en français ni en néerlandais) »[387], constituant une infraction à l'article 12 du RGPD.

174. La jurisprudence n'est certes pas très riche en matière d'exigences linguistiques applicables à l'obligation de transparence en matière de données à caractère personnel, mais elle semble appliquer strictement l'interprétation du Groupe de travail « Article 29 »[388]. Il apparaît *a priori* que l'Union européenne abandonne sa jurisprudence de la « langue facilement compréhensible » au profit de la langue dominante de la région de la personne concernée ciblée par le site internet. Le fait que la jurisprudence provienne de l'APD renforce d'autant plus cette apparence. En effet, la jurisprudence *Peeters* établissant la jurisprudence de la « langue facilement compréhensible » concernait un cas d'étiquetage de denrées alimentaires en français et en allemand en Flandre, donc dans une région de la Belgique où la langue dominante est le flamand : la Cour avait à l'époque déterminé que les Flamands pouvaient aisément comprendre le français ou l'allemand[389]. L'APD juge désormais le contraire en protection des données à caractère personnel : il n'est pas admis qu'une personne concernée francophone soit capable de comprendre des informations délivrées en néerlandais et en anglais.

175. Le RGPD pose ainsi un certain nombre d'obligations à la charge du responsable de traitement d'adaptation de la délivrance de l'information à la personne concernée, aussi bien en matière de langage que de langue utilisée. Néanmoins, l'ensemble de ces exigences s'évaluent par rapport aux capacités de compréhension de la « personne concernée raisonnable ». Ainsi, des adaptations de la délivrance de l'information devront être plus poussées lorsque cette information s'adresse à une personne vulnérable, qu'il s'agisse d'une personne majeure vulnérable ou en situation de handicap ou d'une personne mineure.

§2 – Les personnes vulnérables

176. À travers le droit, les États ont parfois cherché à protéger les personnes les plus vulnérables : on y retrouve notamment le droit des incapacités. Selon Gérard Mémeteau, ce corpus de texte formerait le « droit des sentiments » :

> « Il reconnaît les faibles, organise leur place dans le monde du droit. En le rédigeant, l'État est juste : il considère puis corrige les inégalités de la nature et du sort »[390].

---

[387] *Ibidem.*
[388] V. également AEPD, PS-00036-2020, publiée le 6 août 2020.
[389] CJCE, 5e ch., 18 juin 1991, ASBL Piageme et BVBA Peeters, C-369/89
[390] MÉMETEAU Gérard, « La protection de principe par l'État des personnes les plus faibles et les plus vulnérables : libres propos », Éthique publique, vol. 3, n° 1, 2001, mis en ligne le 13 septembre 2016, disponible sur : http://journals.openedition.org/ethiquepublique/2614.

Se décèle, derrière une telle qualification de la protection des personnes vulnérables comme « droit des sentiments », l'influence de Georges Ripert voyant dans la protection des faibles une traduction des « intérêts et [d]es passions du jour dans la loi, comme si c'était un progrès »[391]. Selon cette doctrine, la protection des personnes vulnérables est un déni de libéralisme et de l'autonomie de la volonté au profit de la finalité et de l'utilité des actes, voire une domination des plus faibles sur les plus forts[392]. Des dires de la Cour de cassation, cette vision du droit civil héritée de Georges Ripert est désormais obsolète, les droits fondamentaux constituant « désormais la boussole de nos systèmes juridiques »[393]. Il est vrai que la protection des personnes vulnérables a au fil du temps opéré un basculement d'une protection ayant pour objectif la protection de l'ordre public et des biens familiaux à une protection des droits et de la dignité de la personne[394].

177. La vulnérabilité se définit comme « ce qui donne prise à une attaque, et se trouve susceptible d'être pris pour cible, blessé ou lésé »[395]. En droit, cette vulnérabilité se traduit par une capacité limitée de faire ou de comprendre des choix, en une difficulté d'accès aux informations nécessaires au choix, ou encore à une dépendance particulière limitant la liberté de choix. En matière de protection des données à caractère personnel, l'adaptation de l'information devrait donc être effectuée en prenant en compte les difficultés particulières des personnes vulnérables. Cette adaptation concernerait ainsi les personnes vulnérables et en situation de handicap (1) et les « enfants » (2).

A. L'adaptation de l'information délivrée aux personnes vulnérables et en situation de handicap

178. La question de la protection des données à caractère personnel des personnes vulnérables et des personnes en situation de handicap se pose de plus en plus avec l'apparition des technologies d'assistance aux personnes âgées, aux personnes handicapées et aux personnes vulnérables[396]. En France, le ministère de l'Économie estime le nombre de personnes ayant plus

---

[391] HERRERA Carlos-Miguel, « Georges Ripert en politique », *Droits*, 2017/1, n° 65, pp. 181-199.
[392] *Ibidem.*
[393] Cour de cassation, « Étude : Les personnes vulnérables dans la jurisprudence de la Cour de cassation », *Rapport 2009*, p. 56.
[394] DAVID Stéphane, PRADO Vincent, « Protéger les personnes vulnérables », *Rapport du 116e congère des notaires de France*, 2020, disponible sur https://rapport-congresdesnotaires.fr/2020-rapport-du-116e-congres/2020-co1-p1-t1-st1-c1/#co1-p1-t1-st1-c1-s1 (consulté en février 2021).
[395] GILLET Jean-Louis, « Réflexions sur le rapport de la Cour de cassation relatif aux « personnes vulnérables » (2010) », *Les Cahiers de la Justice*, 2019, p. 649.
[396] FERRER Morte *et al.*, « Personal Autonomy in Elderly and Disabled: How assistive technologies impact on it », *in* HALTAUFDERHEIDE Joschka *et al.* (dir.), *Aging Between Participation and Simulation: Ethical Dimensions of Social Assistive Technologies in Elderly Care*, Walter de Guyter GmbH & Co KG, 2020, p. 187.

de soixante ans à vingt millions de personnes en 2030 (contre quinze en 2017)[397]. Par conséquent, BPI France estime que la silver économie est « un marché à fort potentiel estimé à 0,25 point de PIB par an et à 93 milliards d'euros qui atteindront 130 milliards en 2013 »[398]. Le marché numérique est d'ailleurs force de proposition sur le marché du bien-vieillir, du bien-vivre et de l'autonomie, à travers divers objets connectés d'aide à la mobilité, d'aide médicale, d'accompagnement vers l'autonomie, etc. Les personnes vulnérables et en situation de handicap sont ainsi des consommateurs cibles de certains marchés dans lesquels évoluent des acteurs du numérique. La question de l'adaptation de l'information délivrée aux personnes vulnérables et en situation de handicap se pose dès lors en ce qui concerne leur capacité de comprendre l'information qui leur est délivrée, afin de consentir aux traitements de leurs données à caractère personnel de manière informée.

179. L'adaptation du langage utilisé aux personnes en situation de handicap n'est pas une règle contenue dans le texte du RGPD : le terme « handicap » n'apparaît qu'à deux reprises et n'est utilisé que pour définir les notions de santé publique[399] et de données à caractère personnel concernant la santé[400]. Peut-être est-il possible de voir une évocation timide des personnes vulnérables dans le considérant 75 qui évoque le fait que « le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants », mais à la lecture de l'ensemble du RGPD, une telle interprétation relèverait d'une interprétation littérale déconnectée de la cohérence générale du règlement. Cependant, si l'adaptation du langage utilisé aux personnes vulnérables et en situation de handicap n'est pas prévue de manière explicite dans le texte, les autorités de contrôle déduisent néanmoins une telle obligation de « la nécessité pour le responsable de traitement d'évaluer le niveau probable de compréhension de son public »[401].

180. Ainsi, d'après le Groupe de travail de l'article 29, dès lors qu'un responsable de traitement a connaissance de l'utilisation de ses biens et/ou services par des personnes vulnérables ou propose des services qui ciblent des personnes vulnérables, telles que « des personnes souffrant de handicaps ou des personnes éprouvant des difficultés à accéder à

---

[397] Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, « Qu'est-ce que la silver économie ou économie des seniors ? », *Bercy Infos*, 14 novembre 2017, disponible sur https://www.economie.gouv.fr/entreprises/silver-economie-definition (consulté en juin 2022).

[398] BPI France, « Silver économie : la mise en orbite », *bpifrance.fr*, 16 juin 2016, disponible sur https://www.bpifrance.fr/nos-actualites/silver-economie-la-mise-en-orbite (consulté en juin 2022).

[399] RGPD, 27 avril 2016, considérant 54.

[400] RGPD, 27 avril 2016, considérant 35.

[401] Groupe de travail « Article 29 », WP 260 rev. 01, p. 12.

l'information »[402], ce responsable de traitement devra prendre en compte ces vulnérabilités de manière à respecter son obligation de transparence à leur égard[403]. La CNIL a également déduit du RGPD une obligation de prendre en compte les éventuelles vulnérabilités des personnes concernées. En effet, en 2017, lors de la période de mise en conformité au nouveau règlement, l'autorité de contrôle française a proposé un « pack de conformité » intitulé « Silver économie et données personnelles »[404]. À propos du consentement, le pack de conformité précise en premier lieu que les responsables de traitement ont à leur charge une obligation de vérifier que les personnes concernées ont la capacité de consentir et, en cas d'incapacité, recueillir le consentement de leurs représentants légaux[405]. En second lieu, la CNIL impose aux responsables de traitement « d'adapter les modalités de recueil du consentement en prenant en compte notamment l'état des personnes concernées, la sensibilité des données collectées et le contexte de mise en œuvre du traitement et d'utilisation du service »[406].

181. Ainsi, une attention particulière à la compréhension de l'information par les personnes vulnérables et en situation de handicap doit être accordée par le responsable de traitement en matière d'accessibilité de l'information délivrée au titre des articles 12 à 14 du RGPD. Une telle obligation de garantir l'accessibilité aux personnes vulnérables et en situation de handicap est cohérente avec la Convention des Nations unies relative aux droits des personnes handicapées, Convention, qui est d'ailleurs mentionnée par le Groupe de travail de l'article 29 dans ses lignes directrices relatives à la transparence. En effet, l'article 21 (d) de la Convention des Nations unies relative aux droits des personnes handicapées dispose que les États parties :

> « demandent instamment aux organismes privés qui mettent des services à la disposition du public, y compris par le biais de l'Internet, de fournir des informations et des services sous des formes accessibles aux personnes handicapées et que celles-ci puissent utiliser »[407].

La Convention des Nations unies propose, à cette fin, des moyens permettant de garantir aux personnes en situation de handicap d'accéder à l'information. Parmi les moyens que les organismes privés peuvent mettre en œuvre pour faciliter l'accès des personnes en situation de handicap à l'information et à la communication, la Convention évoque notamment comme moyens de communication « les langues, l'affichage de texte, le braille, la communication

---

[402] *Ibidem.*
[403] *Ibidem.*
[404] CNIL, « Silver économie et données personnelles », *Pack de conformité*, novembre 2017, disponible sur https://www.cnil.fr/sites/default/files/atoms/files/pack_silver_economie_v4.pdf (consulté en janvier 2021).
[405] *Ibidem.*
[406] *Ibidem.*
[407] Convention des Nations unies relatives aux droits des personnes handicapées, Article 21 (d).

tactile, les gros caractères, les supports multimédias accessibles ainsi que les modes, moyens et formes de communication améliorée et alternative à base de supports écrits, supports audio, langue simplifiée et lecteur humain »[408].

182. Le Conseil national du numérique (CNNum) s'est également intéressé à l'accessibilité de l'information aux personnes en situation de handicap. Dans son avis relatif à l'application « StopCovid », la recommandation n° 12 adoptée par le CNNum recommande au gouvernement l'utilisation du français facile à lire et à comprendre (FALC)[409]. Comme son nom l'indique, le français facile à lire et à comprendre (FALC) est une façon de délivrer l'information simplifiée, ayant pour objectif la compréhension facile de l'information par son récepteur. Par exemple, le rédacteur d'un texte en FALC n'utilisera par exemple ni métaphore, ni acronyme, ni abréviations, privilégiera les phrases courtes actives et sans négations, n'évoquera qu'une seule idée par phrase et prendra le soin d'utiliser un vocabulaire simple[410]. Les règles européennes pour une information facile à lire et à comprendre prêtent également une importance particulière à la mise en page, bannissant les polices d'écriture à empattement (comme le Times New Roman ici utilisé), les lettrages trop rapprochés ou encore un choix de couleur rendant la lecture plus difficile[411]. En effet, l'utilisation d'un langage simplifié présente des vertus au niveau de la compréhension de la personne concernée à la fois pour des personnes atteintes de déficience intellectuelle, mais aussi à d'autres publics présentant des difficultés de lecture et de compréhensions telles que « les personnes ayant une dyslexie ou un trouble du spectre de l'autisme, les personnes de langue étrangère, malentendantes, âgées ou encore les jeunes enfants »[412]. Contrairement à un affichage grossi du texte de la politique de protection des données ou la proposition d'une lecture vocale du texte rédigé, l'utilisation du français facile à lire et à comprendre nécessite de « changer le contenu du texte lui-même » pour l'adapter aux personnes porteuses de déficience intellectuelle[413].

183. L'adaptation de l'information délivrée aux personnes vulnérables et aux personnes en situation de handicap ne semble pas, pour l'instant, faire l'objet de décisions des autorités de contrôle. Une telle adaptation de l'information délivrée aux personnes concernées demande des

---

[408] Convention des Nations unies relatives aux droits des personnes handicapées, Article 2.
[409] CNNum, « Stop Covid », Avis du Conseil national du Numérique, 24 avril 2020..
[410] ANCET Pierre, « L'écart entre les lois et les pratiques : le problème du statut des personnes », *in* MASSE Manon *et al.* (dir.), *Accessibilité et participation sociale. Vers une mise en œuvre de la Convention relative aux droits des personnes handicapées*, IES éditions, 2020, p. 36.
[411] UNAPEI, *L'information pour tous. Règles européennes pour une information facile à lire et à comprendre*, 2009, p. 15.
[412] DIACQUENOD Cindy, SANTI France, « La mise en œuvre du langage facile à lire et à comprendre (FALC) : enjeux, défis et perspectives », *Revue suisse de pédagogie spécialisée,* 2018, p. 30.
[413] ANCET Pierre, *op. cit.*, p. 34.

efforts importants et la mobilisation de compétences particulières de la part du responsable de traitement, qui peuvent sembler excessifs d'un point de vue économique. Le poids économique de l'adaptation du langage aux personnes vulnérables et en situation de handicap explique peut-être l'absence d'une telle obligation au sein du RGPD, et la circonscription du champ d'application d'une telle obligation aux traitements visant particulièrement ce public par la CNIL. Pourtant, protéger le consentement éclairé de ces personnes représente un enjeu important pour l'effectivité de la protection des données à caractère personnel et de sa logique d'*empowerement* au sein de l'Union européenne.

184. Idéalement, l'adaptation de l'information aux personnes vulnérables devrait être généralisée à l'ensemble du principe de transparence. En effet, il faut noter que plus d'un cinquième de la population de l'Union européenne était âgé de soixante-cinq ans et plus[414] et que le handicap touche une personne sur six au sein de l'Union européenne[415]. Si l'ensemble de la population âgée de plus de soixante-cinq and et des personnes touchées par un handicap ne nécessitent pas une adaptation de l'information pour émettre un consentement éclairé, le potentiel de personnes nécessitant une telle adaptation paraît suffisamment important pour justifier l'effort économique[416]. De plus, l'adaptation de l'information aux personnes vulnérables et en situation de handicap s'inscrit dans un projet de société plus large visant à inclure ces populations dans la société ainsi qu'à promouvoir leur participation et leur autonomie. Ainsi, en 2018, le Défenseur des droits rappelait à propos du principe général d'accessibilité :

> « La CIPH appréhende la question de l'accessibilité dans le contexte de l'égalité et de la non-discrimination. Ce n'est donc pas, une simple de question de respect de normes techniques destinées à répondre à des besoins catégoriels. C'est avant tout une condition préalable et essentielle pour garantir aux personnes handicapées, quel que soit leur handicap, un accès effectif aux droits civils, politiques, économiques, sociaux et culturels, sur la base de l'égalité avec les autres ».[417]

---

[414] Eurostat, « Structure et vieillissement de la population », *ec.europa.eu*, 21 décembre 2020, disponible sur https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Structure_et_vieillissement_de_la_population&oldid=510188 (consulté en juin 2022).

[415] Ministère de la Transition économique et de la Cohésion des territoires, Ministère de la Transition énergétique, « L'Union européenne, droits des personnes handicapées et accessibilité », *ecologie.gouv.fr*, 21 mai 2021, disponible sur https://www.ecologie.gouv.fr/lunion-europeenne-droits-des-personnes-handicapees-et-accessibilite (consulté en juin 2022).

[416] D'autant plus que cette adaptation pourrait bénéficier à d'autres populations telles que les personnes en situation d'illettrisme numérique ou encore les personnes dont le français n'est pas la langue maternelle.

[417] Défenseur des droits, *La Convention relative aux droits des personnes handicapées. Comprendre et mobiliser la Convention pour défendre les droits des personnes handicapées*, Guide, décembre 2016, p. 16.

L'accessibilité de l'information nécessaire à l'exercice de ses droits en matière de protection des données à caractère personnel ne doit pas, dans ce cadre, être cantonnée aux secteurs d'activité dont les personnes vulnérables et en situation de handicap sont le public cible. L'approche catégorielle française avait d'ailleurs été dénoncée en 2018 par un petit nombre de députés qui avaient appelé à la reconnaissance de la personne en situation de handicap comme un « citoyen ordinaire » et à la mise en place de règles leur permettant d'accéder à ce principe[418]. Une loi à article unique avait alors été proposée, incitant le législateur à sortir d'une logique sectorielle au profit d'une approche plus générale de la prise en compte du handicap :

> « Tout projet de réforme envisagé par le Gouvernement fait l'objet d'une réflexion préalable en vue de son adaptation à la situation des personnes handicapées et prévoit, autant que besoin, les dispositions législatives ou réglementaires nécessaires à cette adaptation »[419].

185. Ainsi, le RGPD ne permet pas de prendre en compte de manière générale les personnes vulnérables et en situation de handicap en requérant des responsables de traitement la mise en œuvre du principe de transparence qui soit également accessible à ces populations. Tout au plus, les autorités de contrôle vont exiger des responsables de traitement l'adaptation de l'information aux personnes vulnérables et en situation de handicap quand les traitements les ciblent directement ou quand le service utilisé est principalement utilisé par des personnes vulnérables[420]. Pourtant, le RGPD protège particulièrement une autre population de personnes concernées vulnérables, qui est directement identifiée par le règlement : les enfants.

B. L'adaptation de l'information délivrée aux enfants

186. Sous le règne de la directive 95/46/CE, la protection des données à caractère personnel était indifférente à l'âge des personnes concernées, en adoptant une « approche indifférente à l'âge » (« *age-blind approach* »)[421]. Cette omission avait été dénoncée, notamment par « les défenseurs de la protection de l'enfance [qui] estiment qu'il est crucial de prendre des mesures

---

[418] Assemblée nationale, *Proposition de loi relative à une société plus inclusive pour les personnes en situation de handicap*, n° 798, 21 mars 2018, renvoyée à la Commission des affaires sociales.
[419] *Idem*, Article unique.
[420] Par exemple, l'autorité de protection des données italienne reproche à TikTok de ne pas suffisamment protéger la vie privée des enfants alors que le réseau est « utilisé avant tout par les très jeunes », préférant retenir la population qui utilise de manière effective l'application plutôt que son public cible officiellement déclaré. v. notamment GPDP, « Tik Tok, a rischio la privacy dei minori: il Garante avvia il procedimento contro il social network », *gpdp.it*, 22 décembre 2020, disponible sur https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9508923 (consulté en juin 2022).
[421] MACENAITE Milda, KOSTA Eleni, « Consent for processing children's personal data in the EU: following in US footsteps? », *Information & Communications Technology Law*, Volume 26, 2017, Issue 2.

pour garantir que les enfants bénéficient de la richesse des possibilités offertes par internet, maintenant et à l'avenir, sans être simultanément exploités, surveillés ou « monétisés » »[422].

187. Lors de l'élaboration du Règlement, le législateur européen a eu à cœur de protéger plus particulièrement les enfants en raison de leur caractère vulnérable. En effet, selon le considérant 38 du RGPD, « les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des garanties et de leurs droits liés au traitement des données à caractère personnel ». Ce constat a une conséquence juridique directe en matière de transparence puisque le considérant 58 du RGPD en déduit que « les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre ».

188. Avant de s'intéresser aux mesures créées par le législateur européen pour protéger plus particulièrement le consentement éclairé des enfants, il faut préalablement s'intéresser à la notion d'« enfant » dans le RGPD. En effet, la notion d'enfant n'est pas définie par le RGPD : cette absence peut interroger dans la mesure où le RGPD ne compte pas moins de vingt-six occurrences du mot « enfant ».

189. Pourtant, dans la proposition initiale de la Commission, la notion d'enfant était doublement définie. En effet, le considérant (29) disposait :

> « *To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention of the Rights of the Child* »[423].

Selon l'article 1 de la Convention des Nations Unies, « un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable ». Cette définition correspondait en partie à la définition proposée par l'article 4 (18) de la proposition de règlement puisque celle-ci définissait l'enfant comme toute personne ayant moins de dix-huit ans.

190. Cette définition n'a pas fait l'unanimité auprès des parlementaires. En effet, elle avait fait l'objet de plusieurs amendements, que ce soit pour abaisser l'âge à treize ans[424] ou quatorze

---

[422] « *child welfare advocates [who] believe it is crucial to take steps to ensure that children benefit from the wealth of opportunities, enabled by the internet, now and in the future without being simultaneously exploited, surveilled or "monitised"* » [traduction libre]. LIVINGSTONE Sonia, « *Children: a special case for privacy*? », *Intermedia* 46(2), p. 18.

[423] Commission européenne, COM (2012) 11 final, *op. cit.*, considérant (29), p. 22.

[424] Parlement européen, Commission LIBE, *Draft report on 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*, 2009-2014, PE506.045, Amendements 797 et 798.

ans[425] ou pour remplacer la notion d'« enfant » par celle de « mineur »[426]. Finalement, aucune définition d'enfant n'est présente dans le RGPD. Cependant, le Règlement permet aux États membres de définir la notion d'enfant au sens du Règlement, dans la mesure où il offre une marge de manœuvre quant au champ d'application des dispositions applicables aux enfants. Le Règlement permet ainsi aux États Membres de « prévoir par la loi un âge inférieur pour ces finalités [(les dispositions applicables aux enfants)] pour autant que cet âge inférieur ne soit pas en dessous de 13 ans ». Par cette règle, le législateur européen a considéré que l'âge de treize ans était l'âge minimum à partir duquel l'enfant pouvait prendre des décisions pour lui-même, c'est-à-dire un âge à partir duquel l'enfant peut être suffisamment mûr pour acquérir « la capacité cognitive de comprendre suffisamment leur situation, et ainsi, de donner leur consentement »[427]. La nécessité pour les enfants de pouvoir comprendre pour consentir est d'autant plus importante concernant les données à caractère personnel que « les pratiques en matière de traitement de données impliquent souvent des méthodes manipulatrices et évocatrices qui peuvent être difficilement perceptibles pour les individus »[428], méthodes qui rendent les enfants, dont le développement cognitif n'est pas encore mature, particulièrement vulnérables. Ainsi, la protection particulière du consentement des enfants s'explique par la difficulté d'obtenir un consentement éclairé de ces derniers du fait de leurs capacités cognitives.

191. La tranche d'âge de treize à seize ans se justifie par deux éléments : l'état du développement cognitif de l'enfant et la culture de l'État membre. Premièrement, l'âge de treize à seize ans est justifié par le fait que le législateur considère qu'à cet âge, l'appareil cognitif de l'enfant est suffisamment mature pour comprendre les informations qui lui sont présentées et d'exercer un consentement éclairé qui prend en compte les risques associés aux traitements de données faisant l'objet du consentement. Cette approche semble globalement s'accorder avec les études de psychologie cognitive. Par exemple, selon Vivian E. Hamilton,

> « *general cognitive capacity – i.e., the abilities to process information, understand and reason from facts, and assess and appreciate the nature of a given situation – improves into-mid-adolescence. By age sixteen, these basic cognitive abilities are mature* »[429].

---

[425] *Idem,* Amendement 796.
[426] *Idem,* Amendement 799.
[427] « *the cognitive ability to sufficiently understand their position, and hence, to give consent* ». VAN DER HOF Simone, « I Agree or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World », *Wisconsin International Law Journal*, vol. 34, no. 2, Winter 2016, p. 421.
[428] « *data processing practices often entail manipulative and evocative methods that can be hard to see through for individuals* ». VAN DER HOF Simone, « I Agree or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World », *Wisconsin International Law Journal*, vol. 34, no. 2, Winter 2016, p. 433.
[429] HAMILTON Vivian E., « Immature Citizens and the State", *BYU Law Rev.*, 2010, p.1055.

Deuxièmement, la définition de l'enfant peut également relever de la culture de l'État membre, culture qui peut d'ailleurs avoir des effets sur le développement cognitif de celui-ci[430]. Les âges retenus pour la protection des données de l'enfant sont d'ailleurs très différents d'un État à l'autre : aux États-Unis, le *Children's Online Privacy Protection Act* (COPPA) protège les mineurs de treize ans[431] ; au Brésil, la Lei Geral de Proteção de Dados (LGPD) protège les enfants et les adolescents jusqu'à dix-huit ans[432] ; en Thaïlande, le *Personal Data Protection Act* (PDPA) protège les mineurs de dix ans, et la protection s'étend jusqu'à vingt ans si le mineur n'a pas acquis la compétence de donner son consentement selon les dispositions du droit commun thaïlandais[433]. En France, l'âge de quinze ans correspond à la fois au développement cognitif de l'enfant, mais également à une étape culturelle de son développement qui est l'entrée au lycée.

192. La question d'inclure uniquement les enfants dans la protection du RGPD ou d'y inclure également les adolescents a été discutée dans l'hémicycle du Parlement européen. Finalement, les députés européens ont voulu permettre aux États membres de protéger également les adolescents s'ils le souhaitaient. Lors du premier débat au Parlement européen, Anna Maria Corazza Bildt argumentait en faveur d'une l'information « adaptée aux enfants et facile à comprendre, car les adolescents peuvent ne pas être conscients et des conséquences et se contenter de cliquer frénétiquement »[434]. D'ailleurs, l'insouciance de la « jeune génération » et leur comportement en découlant sur internet, a été très présente dans les débats. Une des expressions les plus révélatrices de cet état d'esprit a été l'intervention de la députée hongroise Kinga Gál lors des débats aboutissant à l'adoption du texte en première lecture :

> « Je me souviens bien de l'époque où nous luttions encore – dans le cadre de nos libertés – pour ne pas être surveillés, pour ne pas donner l'accès à nos données. Grotesquement, une génération ou deux plus tard, nos jeunes le font aujourd'hui volontairement. Ils mettent leurs propres informations personnelles à la disposition de tous »[435].

---

[430] TROADEC Bertrand, « La relation entre culture et développement cognitif : une introduction », *Enfance*, 2006/2, vol. 58, pp. 108-117 ; MAYNARD Ashley, GREENFIELD Patricia, « Le rôle des outils et des artefacts culturels dans le développement cognitif », *Enfance*, 2006/2, vol. 58, pp. 135-145.
[431] Children's Online Privacy Protection Rule (COPPA), §312.2.
[432] Lei Geral de Proteção de Dados (LGPD), article 14.
[433] Personal Data Protection Act, Chapter II, Part 1, Section 20.
[434] Information « *should be child-friendly and easy to understand, because teenagers may not be aware of the consequences and just «click it away'* ». Parlement européen, Protection of individuals with regard to the processing of personal data – processing of personal data for the purpose of crime prevention (debate), Strasbourg, 11 mars 2014, CRE 11/03/2014 – 13, 2012/0011 (COD).
[435] *Ibidem.*

L'ensemble de ces données cognitives et sociologiques justifient ainsi une obligation d'information renforcée quant à son accessibilité à destination des enfants.

193. Cependant, l'article 8 n'est pas très clair sur l'existence ou non d'une obligation de double consentement de l'enfant et du titulaire de la responsabilité parentale. L'obligation d'information est indifférente de la solution retenue dans la mesure où, que l'enfant consente ou soit associé au consentement des titulaires de la responsabilité parentale, l'information ne pourra être valide pour l'enfant que dans la mesure où celui-ci la comprend. L'indifférence du droit à l'information à la nature de l'association de l'enfant sur les choix qui le concernent a été fortement confirmée en 2018 par le Groupe de Travail « Article 29 » :

> « WP 29 emphasises in particular that children do not lose their right as data subjects to transparency simply because consent has been given/authorised by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies ».

L'association de l'enfant dans les choix qui le concernent suit une évolution juridique qui ne s'intéresse pas uniquement le domaine des données à caractère personnel. La Convention des droits de l'enfant, dispose en effet, dans son article 12 qu'il doit être conféré à « l'enfant qui est capable de discernement, le droit d'exprimer librement son opinion sur toutes les questions l'intéressant, les opinions de l'enfant étant dûment prises en considération eu égard à son âge et à son degré de maturité ».

194. L'association de l'enfant dans les décisions qui le concernent a déjà été consacrée dans plusieurs domaines juridiques. En droit médical, la déclaration d'Amsterdam[436] sur la promotion des droits des patients en Europe et la Convention d'Oviedo[437] reconnaissent toutes deux l'association de l'enfant à la prise de décision en fonction de ses capacités. Cette idée est reprise en droit national, comme dans l'article L. 1111-2 du code de la santé publique sur le droit à l'information en matière médicale, qui dispose que les mineurs « ont le droit de recevoir eux-mêmes une information et de participer à la prise de décision les concernant, d'une manière adaptée […] à leur degré de maturité ». L'association de l'enfant dans les décisions qui le concernent a aussi été largement constatée en droit de la famille, son consentement étant notamment requis en matière d'adoption[438].

---

[436] « Le patient mineur doit être associé à la prise de décision, dans toute la mesure où ses capacités le permettent ». OMS, *Déclaration sur la promotion des droits des patients en Europe*, Amsterdam, 1994.

[437] « L'avis du mineur est pris en considération comme un facteur de plus en plus déterminant en fonction de son âge et de son degré de maturité ». Convention sur les droits de l'homme et de la biomédecine, Oviedo, 1997, Article 7.

[438] EUDIER Frédérique, « Adoption – Adoption plénière », *Répertoire de droit civil*, octobre 2008, § 262-263.

195. Ainsi, en matière de protection des données à caractère personnel, le législateur a considéré que « conformément aux exigences de la Convention des Nations unies relative aux droits de l'enfant, les enfants devraient être de plus en plus consultés sur les questions qui les concernent et les solutions en matière de consentement pourraient donc aller de la simple consultation de l'enfant au consentement parallèle ou conjoint de l'enfant et d'un parent, voire au consentement autonome d'un enfant mûr »[439].

Le législateur, ayant ainsi associé l'enfant aux décisions qui le concernent en matière de traitement de données à caractère personnel, a créé une obligation à la charge du responsable du traitement :

> « Les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre »[440].

196. En 2008, le Groupe de travail « Article 29 » avait conclu à une obligation similaire en interprétant largement la directive 95/46/CE comme créant « l'obligation d'informer de manière adéquate la personne concernée (articles 10, 11 et 14) »[441], alors même que la directive ne comportait en matière d'information que des obligations de mention. Le Groupe de travail « Article 29 » préconisait ainsi que « priorité doit être donnée aux messages structurés, rédigés dans un langage simple, concis et pédagogique facilement accessible »[442]. Ces recommandations peinaient d'ailleurs à s'appliquer : en 2015, lors de l'examen par la CNIL de cinquante-quatre sites internet qui s'adressaient aux enfants et adolescents, l'autorité de contrôle avait constaté que « seulement 33 % [de ces sites internet] adaptent l'information au jeune public visé »[443].

197. En 2018, le Groupe de travail « Article 29 » a étoffé cette obligation et interprète le considérant 38 du RGPD en considérant que le responsable de traitement « doit veiller à ce que

---

[439] « *following the requirements of the UN CRC, children should be increasingly consulted on matters relating to them and thus solutions for consent could range from mere consultation with the child, to parallel or joint consent of the child and a parent, or even to the autonomous consent of a mature child* ». MACENAITE Milda, KOSTA Eleni, *op. cit.*, Issue 2.

[440] RGPD considérant 58. Cette phrase est puisée directement de l'avis du Conseil pendant les négociations du RGPD, voir Conseil de l'Union européenne, *Position of the Council at first reading with a view to the adoption of a regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* -, Bruxelles, 8 avril 2016, 2012/0011 (COD).

[441] Groupe de travail Article 29, *Document de travail sur la protection des données à caractère personnel de l'enfant (cas particulier de l'école)*, 18 février 2008, 00483/08/FR, WP 147, p. 10.

[442] *Ibidem.*

[443] CNIL, « Vie privée des enfants : une protection insuffisante sur les sites Internet », *CNIL.fr*, 2 septembre 2015, disponible sur https://www.cnil.fr/fr/vie-privee-des-enfants-une-protection-insuffisante-sur-les-sites-internet-0 (consulté en octobre 2020).

le vocabulaire, le ton et le style du langage utilisé soient appropriés et trouvent un écho auprès des enfants afin que l'enfant destinataire de l'information reconnaisse que le message/l'information lui est destinée »[444]. Le Groupe de travail donne comme exemple de langage approprié pour un enfant l'adaptation proposée par l'UNICEF à destination des enfants de la Convention sur les droits des enfants[445].

198. Dans un guide destiné à l'adaptation de la Convention des droits de l'enfant dans un langage adapté aux enfants, l'UNICEF considère également que non seulement l'information doit être facilement compréhensible par l'enfant, mais doit également les inviter à interagir avec le document[446]. Pour parvenir à un tel résultat, le document liste une série de critères établie par des enfants pour parvenir à un langage adapté aux enfants : l'auteur d'un document adapté aux enfants se devra d'utiliser un langage clair et simple, d'expliquer les mots qui peuvent être difficiles à comprendre, d'illustrer ses propos par des exemples, d'utiliser des couleurs et des images qui parlent aux enfants[447].

199. Ainsi, le responsable de traitement est tenu d'adapter l'information qu'il délivre aux enfants, tels que définis par le droit national des États membres dans lequel il traite des données à caractère personnel d'enfants. L'adaptation de l'information revêt les mêmes modalités que l'adaptation de l'information à la personne concernée puisqu'il s'agit d'adapter l'information délivrée à un niveau compréhensible par sa cible. L'intensité de l'information diffère cependant puisque la particularité des enfants réside dans une capacité de compréhension et d'attention diminuée. Le responsable de traitement doit donc recourir à des techniques de communication particulières, se traduisant dans l'utilisation d'images, de vocabulaire simple, de systèmes interactifs, etc.

200. Conclusion de section. – Le RGPD est une avancée substantielle en ce qui concerne l'accessibilité du contenu de l'information. En effet, le législateur a annihilé la possibilité pour les responsables de traitement de recourir à des techniques d'influence ou de manipulation de la personne concernée en ayant recours à un discours trop juridique, trop technique ou difficile

---

[444] « *it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/ information is being directed at them* ». Groupe de travail « Article 29 », WP260 rev.01, *op. cit.*, p. 10.

[445] UNICEF, « La Convention relative aux droits de l'enfant – Version pour les enfants », *unicef.org*, disponible sur https://www.unicef.org/fr/convention-droits-enfant/convention-droits-version-enfants (consulté en octobre 2020). Mentionné par le Groupe de travail « Article 29 », WP260 rev.01, *op. cit.*, p. 10.

[446] UNICEF et al., *Adapting the Child-Friendly Example of the Convention on the Rights of the Child (Convention) with and for Children in your Context*, p. 4, disponible sur https://www.childrightsconnect.org/wp-content/uploads/2019/08/cf_crc_translation_guide_final.pdf

[447] *Ibidem.*

à lire. Désormais, la compréhension de la personne concernée constitue la règle, le standard à atteindre, qui à défaut d'être atteint, sera sanctionné au titre du manquement à l'obligation de transparence et dans le cadre du consentement, à l'invalidation du consentement pour faute d'information nécessaire à l'obtention d'un consentement éclairé. Le RGPD protège également les personnes particulièrement défavorisées face au responsable de traitement, et notamment les enfants. Cependant, il est regrettable que, si l'adaptation relative à l'information délivrée à l'enfant constitue un cadre juridique solide permettant à celui-ci de comprendre l'information qui lui est ainsi délivrée, le législateur européen ait exclu les autres populations vulnérables de sa protection. Une interprétation fidèle à l'esprit plutôt qu'à la lettre du règlement pourrait aboutir à une obligation pour les responsables de traitement proposant des biens et services dirigées vers les personnes vulnérables, alors même que les données à caractère personnel de ces personnes vulnérables font l'objet de traitements de données dont elles ne sont pas le public cible.

Conclusion du Chapitre 1

201. Les conditions formelles attachées à l'obligation d'information ont permis de renforcer la réalité du caractère éclairé du consentement de la personne concernée. Désormais, la personne concernée a accès à l'information à la fois physiquement et intellectuellement.

202. Physiquement, l'évolution de l'obligation de transparence à un droit à l'information a permis d'interpréter concrètement la possibilité pour la personne concernée d'accéder à l'information. En effet, le responsable de traitement est lié par une obligation de résultat de délivrance de l'information. Dès lors, l'évaluation du respect ou non des dispositions relatives à la transparence ne se réfère plus aux moyens utilisés par le responsable de traitement, mais à la capacité concrète pour la personne concernée d'accéder à l'information.

203. Intellectuellement, l'évolution est similaire. Le législateur européen a en effet créé à la charge du responsable de traitement l'obligation d'adapter le langage et la langue de l'information aux personnes concernées dont les données sont traitées. Également évaluée dans une logique d'obligation de résultat, l'adaptation de l'information nécessite d'éliminer tout langage ou toute syntaxe complexe ou technique au profit d'un vocabulaire ordinaire et d'une structure grammaticale simple. L'adaptation de l'information devient plus intense lorsque le public cible du responsable de traitement se compose de personnes vulnérables, en particulier les enfants, ce qui révèle l'ambition du législateur de garantir à tous l'accès à l'information.

204. Cependant, il est parfois regrettable que le législateur ne soit pas allé plus loin dans la mise en œuvre de cet objectif. Notamment, le législateur européen a manqué l'opportunité d'intégrer la logique d'*accountability* aux moyens de délivrance de l'information et de protéger de manière plus importante les personnes vulnérables pour les accompagner dans l'exercice de leur consentement.

205. Au-delà des conditions formelles qui, malgré un bilan nuancé, constituent une avancée dans la réalité du consentement éclairé, les conditions matérielles s'intéressent au fond de l'information délivrée, afin que la personne concernée ait l'ensemble des informations nécessaires à sa prise de décision.

CHAPITRE 2 – LES CONDITIONS MATÉRIELLES ATTACHÉES A L'OBLIGATION D'INFORMATION

206. Les conditions matérielles du principe de transparence sont une traduction de la double nature obligation-droit de ce principe. Les conditions matérielles sont d'abord une obligation de résultat à la charge du responsable de traitement de transmettre un certain nombre de données à la personne concernée. Elles peuvent également être considérées comme la substance du droit à l'information, déterminant l'ensemble des informations nécessaires pour que la personne concernée puisse, à la fois, avoir le contrôle de ses données à caractère personnel et exprimer un consentement de manière éclairée.

207. Les conditions matérielles peuvent également être envisagées selon le prisme plus large du double objectif du RGPD : protéger les personnes concernées tout en assurant la libre circulation des données à caractère personnel sur le marché numérique. L'élan de transparence « promu avec vigueur » par l'Union européenne sur le marché[448] rencontre alors la dimension protectrice du droit à l'information (Section 1).

208. À ce titre, les articles 13 et 14 du RGPD énumèrent de manière précise les informations à fournir lorsque les données à caractère personnel traitées sont collectées auprès de la personne concernée (Article 13) ou sont obtenues par d'autres moyens (Article 14). La multiplication des informations que le responsable de traitement doit transmettre à la personne concernée par rapport au régime précédent de la directive 95/46/CE révèle une volonté du législateur de lutter contre l'opacité de certaines pratiques en matière de traitement de données à caractère personnel. Cette volonté se traduit par la recherche de l'exhaustivité des informations nécessaires à la personne concernée pour exprimer un consentement éclairé (Section 2).

[448] DIEUX Xavier, *Droit, morale et marché,* Bruxelles, Bruylant, 2003, pp. 441-442.

Section 1 – Raison d'être des conditions matérielles

209. Les conditions matérielles de l'obligation d'information ont comme objectif de délivrer l'ensemble exhaustif des informations nécessaires à la personne concernée afin que celle-ci soit correctement informée sur les traitements de ses données à caractère personnel.

210. Le terme « exhaustif » se définit, au figuré, comme « ce qui épuise une matière, une question, qui traite un sujet d'étude à fond et sans rien omettre »[449]. Cette définition fait écho à une des facettes du consentement éclairé tel que développé par Cicéron, celle de l'obligation de bonne foi et de transparence de l'offrant[450]. C'est ainsi dans cette démarche que s'inscrivent les conditions matérielles attachées à l'obligation de transparence en matière de protection des données à caractère personnel. En effet, l'exhaustivité va éclairer le choix de la personne concernée aussi bien au niveau de son choix économique (§1) que de son choix juridique (§2).

§1 – Le rôle économique des conditions matérielles

211. Si le rôle de la transparence dans le marché ne relève d'aucun consensus dans la littérature scientifique quant à son effet positif ou négatif sur le marché financier[451], le rôle de la transparence a quant à lui été rapidement souligné lorsqu'il s'agissait de l'information du consommateur. L'évolution technologique, et plus particulièrement la généralisation de l'usage d'internet et des technologies mobiles, « a rapproché les marchés de l'état utopique de *l'information parfaite* en réduisant l'asymétrie informationnelle entre les vendeurs et les acheteurs »[452].

212. Au sein de l'Union européenne, la prise en compte du rôle bénéfique de la transparence pour la protection du consommateur est exprimée au cœur même du Traité sur le fonctionnement de l'Union européenne :

> « Afin de promouvoir les intérêts des consommateurs et d'assurer un niveau élevé de protection des consommateurs, l'Union contribue […] à la promotion de leur droit à l'information […] »[453].

---

[449] CNRTL, « Exhaustif, ve », *Portail Lexical*, Lexicographie, disponible sur https://www.cnrtl.fr/definition/exhaustif (consulté en février 2021).
[450] CICERON, *De officiis*, *op. cit.*
[451] EOM Kyong Shik *et al.*, « Pre-Trade Transparency and Market Quality », *Journal of Financial Markets*, 2007, vol 10 p. 319.
[452] « *The Internet and mobile technologies have brought markets closer to the utopian state of perfect information by reducing the information asymmetries between sellers and buyers* » [traduction libre]. GRANADOS Nelson, GUPTA Alok, « Transparency Strategy: Competing with Information in a Digital World », *MIS Quarterly*, Juin 2013, vol. 37, p. 637.
[453] Article 169 TFUE (ex-article 153 TCE).

La Commission européenne a ainsi, sur la base du TFUE, œuvré pour protéger le consommateur européen en protégeant notamment son droit à l'information. La Commission a d'ailleurs affirmé en 2012 sa volonté de mener une « politique des consommateurs » et en a dégagé deux effets vertueux pour le marché européen : « favoriser la confiance et la croissance » et renforcer la sécurité des consommateurs[454].

213. En 2018, le Crédoc a mené une enquête sur les freins à l'utilisation d'internet dans la population française concluant au fait que « la protection des données est considérée par 40 % de la population comme le principal frein à l'utilisation d'internet »[455], d'autant plus que « pour 86 % des français il est sûr ou probable que des logiciels capables de transmettre des informations à l'insu des utilisateurs soient installés sur les téléphones mobiles »[456]. Les résultats de cette enquête avaient alors montré un déficit important de confiance dans le marché numérique.

214. Or, la confiance est très importante pour l'Union européenne parce qu'elle est utile au bon fonctionnement du marché. La confiance peut en effet être décrite comme « un des rouages de la coopération et de la fluidité des marchés »[457]. Concernant le marché numérique, la protection des données à caractère personnel intéresse particulièrement les usagers. En 2003, la Commission européenne reconnaissait déjà le rôle fondamental de la confiance dans le marché numérique européen :

> « L'objectif n'est pas uniquement d'améliorer les pratiques en matière de protection de la vie privée, mais également d'accroître la transparence et, partant, la confiance des utilisateurs et de donner la possibilité à ceux qui investissent dans le respect de la vie privée et même en accroissent la protection de montrer leurs résultats dans ce domaine et d'en faire un avantage concurrentiel »[458].

215. L'inclusion des enjeux relatifs à la protection de la vie privée et des données à caractère personnel va alors inciter le législateur à encourager la confiance à travers plusieurs leviers que constituent le droit de la consommation et la protection des données à caractère personnel. À ce titre, la Communication de la Commission intitulée « Un agenda du consommateur européen

---

[454] Commission européenne, *Un agenda du consommateur européen – Favoriser la confiance et la croissance*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Bruxelles, 22 mai 2012, COM (2012) 225 final.
[455] Crédoc, *Baromètre du numérique 2018*, 18e édition, p. 195.
[456] *Idem*, p. 199.
[457] HOIBIAN Sandra, « Demande de transparence ou de sincérité ? », *Constructif*, 2018/3, n°51, p. 6.
[458] Commission des Communautés européennes, *Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)*, Rapport de la Commission, Bruxelles, 15 mai 2003, COM (2003) 265 final, p. 19.

– Favoriser la confiance et la croissance » avait eu, en 2012, pour objet d'accroître la confiance sur le marché, dont le marché numérique. Il a cependant été regretté que la Commission ne couvre pas l'ensemble des enjeux liés au marché numérique puisque la protection des données à caractère personnel est plus large que la protection des consommateurs dans la mesure où elle protège les individus « y compris lorsqu'ils n'agissent pas en tant que consommateurs »[459]. Ainsi, la protection du consommateur et la protection des données à caractère personnel sont complémentaires et « peuvent créer des synergies utiles, notamment dans l'environnement numérique »[460].

216. Ainsi, la confiance doit être générée, protégée et garantie sur le marché numérique, que l'on se place du côté du consommateur ou de l'individu non consommateur, c'est-à-dire la personne concernée. Dans ses récentes communications détaillant la priorité 2019-2024 « Une Europe adaptée à l'ère numérique », la Commission européenne inclut dans sa stratégie la confiance sur le marché numérique. La Commission a ainsi déclaré, dans une Communication intitulée « Façonner l'avenir numérique de l'Europe », que la confiance va au-delà des aspects de cybersécurité[461] et qu'ainsi, « les citoyens doivent faire confiance à la technologie elle-même, ainsi qu'à la manière dont elle est utilisée »[462]. La Commission a réaffirmé en 2020 que la confiance numérique instaurée par le RGPD était partie intégrante de la stratégie européenne pour les données, qui a pour but de conduire à « une économie fondée sur les données au cours des cinq prochaines années »[463].

217. Concernant les nouvelles technologies, la confiance incorporera le libellé du texte, à l'image du *Livre blanc sur l'intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance*[464]. En France, la notion de confiance a même intégré le vocabulaire législatif avec la loi du 21 juin pour la confiance dans l'économie numérique[465], dont certains

---

[459] EDPS, « Commentaire du CEPD sur la communication de la Commission – Un agenda du consommateur européen – Favoriser la confiance et la croissance », 16 juillet 2012, disponible sur https://edps.europa.eu/data-protection/our-work/publications/comments/european-consumer-agenda-boosting-confidence-and_fr

[460] *Ibidem.*

[461] Le rôle crucial de la cybersécurité pour engendrer la confiance dans les nouvelles technologies a tout de même été récemment souligné par la Commission européenne, voir Commission européenne, Haut représentant de l'Union pour les affaires étrangères, « The EU's Cybersecurity Strategy for the Digital Decade », *Joint Communication to the European Parliament and the Council*, Bruxelles, 16 décembre 2020, JOIN (2020) 18 final.

[462] Commission européenne, COM (2020) 67 final, *op. cit.*, p. 6.

[463] Commission européenne, COM (2020) 66 final, *op. cit*.

[464] Commission européenne, *Livre blanc sur l'intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance*, Bruxelles, 19 février 2020, COM (2020) 65 final.

[465] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JO n°143 du 22 juin 2004.

objectifs, tels que la lutte contre la publicité et la prospection indésirables en ligne, relèvent de la protection des données à caractère personnel.

218. Cet objectif si fortement exprimé de confiance est atteint grâce à une multiplication de facteurs plus ou moins influents favorisant l'image attachée à un produit, à un service ou à une technologie. L'un des facteurs déterminants sera la connaissance que la personne acquiert du fonctionnement, de la protection et des utilisations attachées à l'usage d'un produit, d'un service ou d'une technologie. Le lien être confiance et transparence ainsi établi, il n'est dès lors plus surprenant de constater que la confiance par la transparence irrigue de plus en plus les instruments juridiques :

> « Qu'il s'agisse de la vie politique, de la vie de l'entreprise, de la qualité des produits que nous consommons ou encore de la qualité de notre environnement, la société attend de ceux qui exercent une responsabilité dans ces domaines que toute l'information lui soit donnée, de la manière la plus fidèle, en toute transparence »[466]

219. L'énumération d'un certain nombre d'informations à fournir quant au traitement de données à caractère personnel par le responsable de traitement vise alors en premier lieu à pérenniser le lien de confiance entre la personne concernée et le responsable de traitement. Elle s'inscrit dans un mouvement plus général visant à instaurer plus de confiance dans les relations entre les personnes physiques, les entreprises publiques et privées et les autorités publiques. En effet, comme l'indique le Groupe de travail « Article 29 » dans ses lignes directrices sur la transparence :

> « La transparence est une caractéristique bien ancrée dans le droit de l'Union européenne. Son objectif premier est de susciter la confiance dans les processus applicables aux citoyens en leur permettant de comprendre et, au besoin, de contester lesdits processus »[467].

220. Ce constat est partagé par la Commission européenne puisque la confiance dans le numérique doit s'accompagner d'une clarification des règles en matière de transparence[468] et d'une politique favorisant les outils et moyens permettant à la personne de gérer ses consentements et de profiter d'un « suivi et [d'] une transparence accrus de leurs données à caractère personnel »[469].

221. La notion de confiance a d'ailleurs été mise en exergue par les autorités de contrôle au moment de la mise en œuvre d'outils informatisés dans le cadre de la réaction à la pandémie de

---

[466] GAURIGAN Jean-Louis, « La transparence pour susciter la confiance », *JA*, 2019, n°60
[467] Groupe de travail « Article 29 », WP260 rev.01, *op. cit.*, p. 4.
[468] Commission européenne, COM (2020) 67 final, *op. cit*.
[469] Commission européenne, COM (2020) 66 final, *op. cit.*, p. 12.

COVID-19. Dans ce cadre, la confiance en la protection des données à caractère personnel lors du déploiement de tels outils est, selon l'EDPB, essentielle pour créer « les conditions d'acceptabilité sociale » à l'égard de ces outils et ainsi garantir leur efficacité[470]. Lors de son avis sur le projet d'application mobile « StopCovid », la CNIL a rejoint la position de l'EDPB en liant le caractère volontaire de l'utilisation de l'application et la transparence à la confiance et à la favorisation de l'adoption de l'application par la population[471]. Cette vision a également été partagée par le Conseil national du numérique, qui place d'ailleurs la transparence dans un système plus global englobant aussi bien l'information des citoyens que la gouvernance des outils numériques :

> « Le Conseil rappelle qu'une relation de confiance robuste constitue la première des conditions à l'implication des citoyennes et des citoyens. Cette relation doit se fonder sur une transparence totale et des moyens de contrôle et de suivi indépendants »[472].

222. La transparence comme vectrice de confiance est aussi vérifiée au niveau économique : selon une théorie développée par Roger C. Mayer, James H. Davis et David Schoorman, le premier facteur de confiance est la dotation de capacité permettant à une personne d'avoir une influence, capacité qui s'acquière en particulier avec une information adéquate et fiable[473]. De la théorie de l'*homo oeconomicus*, soit l'agent économique rationnel « présumé capable de faire des choix optimaux en s'appuyant sur un calcul approprié »[474] à la théorie de la rationalité limitée voire minimale[475], l'agent économique est au cœur des théories économiques depuis le XVIIIe siècle[476]. Appliquée au marché numérique, l'information permet d'évaluer *a priori* les attributs ayant un impact sur la protection des données à caractère personnel. En marketing, la classification dite « *Search – Experience – Credence* » ou « SEC » définit trois types d'attributs. Premièrement, les *search attributes* sont les attributs pouvant être évalués à l'avance, comme l'apparence d'un produit[477]. Deuxièmement, les *experience attributes* sont les attributs ne pouvant être évalués qu'après l'achat ou l'utilisation, comme la lecture d'un article[478]. Enfin,

---

[470] EDPB, *Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19*, adoptées le 21 avril 2020, p. 4 (disponible sur https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_fr.pdf (consulté en janvier 2021).
[471] CNIL, Délibération n°2020-046 du 24 avril 2020, *op. cit.*
[472] Conseil national du numérique, « StopCovid », *op. cit.*, p. 4.
[473] JEACLE Ingrid, CARTER Chris, « In TripAdvisor we trust: Rankings, calculative regimes and abstract systems », *Accounting, Organizations and Society*, Volume 36, Issues 4-5, mai-juin 2011, pp. 293-309.
[474] LAGUEUX Maurice, « L'agent économique : rationalité maximale ou minimale », *Cahiers d'économie politique,* 2005/2, n°49, p. 143.
[475] *Ibidem.*
[476]DIATKINE Daniel, STEINER Philippe, « Introduction », », *Cahiers d'économie politique,* 2005/2, n°49, p. 7.
[477] MCDONALD Aleecia, FAITH CRANOR Lorrie, *op. cit.*, p. 5.
[478] *Ibidem*.

les *credence attributes* ne peuvent être déterminés même après leur usage, comme les effets nutritionnels[479]. Les informations délivrées par le responsable de traitement à la personne concernée permettent de convertir les *credence attributes* du choix proposé en *search attributes* : la personne concernée va en effet pouvoir évaluer, avant d'effectuer son choix, les impacts de ce dernier sur la protection de ses données à caractère personnel[480].

223. Néanmoins, afin d'effectuer ce calcul, la personne concernée en tant qu'individu ayant des droits fondamentaux et consommateur, va devoir avoir accès à un certain nombre d'informations dont la délivrance sera assurée législativement. La personne concernée est ainsi placée dans une relation de confiance avec le responsable de traitement et est capable d'effectuer des choix économiques informés. Le marché numérique présente cependant une particularité : la donnée à caractère personnel relève à la fois du marchand et du droit humain. La double nature de la donnée à caractère personnel sur le marché imprègne la transparence dont le rôle sera également double : permettre le bon fonctionnement du marché et protéger la personne concernée.

§2 – Le rôle protecteur des conditions matérielles

224. Le respect de l'obligation d'information et plus particulièrement la question du « défaut d'information » a de plus en plus été protégé par le législateur et par la jurisprudence afin de protéger son bénéficiaire. La protection des données à caractère personnel n'échappe pas à cette logique, et le RGPD ainsi que son interprétation lie l'exhaustivité des informations délivrées à la personne concernée à différents principes de protection garantis par le texte. Dès sa naissance, la protection des données à caractère personnel a envisagé l'information comme un moyen de protection de la personne concernée. Durant les débats parlementaires aboutissant à l'adoption de la loi informatique et libertés en 1978, M. Alain Peyrefitte, alors Garde des Sceaux, affirmait :

> « Vis-à-vis de la presse, la première défense du citoyen est le droit de réponse. Vis-à-vis de l'informatique, ce sera un droit de regard. Il s'agit toujours, face à de nouvelles puissances, d'aménager un nouvel équilibre »[481].

[479] *Ibidem.*
[480] *Ibidem.*
[481] PEYREFITTE Alain, Garde des Sceaux, JORF 5 octobre 1977 (séance du 4 octobre 1977), p. 5789, disponible sur http://archives.assemblee-nationale.fr/5/cri/1977-1978-ordinaire1/002.pdf (consulté en janvier 2021).

225. La question de la transparence a alors évolué au fil des textes de protection des données à caractère personnel[482], jusqu'à être consacrée comme principe et droit au sein du RGPD. En effet, lors de l'étude d'impact de la proposition de règlement de la Commission européenne, cette dernière a expressément lié l'objectif de transparence à la protection des droits fondamentaux de la personne :

> « Lack of transparency of data processing, lack of credible enforcement and the absence of effective remedies and sanctions for violations of the principles contribute to creating a climate in which the individuals do not rely on exercising their fundamental freedoms and economic rights fully, even when some concerns regarding data collection and surveillance may be exaggerated over the reality »[483].

226. Sur le plan de la protection juridique des données à caractère personnel, la transparence se rattache en premier lieu au principe de loyauté des traitements de données à caractère personnel[484]. Énoncé dans la Charte des droits fondamentaux de l'Union européenne[485], le principe de loyauté est quasiment systématiquement rattaché au principe de transparence au sein du RGPD[486]. Le principe de transparence est aussi intrinsèquement lié au consentement éclairé puisque, comme l'a rappelé le Groupe de travail « Article 29 », « la transparence, lorsqu'elle est respectée par les responsables du traitement, permet aux personnes concernées […] d'exercer un contrôle sur leurs données à caractère personnel, par exemple en donnant ou en retirant leur consentement éclairé »[487]. Logiquement, en permettant à la personne concernée d'avoir accès à l'ensemble des informations sur le traitement de ses données à caractère personnel, le principe de transparence octroie à la personne concernée la capacité de donner son consentement éclairé.

---

482 Au sein de la directive 95/46/CE, la seule mention explicite à la transparence au sein de la directive consistait à encourager les autorités à « contribuer à la transparence du traitement de données effectué dans l'État membre dont elles relèvent »[482], mais aucune mention de l'obligation de transparence n'est présente au sein des principes relatifs au traitement de données à caractère personnel. V. Directive 95/46/CE, 24 octobre 1995, considérant 63.

483 Commission européenne, *Impact Assessment*, SEC(2012) 72 final, *op. cit.* p. 30.

484 Groupe de travail « Article 29 », WP260 rev.01, *op. cit.*, pp. 4-5.

485 Charte des droits fondamentaux de l'Union européenne, Article 8 (2).

486 RGPD, 27 avril 2016, considérant 39, considérant 60, Article 5 (1) (a), Article 40 (2) (a). Le considérant 45 et l'article 6 (3) mentionnent la loyauté du traitement sans mentionner le principe de transparence, même si, implicitement, les « mesures visant à garantir un traitement licite et loyal » sont énumérées comme mention obligatoire dans la loi pour que celle-ci soit suffisamment transparente. L'article 6 (2) est le seul à mentionner le principe de loyauté indépendamment du principe de transparence.

487 Groupe de travail « Article 29 », WP260 rev.01, *op. cit.*, p. 5. Un avis similaire est donné dans Groupe de travail « Article 29 », WP 259 rev. 01, *op. cit.*, p. 14.

227. De plus, le principe de transparence contribue à visibiliser des traitements dont la personne concernée pourrait ne pas avoir conscience. Déjà en 1999, le Groupe de travail « Article 29 » avait exprimé ses craintes sur les « risques inhérents aux traitements de données à caractère personnel de personnes concernées qui ne seraient pas au courant de tels traitements »[488] : la recommandation du G29 avait été d'ailleurs d'inviter les responsables de traitement à informer les personnes concernées des données à caractère personnel qu'ils avaient l'intention de collecter, stocker et transférer ainsi que les buts pour lesquels un tel traitement était nécessaire[489]. Le même raisonnement avait été retenu par la directive 2002/58/CE à propos de l'information stockée sur l'équipement terminal de l'utilisateur d'un réseau de communications électroniques :

> « Or, les logiciels espions, les pixels invisibles (web bugs), les identificateurs cachés et les autres dispositifs analogues peuvent pénétrer dans le terminal de l'utilisateur à son insu afin de pouvoir accéder à des informations, stocker des informations cachées ou suivre les activités de l'utilisateur, et peuvent porter gravement atteinte à la vie privée de ce dernier. L'utilisation de tels dispositifs ne devrait être autorisée [qu'en] étant portée à la connaissance de l'utilisateur concerné »[490].

228. Par exemple, en 2020, la CNIL a détecté un manquement à l'obligation d'information de l'application StopCovid en raison de l'utilisation, sans information de la personne concernée, d'un traitement de données à caractère personnel, en l'espèce la « technologie reCaptcha, dans sa version invisible, développée par la société Google »[491]. Dans ce cadre, il s'agit d'une technologie visant à sécuriser une application, mais dont l'utilisation implique un traitement de données à caractère personnel invisible. Cette technologie collecte ainsi des données sur les appareils et applications des personnes concernées en vue de les transmettre à la société Google pour analyse : dès lors, les personnes concernées n'étaient à aucun moment informées ni en capacité de donner ou refuser de donner leur consentement lors de l'activation de l'application[492]. Attacher des conditions matérielles au principe de transparence paraît dans ce cadre indispensable pour que la personne concernée ait suffisamment d'informations pour comprendre le traitement sans le voir.

---

[488] Groupe de travail « Article 29 », *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware*, adoptée le 23 février 1999, p. 5.
[489] *Idem*, p. 2.
[490] Directive 2002/58/CE, 12 juillet 2002, considérant 24.
[491] CNIL, Décision MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des Solidarités et de la Santé.
[492] *Ibidem.*

229. Une information suffisamment complète délivrée à la personne concernée lui permet donc de consentir en toute connaissance de cause à l'ensemble des traitements de leurs données à caractère personnel, qu'ils soient à première vue visibles ou invisibles. Une telle information aura enfin également comme conséquence de permettre à la personne concernée d'exercer les différents droits attachés à ses données à caractère personnel (droit d'accès, de rectification, d'effacement, etc.). Dès lors, le prisme choisi par les institutions européennes de la confiance de la personne concernée accordée aux acteurs du marché numérique s'inscrit sans surprise dans un mouvement de transparence des relations économiques entre le consommateur et le professionnel. Les dispositions relatives à la transparence seront parfois tellement similaires entre droit de la consommation et protection des données à caractère personnel que le juge national envisagera parfois la protection des données à caractère personnel sous l'angle du droit de la consommation : l'information de la personne concernée à propos de ses données à caractère personnel aura d'ailleurs été analysée sous l'angle l'article L. 211-1 du code de la consommation créant une obligation à la charge du professionnel de délivrer une information claire et compréhensible au consommateur[493].

230. Cependant, si le principe de transparence n'est pas explicitement cité, le considérant 38 inclut l'obligation de transparence du traitement au sein du principe de loyauté du traitement, en affirmant que « le traitement loyal des données suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de la collecte ». De plus, les articles 10 et 11 de la directive énumèrent les informations que le responsable de traitement doit fournir à la personne concernée, qu'il collecte ces données auprès de la personne concernée (article 10) ou non (article 11). Toutefois, cette obligation est bien plus légère que celle du Règlement puisque la directive se contente d'exiger du responsable de traitement de fournir à la personne concernée des informations sur son identité (ou l'identité de son représentant), les finalités du traitement et toute information complémentaire telle que les destinataires ou catégories de destinataires des données, le fait de savoir si la question est obligatoire ou facultative et l'existence d'un droit d'accès et de rectification de ses données[494]. Le lien avec le principe de loyauté du traitement est d'ailleurs une nouvelle fois présent au sein de la directive puisque l'obligation de délivrance de ces informations supplémentaires est

[493] TGI Paris, 17 septembre 2019, n°16/01008.
[494] Directive 95/46/CE, 24 octobre 1995, articles 10 et 11.

conditionnée au fait que « ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal de ces données »[495].

231. En 2009, le Groupe de travail « Article 29 » protection des données et le Groupe de travail « Police et justice » préconisaient à la Commission européenne de « préciser les modalités d'application de certaines règles et principes clés en matière de protection des données (tels que le consentement et la transparence) »[496]. Ces préconisations ont été entendues puisque le RGPD comporte désormais une obligation de transparence bien plus détaillée que celle de la directive. Ainsi, l'étoffement des conditions matérielles attachées à l'obligation d'information relève d'une volonté du législateur européen de protéger la personne concernée, qui se situe dans une position d'asymétrie d'information vis-à-vis du responsable de traitement.

232. Conclusion de Section. – Les conditions matérielles attachées à l'obligation d'information poursuivent un double objectif qui se confond avec le double objectif poursuivi par le RGPD : assurer le bon fonctionnement du marché et protéger la personne concernée à travers le droit à la protection des données à caractère personnel. Concrètement, les conditions matérielles permettent à la personne concernée de prendre une décision informée qui d'une part, introduit un élément de raisonnabilité sur le marché de son comportement en tant qu'agent économique et d'autre part, lui octroie les capacités de contrôler le traitement de ses données à caractère personnel. Ainsi, conduit par ce double objectif, le législateur a souhaité garantir l'exhaustivité des informations nécessaires à la prise de décision de la personne concernée.

Section 2 – La recherche de l'exhaustivité de l'information

233. Le RGPD a considérablement étoffé les informations matérielles à fournir à la personne concernée par rapport à la directive 95/46. Les informations nouvellement obligatoires se rapportent à l'ensemble des éléments entourant le traitement de données à caractère personnel : le responsable de traitement, les modalités du traitement, les destinataires de données, le couplage éventuel des données avec d'autres obligations, et les droits des personnes concernées. Le tableau suivant permet de comparer l'évolution de l'obligation d'information entre la directive 95/46/CE et le RGPD :

Tableau comparatif de l'article 10 de la directive 95/46/CE et du Règlement (UE) 2016/679

---

[495] *Ibidem.*
[496] Groupe de travail « Article 29 », WP 168., *op. cit.* p. 2 et p. 8.

Informations	Directive 95/46/CE	Règlement (UE) 2016/679
Responsable du traitement	Identité du responsable du traitement et, le cas échéant, de son représentant	Identité et coordonnées du responsable du traitement et, le cas échéant, de son représentant
		Le cas échéant, les coordonnées du délégué à la protection des données
Informations sur le traitement	Les finalités du traitement auquel les données sont destinées	Les finalités du traitement auquel les données sont destinées
		La base juridique du traitement
		Les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers
		La durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer leur durée
		L'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.
Destinataires des données	Les destinataires ou les catégories de destinataires de données*	Les destinataires ou les catégories de destinataires de données
		L'existence d'un transfert (ou projet de transfert) ainsi que la base juridique sur laquelle s'effectue le transfert (décision d'adéquation ou autre)
Couplage ou non des données	Le caractère obligatoire ou facultatif des réponses aux questions posées par le responsable de traitement et les conséquences éventuelles d'un défaut de réponse*	Le caractère réglementaire ou contractuel de l'exigence de fourniture de données à caractère personnel, le fait que cette fourniture de données conditionne la conclusion d'un contrat ou son caractère obligatoire, ainsi que les conséquences éventuelles de la non-fourniture de ces données
Droit des personnes concernées	L'existence d'un droit d'accès aux données la concernant et de rectification de ces données*	L'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données
		L'existence du droit de retirer son consentement à tout moment sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci
		Le droit d'introduire une réclamation auprès d'une autorité de contrôle

* Dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal de ses données.

234. La délivrance d'informations a pour vocation de permettre à la personne concernée de connaître les contours du traitement de données à caractère personnel. Informée des risques et modalités du traitement, la personne concernée pourra vérifier l'adéquation du traitement avec son référentiel de consentement et contrôler, à travers l'exercice de ses droits, l'adéquation du traitement avec les informations délivrées par le responsable de traitement (§1).

235. Comme il l'a déjà été mentionné, la nature de l'information est double : elle est à la fois un droit pour la personne concernée et une obligation à la charge du responsable de traitement. Dans sa deuxième acception, fournir une information est une fin et non un moyen. Ainsi, il

semble que certaines informations soient principalement utiles aux personnes déjà sensibilisées à la protection des données à caractère personnel. En effet, la base juridique du traitement ou encore la base juridique sur laquelle est fondé le transfert sont des exemples d'information dont la compréhension nécessite des connaissances juridiques en matière de protection des données à caractère personnel. L'information-obligation se voit donc dotée d'une autre vocation : le contrôle des traitements de données à caractère personnel par l'expert (§2).

§1 – L'exhaustivité de l'information à des fins de vérification par la personne concernée

236. Le consentement éclairé est directement lié à l'exigence de transparence[497]. Dans le cadre d'une demande de consentement, le rôle primaire de l'information sera de permettre à la personne concernée d'exercer un consentement éclairé (A). Le principe de transparence permettra également de renforcer le contrôle de la personne concernée sur le traitement au-delà du simple consentement éclairé (B).

A. L'information aux fins de consentement éclairé

237. L'information aux fins de consentement éclairé présente la particularité d'examiner l'information du point de vue de l'autonomie de choix de la personne concernée et non du point de vue de la responsabilité des responsables de traitement en tant que responsables de la divulgation de l'information[498]. Dans ce cadre, le contrôle de la personne concernée sur ses données à caractère personnel dépend de sa capacité à évaluer la situation afin de prendre une décision sur le traitement de ses données à caractère personnel[499]. Le lien entre l'information et la capacité pour la personne de consentir pose la question de la spécialité de l'information aux fins de consentement : le juriste doit-il examiner de la même manière l'information aux fins de consentir et l'information aux fins de respect du principe de transparence des traitements ? Au premier abord, l'information aux fins de consentement appelle à un seuil d'informations jugées nécessaires à l'exercice de l'autonomie de choix de la personne concernée, alors que l'information destinée au respect du principe de transparence présente un aspect plus déclaratif. Dans cette acception, l'information aux fins de consentement serait interprétée de manière subjective, de manière à évaluer, de manière casuistique ou à travers le recours à la figure de la

---

497 Groupe de travail « Article 29 », WP 259 rev. 01, *op. cit.*, p. 17.

498 FADEN Ruth R., BEAUCHAMP Tom L., *A History and Theory of Informed Consent*, Oxford University Press, 1986, p. 3.

499 GIANNOPOULOU Alexandra, « Algorithmic systems: the consent is in the detail? », *Internet Policy Review*, mars 2020, Volume 9, Issue 1.

personne raisonnable, si l'information fournie permet effectivement à la personne concernée d'exercer son consentement de manière éclairée. L'information aux fins de respect du principe de transparence serait quant à elle évaluée de manière objective, la simple mention de l'information entraînant la conformité au principe de transparence et la simple absence entraînant son non-respect.

238. Les lignes directrices du G29 sur le consentement, adoptées en 2017, semblent s'inscrire dans la lignée d'une spécificité de l'information conditionnant la validité du consentement. Le G29 y affirme en effet que « pour que le consentement soit éclairé, il est nécessaire d'informer la personne concernée de certains éléments cruciaux pour faire un choix »[500]. La notion d'éléments cruciaux sous-entend dès lors l'existence d'un seuil d'informations à atteindre afin de pouvoir considérer qu'un consentement est exercé de manière éclairée. Dans cette situation, le consentement éclairé ne se confond pas avec le principe de transparence. Par conséquent, la simple absence d'information sur un élément requis par l'article 13 ou 14 du RGPD n'entraîne pas *a priori* l'absence de validité du consentement : seule la dissimulation d'informations pouvant amener la personne concernée à refuser le traitement entraînerait l'invalidité du consentement. Au niveau de la responsabilité du responsable de traitement, le prisme est également différent. Dans le cadre de la validité du consentement au regard des exigences de consentement éclairé, il n'est plus reproché au responsable de traitement de ne pas divulguer des informations utiles à la transparence de ses traitements. En effet, un élément d'intention s'ajoute au simple respect du principe de transparence. Il sera alors reproché au responsable de traitement de ne pas avoir divulgué des informations utiles à l'exercice du consentement et donc d'avoir manipulé la personne concernée en ne lui donnant accès qu'à une quantité minimale d'information concernant les éléments pertinents à l'exercice de son choix. Interroger la distinction entre la validité du consentement éclairé et le respect du principe de transparence n'est donc pas dénué d'intérêt pratique puisqu'il module la sanction d'une lacune d'information délivrée à la personne concernée. Si l'information est nécessaire à l'exercice du consentement éclairé, la sanction consistera en une invalidation du fondement de licéité du traitement ; si l'information n'est pas nécessaire à l'exercice du consentement, le responsable de traitement sera sanctionné sur le fondement de la violation d'un principe de base du traitement[501].

---

[500] Groupe de travail « Article 29 », WP 259 rev. 01, *op. cit.*, p. 15.

[501] Il pourra être remarqué que la licéité et la transparence sont inscrites au sein du même principe relatif au traitement des données à caractère personnel (article 5 (1)(a)). Nous sommes cependant d'avis que les conséquences de l'illicéité du traitement sont plus importantes que les conséquences de la violation du principe de transparence

239. Il semble ainsi nécessaire de distinguer les informations nécessaires à l'exercice d'un consentement éclairé des informations délivrées au titre du principe de transparence. Un premier élément de réponse est délivré par les lignes directrices du G29 relatives au consentement, qui s'efforce d'identifier les informations minimales nécessaires pour obtenir un consentement éclairé, et donc valable : l'identité du responsable de traitement, la finalité de chaque traitement pour lequel le consentement est sollicité, les types de données ou les données collectées et utilisées, l'existence du droit de retirer son consentement, et, le cas échéant, les informations concernant l'existence d'une prise de décision automatisée ou encore les informations relatives aux risques de transferts de données en dehors des cas de décision d'adéquation de la Commission européenne[502]. L'absence de consentement éclairé relèverait donc de l'absence des mentions d'information déjà obligatoires sous le régime de la directive, des mentions d'information relatives aux risques particuliers (prise de décision automatisée et transferts de données sans décision d'adéquation de la Commission) ainsi que la mention du droit de retirer son consentement. Dans ce contexte, la simple absence d'information ou la présence d'information incomplète permet de conclure automatiquement à l'absence de consentement éclairé[503]. Cette liste d'informations essentielles au recueil du consentement éclairé a notamment été reprise par les autorités de contrôle française[504], belge[505] et britannique[506]. Par exemple, cette liste d'informations est reprise au sein de la décision de la CNIL relative au recueil du consentement par Google : la CNIL conclut à l'absence de consentement éclairé dans la mesure où l'ensemble de ces informations n'était pas délivré de manière suffisamment accessible, claire et compréhensible[507].

240. Néanmoins, il semble que la distinction entre l'information aux fins de transparence et l'information aux fins de consentement ne relève pas exclusivement d'une liste d'informations jugées essentielles à l'exercice du consentement éclairé. Les lignes directrices du G29

---

dans la mesure où la licéité du traitement est l'élément de transformation de l'illicite en licite. La sanction de la violation du principe de transparence n'invalidera pas automatiquement la licéité du traitement, et sera réparable sans qu'il soit nécessaire de mettre en place un nouveau traitement de données à caractère personnel.

[502] Groupe de travail « Article 29 », WP 259 rev. 01, *op. cit.*, p. 15.

[503] V. par exemple CNIL, Délibération n° MED-2020-015 du 15 juillet 2020, *op. cit.*

[504] CNIL, Délibération de la formation restreinte SAN-2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société Google LLC.

[505] APD, Décision quant au fond 04/2021 du 20 janvier 2021, §140.

[506] ICO, 10 mai 2021, *ICO Monetary Penalty on Tested.me Ltd.*

[507] CNIL, Délibération n° SAN-2019-001 du 21 janvier 2019, *op. cit.*

proposent en effet une seconde piste qui semble être privilégiée par les autorités de contrôle dans leur évaluation de la validité du consentement. En effet, à la suite de la liste d'informations nécessaires à l'obtention d'un consentement éclairé, le G29 précise « qu'en fonction des circonstances et du contexte de chaque cas, plus d'informations peuvent être nécessaires afin que la personne concernée puisse réellement comprendre les opérations de traitement envisagées ». Le G29 propose ainsi une analyse casuistique du consentement éclairé, qui s'évaluerait en fonction de l'objectif poursuivi par le règlement, soit mettre la personne concernée en position de comprendre le traitement de ses données à caractère personnel. Il semble que les autorités de contrôle privilégient l'interprétation téléologique du consentement éclairé puisqu'une telle interprétation se retrouve soit en complément d'interprétation de la liste proposée par le G29[508], soit analysé de manière autonome dans les décisions des autorités de contrôle[509] et les autorités judiciaires[510]. Cette position est également suivie par la CJUE qui évalue le caractère éclairé du consentement en fonction de la capacité accordée à la personne concernée « de déterminer facilement les conséquences du consentement qu'elle pourrait donner et garantir que ce consentement soit donné en pleine connaissance de cause »[511]. L'évaluation casuistique du caractère éclairé du consentement présente l'intérêt de prendre en compte des informations supplémentaires à la liste initialement dressée par les lignes directrices du G29. Un exemple significatif est la question de la durée de conservation des données à caractère personnel[512] qui peut, malgré la possibilité de retirer son consentement à tout moment, influencer le consentement de la personne concernée au traitement de ses données à caractère personnel.

241. La démarche du législateur européen et son interprétation par le G29 ne sont pas sans rappeler la logique contractuelle des éléments essentiels du contrat. L'article 1114 du Code civil crée en effet une obligation d'information à la charge de l'offrant puisque c'est l'information sur les éléments du contrat envisagé qui transforme la proposition en offre. Ces éléments essentiels du contrat sont soit communs à la nature du contrat – par exemple, ne sera pas considérée comme une offre de contrat de travail une proposition ne précisant ni la

[508] APD, 20 janvier 2021, *op. cit.* §140.
[509] AEPD, PS-00070-2019, publiée le 11 décembre 2020 ; Datatilsynet, 18 juin 2020, 2020-431-0085 ; Datatilsynet, 1e mars 2021, 2019-431-0052 ; Datatilsynet, 11 décembre 2020, 2020-31-3354.
[510] Cass. Civ. (Italie), 25 mai 2021, 14381/2021 ; CJUE, 11 novembre 2020, *Orange Romãnia SA c. Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP),* C-61/19 ; LG Rostock, 15 septembre 2020, 3 O 762/19 ; OGH (Cour suprême autrichienne), 15 novembre 2018, 9 Ob 38/19 g.
[511] CJUE, C-61/19, *op. cit.*.
[512] Datatilsynet, 18 juin 2020, *op. cit.* ; CJUE, C-61/19, *op. cit.*.

rémunération ni la date d'embauche du candidat[513] –, soit particuliers à une situation donnée – par exemple, la durée de travail n'est normalement pas un élément essentiel du contrat dans le cadre d'un contrat de travail à temps complet, mais le devient lorsqu'il conditionne un élément sur lequel porte le consentement (par exemple, la rémunération)[514].

242. L'interprétation téléologique de l'obligation d'obtenir un consentement éclairé s'inscrit dans la volonté de concilier la protection (de l'individu, de ses données à caractère personnel) et la liberté (de l'individu, du responsable de traitement). Les deux notions paraissent en première lecture associées dans les expressions « protection de la liberté » ou « protection des droits et libertés fondamentales ». Cependant, la granularité de la protection étatique et son entrée dans des aspects de vie quotidienne considérés comme relevant de l'intime ont, depuis de nombreuses années, montré que les notions de protection et de liberté pouvaient également être analysées comme des notions antagonistes que le juriste devait s'efforcer de concilier. L'essai *De la liberté* de John Stuart Mill s'efforce de décrire la raison pour laquelle protection et liberté s'opposent, peu importe le système politique dans lequel ces notions sont analysées[515]. Le philosophe anglais démontre que le passage entre la lutte entre l'autorité et la liberté (opposant le souverain et ses sujets) à l'avènement de régimes démocratiques n'a pas effacé le besoin de protéger la liberté, puisque le pouvoir du peuple sur lui-même ne pouvait être illimité en raison du risque de tyrannie de la majorité qui s'inscrit « au nombre des maux contre lesquels la société doit se protéger »[516]. John Stuart Mill considère que l'individu ne doit être responsable que ses actions portant préjudice à autrui : « partout où il y a un dommage défini, ou un risque défini de dommage, soit pour un individu, soit pour la société, le cas sort du domaine de la liberté pour tomber sous le coup de la morale ou de la loi »[517]. Dans le cas d'une action ne concernant que l'individu, celui-ci est souverain[518]. L'essai de John Stuart Mill rejoint donc la définition de la liberté proposée par la Déclaration des droits de l'homme et du citoyen :

> « La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de tout homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits ».

---

513 V. par ex Cass, Soc., 28 novembre 2018, n°1704.

514 V. par ex Cass, Soc., 22 février 2000, n°97-44.339 ; ROSE Hubert, « Durée du travail : fixation et aménagement du temps de travail », *Répertoire du droit du travail*, Dalloz, §15.

515 MILL John Stuart, *De la liberté*, Paris, Gallimard, 1990, traduit de l'anglais par Laurence Lenglet, 242 p.

516 *Idem,* pp. 6-7.

517 *Idem,* p. 64.

518 Déclaration des droits de l'homme et du citoyen, 1789, article 4.

243. Aujourd'hui, l'enjeu de la réconciliation entre protection et liberté s'inscrit dans la gestion du risque. Le droit moderne est en effet si centré sur le risque qu'il « paraît aujourd'hui banal d'énoncer que le triptyque « Droit, Risques et Responsabilité » innerve l'ensemble des activités des sociétés modernes »[519]. La notion de risque est en effet omniprésente dans la société, sémantique récurrente depuis quatre siècles dans les sociétés européennes[520], sujet privilégié des sociologues[521] depuis quelques décennies. Initialement omniprésent dans le domaine économique, le risque est devenu un outil de contrôle et de prévoyance, traduisant historiquement le passage de l'explication divine et métaphysique des événements à la raison scientifique par le jeu des circonstances[522]. Le discours autour du risque a désormais envahi « le champ de la médecine, de la politique, du droit, de l'économie, de la recherche scientifique, des sciences sociales, de l'écologie, de la climatologie, de la philosophie, etc., sans épargner le domaine de la vie quotidienne »[523]. Ainsi, le droit, et particulièrement la protection des droits fondamentaux, n'échappe pas au phénomène. Frédéric Bouhon identifie l'origine du risque dans le champ du droit comme la conséquence de sa nature : « de manière fondamentale, si l'on accepte de considérer que la norme de droit est essentiellement un acte qui vise à influencer le comportement des individus, on comprend que la norme encadre la manière dont ces derniers prennent des décisions, d'agir ou de ne pas agir, notamment face à des risques »[524]. En matière de droits fondamentaux, le risque ne va pas être considéré comme évitable, mais comme suffisamment maîtrisé pour ne pas menacer la jouissance des droits fondamentaux de l'individu[525].

244. À travers cette notion de risque, de plus en plus de comportements de l'individu considérés comme dangereux ou potentiellement dangereux pour lui-même vont être encadrés par le droit. Par exemple, le port de la ceinture de sécurité est obligatoire alors même que

---

[519] LIENHARD Claude, « Le droit du risque », *in* AGUILA Yann (dir.), *Quelles perspectives pour la recherche juridique ?*, Paris, Presses Universitaires de France, Droit et Justice, 2007, p. 263.
[520] MYTHEN Gabe, « Sociology and the Art of Risk », *Sociology Compass*, 2008, p. 299.
[521] V. par exemple BECK Ulrich, *La société du risque. Sur la voie d'une autre modernité,* Paris, Aubier, 2001, 528 pages ; LUHMANN Niklas, *Risk. A Sociological Theory*, New York, Routledge, 2002, 270 pages.
[522] LE BRETON David, *Sociologie du risque*, Presses Universitaires de France, Que sais-je ?, 2017, p. 35.
[523] *Idem*, p. 38.
[524] BOUHON Frédéric, « Le risque et la Cour européenne des droits de l'homme – Premières esquisses d'une réflexion sur le risque à l'aune des droits fondamentaux », *RDLF*, chronique n°46, disponible sur http://www.revuedlf.com/droit-fondamentaux/le-risque-et-la-cour-europeenne-des-droits-de-lhomme-premieres-esquisses-dune-reflexion-sur-le-risque-a-laune-des-droits-fondamentaux/
[525] SEMINARA Letizia, « Risk Regulation and the European Convention on Human Rights », *European Journal of Risk Regulation*, 2016, n°4, p. 733.

l'individu « supporte seul le risque », au nom du coût social de l'accident[526]. Cependant, si le droit s'est aventuré à légiférer sur des comportements relevant du « rapport de soi à soi »[527], cette extension du domaine d'application du droit ne constitue pas la règle. L'autonomie individuelle est d'ailleurs proclamée par la Cour européenne des droits de l'homme comme un principe important du droit à l'autodétermination, lui-même inclus au sein du droit à la protection de la vie privée et familiale, du domicile et de la correspondance[528]. La Cour a notamment affirmé dans l'arrêt *Pretty c. Royaume-Uni :*

> « la faculté pour chacun de mener sa vie comme il l'entend peut également inclure la possibilité de s'adonner à des activités perçues comme étant d'une nature physiquement ou moralement dommageable ou dangereuse pour sa personne »[529].

245. Ainsi, il n'est pas question d'empêcher l'individu de prendre les risques qu'il a décidé de prendre, mais d'assister l'individu dans la gestion de ces risques. La nécessité d'assister l'individu se justifie aisément par la double complexité des enjeux liés aux traitements de données à caractère personnel : la complexité est à la fois économique et technologique. Dès les premiers considérants du RGPD, le législateur identifie un des aspects du manque de confiance des utilisateurs européens envers les acteurs du numérique : « le sentiment, largement répandu dans le public, que des risques importants pour la protection des personnes physiques subsistent, en particulier en ce qui concerne l'environnement en ligne »[530]. Une recherche d'occurrence du terme risque dans le texte du RGPD révèle soixante-dix-huit occurrences, dont sept s'intéressent à la perception ou à la gestion du risque par l'individu[531]. Ainsi, si la gestion du risque relève principalement du rôle du responsable de traitement dans sa mise en œuvre des traitements, la personne concernée reste tout de même un acteur de sa propre gestion des risques à travers le contrôle de ses données à caractère personnel.

246. Le rôle du législateur est dans ce contexte de permettre à l'individu de décider du traitement de ses données à caractère personnel, en toute connaissance des risques attachés à une telle opération. Il s'agit ainsi de créer les conditions favorables à l'autonomie de la personne, afin que « loin de subir les évolutions de son environnement, [elle] dispose des

---

[526] FÉVRIER Jean-Marc, « Vaccination obligatoire, consentement et expérimentation », *AJDA,* n°29, 2021, p. 1677.
[527] FABRE-MAGNAN Muriel, « Le domaine de l'autonomie personnelle. Indisponibilité du corps humain et justice sociale », *D.,* 2008, p. 31.
[528] CEDH, Guide sur l'article 8 de la Convention européenne des droits de l'homme, *op. cit.*
[529] CEDH, 29 avril 2002, *Pretty c. Royaume-Uni,* 2346/02, §62.
[530] RGPD, 27 avril 2016, considérant 9.
[531] RGPD, 27 avril 2016, considérant 9, considérant 38, considérant 39, considérant 65, considérant 122, Article 49 (1) (a), Article 57 (1) (b).

moyens nécessaires pour provoquer l'apparition d'événements favorables ou éviter la survenance d'événements défavorables[532]. Cette démarche rejoint la position de la CJUE en matière de risque et droit de la consommation : puisque le professionnel est le détenteur de la connaissance, la transparence des clauses du contrat n'est satisfaite que si « le professionnel a fourni au consommateur des informations suffisantes et exactes permettant à un consommateur moyen, normalement informé et raisonnablement attentif et avisé » de comprendre et évaluer le risque associé au contrat[533]. Dès lors qu'il y a asymétrie d'information entre les deux parties, il ne peut être reproché à la partie profane ni son manque de compréhension ni l'absence de recherche d'informations complémentaires[534]. L'obligation d'information sur le risque est donc à la charge de la personne informée, qui est le responsable de traitement.

247. Ainsi, l'information aux fins de consentement éclairé vise à placer la personne concernée en position de contrôle du traitement de ses données à caractère personnel, en lui permettant d'avoir accès aux informations essentielles à l'exercice de son consentement, y compris les risques associés au traitement. La volonté de permettre à la personne concernée d'avoir le contrôle de ses données à caractère personnel est renforcée par une obligation d'information aux fins de contrôle du traitement par la personne concernée.

B. L'information aux fins de contrôle par la personne concernée

248. L'information de la personne concernée est prévue par la section 2 du RGPD intitulée « information et accès ». L'obligation de transparence du responsable de traitement constitue un droit à l'information *ex ante* de la personne concernée tandis que le droit d'accès de la personne concernée constitue un droit à l'information *ex post*. Le droit d'accès de la personne concernée à ses données à caractère personnel traitées par le responsable de traitement peut être analysé comme un droit à l'information « personnalisé » à la situation de la personne concernée.

249. La transparence est un des principes clés gouvernant les sociétés démocratiques. L'apparition du principe de transparence est généralement affiliée au mouvement des Lumières

---

[532] DABOSVILLE Benjamin, *op. cit.*, p. 203

[533] CJUE, 10 juin 2021, affaires jointes C776-19 à C-782/19, §78.

[534] Par exemple, en matière de vente immobilière, non seulement, il n'est pas possible de reprocher à des acheteurs profanes l'absence de plus amples investigations sur la zone d'exposition au risque d'inondation, mais il convient également au professionnel (en l'espèce, le notaire), d'attirer l'attention des acquéreurs sur cette difficulté. CA Montpellier, 23 mars 2017, n°14/01306 ; DUPIE Agnès, « Rubrique de jurisprudence Risques naturels et technologies », *Bulletin du droit de l'environnement industrie*, mars 2013.

et à l'avènement du gouvernement représentatif qui lui a succédé[535]. Remède contre l'arbitraire et la corruption, le principe de transparence repose sur l'idée de contrôle, dans la lignée de la devise attribuée à Jeremy Bentham selon laquelle « plus on est surveillé strictement, mieux on se comporte »[536]. La transparence est ainsi regardée comme la volonté des citoyens de participer non seulement à l'élaboration des normes, mais également au contrôle de l'action publique[537]. La transparence est ainsi regardée comme un principe permettant aux citoyens de contrôler que leur volonté, à l'origine du pouvoir dans une société démocratique, est respectée par l'autorité publique.

250. De même, la protection des données à caractère personnel va envisager la transparence comme un outil permettant à la personne concernée de garder le contrôle sur ses données à caractère personnel[538]. La transparence de l'information en faveur de la personne concernée s'inscrit dans la volonté d'assurer « une surveillance cohérente du traitement des données à caractère personnel »[539]. L'obligation d'information peut ainsi être interprétée comme le propose le G29, en fonction du pouvoir de contrôle de l'individu sur le traitement de données à caractère personnel : plus il est difficile pour l'individu de surveiller le traitement auquel il consent, plus il est requis du responsable de traitement un effort pour démontrer que le consentement est obtenu de manière éclairée[540]. Cette volonté est notamment consacrée à travers le droit d'accéder à ses données à caractère personnel afin « d'en vérifier la licéité »[541]. Le Règlement s'inscrit ainsi dans la tendance du principe de transparence, faisant de « toute personne curieuse un enquêteur, ou, au moins, un informé »[542]. Le considérant 11 du RGPD rappelle qu'une protection effective des données à caractère personnel présuppose une capacité de contrôle des règles inhérentes à cette protection. Si les acteurs privilégiés de la surveillance sont les autorités de contrôle et les magistrats, le règlement européen a eu cependant à cœur d'élargir la capacité de contrôle à la personne concernée elle-même : c'est le sens du

---

[535] PUYDEBOIS Grégori, *La transparence de la vie publique en France*, Thèse présentée pour obtenir le grade de docteur en droit sous la direction de MÉLIN-SOUCRAMANIEN Ferdinand, Université de Bordeaux, 2019, pp. 18-19.

[536] ROBERT Cécile, « La transparence comme nouvel horizon des démocraties européennes : Genèses et usages d'une injonction ambivalente », *Politique européenne*, 2018, n°61, p. 16

[537] SAUVÉ Jean-Marc, « Transparence et efficacité de l'action publique », *Intervention lors de l'Assemblée générale de l'administration*, 3 juillet 2017, disponible sur le site du Conseil d'État : https://www.conseil-etat.fr/actualites/discours-et-interventions/transparence-et-efficacite-de-l-action-publique

[538] Groupe de travail « Article 29 », WP 260 rev. 01, *op. cit.*, p. 6.

[539] RGPD, 27 avril 2016, considérant 13.

[540] Groupe de travail « Article 29 », WP 187, p. 23.

[541] RGPD, 27 avril 2016, considérant 63.

[542] LE CANNU Paul, « Le combat du voile et de la transparence », *Bulletin Joly Sociétés*, n°11, p. 609.

considérant 7 qui affirme que « les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant ».

251. Dès lors, le contrôle de la protection des données à caractère personnel recouvre un double rôle. La notion de contrôle se définit de manière usuelle comme une « vérification portant sur des choses en vue d'examiner si elles remplissent les conditions demandées »[543]. Le contrôle se définit donc en fonction d'un référentiel prédéfini. Premièrement, le référentiel légal permet de contrôler la conformité du traitement de données à caractère personnel avec les règles de protection des données à caractère personnel. Deuxièmement, le référentiel personnel de la personne concernée lui permet de contrôler que les traitements de ses données à caractère personnel correspondent bien au traitement de données à caractère personnel auquel elle consent ou va consentir.

252. La légalité du traitement de données à caractère personnel ne sera probablement pas contrôlée de manière principale par la personne concernée. Cependant, certaines informations obligatoirement délivrées au titre de l'article 13 du RGPD lui présenteront des outils lui permettant de vérifier et de contester un traitement de données à caractère personnel qu'elle estimerait illégal : parmi ces outils, la mention obligatoire du droit de demander au responsable de traitement l'accès à ses données à caractère personnel aux fins de contrôle des données collectées par celui-ci, le droit à la limitation des données lui permettant d'exercer un recours contre le responsable de traitement en cas de traitement illicite sans que celui-ci puisse être continué par le responsable de traitement, ou encore le droit d'introduire une réclamation auprès d'une autorité de contrôle. La personne concernée va également avoir accès à une information sur la base légale sur laquelle se fonde le traitement de données à caractère personnel, ce qui facilite le contrôle exercé par la personne concernée.

253. Cependant, la personne concernée va principalement vérifier l'adéquation du traitement de données à caractère personnel avec son propre référentiel de consentement. Ainsi, les mentions obligatoires précitées à titre d'information permettent à la personne d'exercer son choix afin de contrôler que ces données à caractère personnel sont traitées de la manière qu'elle le souhaite. Par exemple, par la mention de l'existence d'une prise de décision automatisée, la personne concernée refusant de faire l'objet d'une telle décision, pourra ne pas accorder son consentement sur ce fondement. Une fois le traitement consenti, la personne concernée va être informée des outils lui permettant de contrôler la conformité du traitement de ses données à

[543] CNRTL, « Contrôle », *Lexicographie*, disponible sur https://www.cnrtl.fr/definition/contr%C3%B4le

caractère personnel avec son consentement : la personne concernée sera informée de son droit d'accès et de limitation de ses données à caractère personnel, mais également à ses droits de rectification et d'effacement des données lui permettant de contrôler la qualité et l'adéquation de ses données à caractère personnel traitées par rapport aux finalités du traitement et aux contours du consentement donné. Aussi, la personne concernée sera informée de son droit de retirer son consentement si elle ne souhaite plus que ses données à caractère personnel soient traitées. Enfin, le responsable de traitement est tenu d'informer la personne concernée de son droit à la portabilité des données, permettant à la personne concernée de comparer les services identiques en matière de protection des données à caractère personnel.

254. Cependant, le juriste aguerri habitué de la permissivité juridique de l'absence de précision des clauses (*legal room*) se méfie de la capacité de contrôle de la personne concernée profane face au responsable de traitement détenteur de l'information. Si la politique de confidentialité se doit d'être précise, il reste cependant des mentions qui peuvent se révéler ambiguës telles que les intérêts légitimes poursuivis par le responsable de traitement, les « catégories » de destinataires de données à caractère personnel (ce qui ne nécessite ainsi pas de révéler leur identité) ou encore les critères utilisés pour déterminer la durée de conservation des données à caractère personnel[544]. Le juriste peut aussi se montrer sceptique quant à la réalité de la politique de protection des données qui, dans le RGPD, revêt un aspect déclaratif qui engage l'*accountability* du responsable de traitement en cas de contrôle. Ainsi, le responsable de traitement est certes dans l'obligation de délivrer des informations sur les traitements de données à caractère personnel, mais reste maître de la délivrance de ces informations. La perplexité du juriste quant à la réalité du principe de transparence n'est d'ailleurs pas propre à la question de la protection des données à caractère personnel, mais semble au contraire s'étendre à l'ensemble des obligations juridiques relatives à la transparence. En matière financière par exemple, où le principe de transparence est central, la doctrine reste perplexe quant au fait que « le client est censé être éclairé sur les intérêts cachés de son interlocuteur »[545].

255. C'est ainsi qu'en matière de protection des données à caractère personnel, le principe de transparence ne se limite pas à la déclaration des modalités de traitement des données à caractère

[544] Il est nécessaire de préciser à cet égard que les autorités de contrôles sont tout de même compétentes pour déterminer le niveau de précision attendu des informations délivrées par le responsable de traitement à la personne concernée. V par ex. AEPD, 13 janvier 2021, PS-00477-2019.

[545] ROUSSILLE Myriam, « Conflits d'intérêts : la transparence sauve-t-elle les apparences ? », *Bulletin Joly Bourse*, 2021, n°4, p. 1.

personnel à travers la politique de confidentialité. La Section 1 dénommée « Transparence et modalités » contient un unique article, l'article 12, qui dispose :

> « Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant »[546].

Ainsi, le principe de transparence se compose de trois composants : la délivrance d'informations à la personne concernée sur le traitement de ses données à caractère personnel (articles 13 et 14 du RGPD), l'exercice des droits de la personne concernée (articles 15 à 22 du RGPD) et enfin, la communication à la personne concernée d'une violation de données à caractère personnel (article 34 du RGPD). Le principe de transparence ne se limite dès lors pas à une passivité de la personne concernée face aux informations délivrées activement par le responsable de traitement (articles 13, 14 et 34), mais contient également toute une panoplie d'outils permettant à la personne concernée d'exercer un contrôle proactif du traitement de ses données à caractère personnel, parmi lesquels le droit d'accès (article 15).

256. Le droit d'accès de la personne concernée constitue sans doute l'outil le plus important à la disposition de la personne concernée : les dispositions relatives au droit d'accès de la personne concernée poursuivent l'objectif de fournir suffisamment d'informations à la personne concernée sur le traitement et l'étendue de ses données à caractère personnel traitées par le responsable de traitement afin qu'elle puisse se rendre compte concrètement des conséquences de la politique de protection des données mise en place par le responsable de traitement, en vérifier la légalité et l'exactitude, mais également permettre à la personne concernée de pouvoir exercer ses autres droits[547]. Sous le régime de la directive 95/46/CE, la CJUE avait déjà eu l'occasion de souligner que le droit d'accès de la personne concernée est nécessaire au contrôle du traitement de ses données à caractère personnel :

> « il y a lieu de rappeler que la protection du droit fondamental au respect de la vie privée implique, notamment, que toute personne physique puisse s'assurer que les données à caractère personnel la concernant sont exactes et qu'elles sont traitées de manière licite. […] C'est afin de

[546] RGPD, 27 avril 2016, Article 12 (1).
[547] EDPB, *Guidelines 01/2022 on data subjects rights – Right of access,* Version 1.0, adoptées le 18 janvier 2022 (ouvertes à consultation publique).

> pouvoir effectuer les vérifications nécessaires que la personne concernée dispose […] d'un droit d'accès aux données la concernant qui font l'objet du traitement »[548].

257. L'importance du droit d'accès de la personne concernée aux données à caractère personnel aux données la concernant est soulignée par son inscription à l'article 8 (2) de la Charte des droits fondamentaux de l'Union européenne. Ainsi, le droit d'accès aux données à caractère personnel le concernant ne constitue pas une modalité du droit à la protection des données définie par un acte de droit dérivé, mais une composante de celui-ci établi par un acte de droit primaire. Le droit d'accès semble d'ailleurs être antérieur à la consécration du droit à la protection des données à caractère personnel comme un droit autonome du droit à la vie privée. En effet, le Parlement européen avait, en 1994, adopté une proposition de constitution pour les communautés européennes contenant d'une part le droit au respect de sa vie privée, et d'autre part, le droit d'accès à l'information rédigé de la façon suivante :

> « Toute personne a le droit d'accéder et le droit de demander des rectifications aux documents administratifs et autres données la concernant »[549].

Dès lors, historiquement, le droit d'accès ne constitue pas une composante ni même une modalité du droit à la protection des données, mais une protection de l'application régulière de la loi (*protection of due process*)[550]. La forte dimension de contrôle et de vérification du droit d'accès, au-delà de l'aspect transparence, est de ce fait héritée de cette dimension historique.

258. Néanmoins, l'approche historique ne saurait à elle seule expliquer les contours actuels du droit d'accès à ses données à caractère personnel. L'arrêt *YS* rendu par la CJUE le 17 juillet 2014 est significatif non seulement de la nature du droit d'accès comme composante de la protection des données à caractère personnel, mais également sur les limites de ce droit d'accès aux seules données à caractère personnel[551]. À travers cette décision, la CJUE ancre le droit d'accès aux données à caractère personnel puisque celui-ci s'applique dès lors qu'une donnée

---

[548] CJUE, 20 décembre 2017, C-434/16, *op. cit.*, §57. V. également Conclusions de l'avocat général Mme Julianne KOKOTT, *Peter Nowak c. Data Protection Officer*, présentées le 20 juillet 2017, C-434/16.

[549] « Everyone has the right of access to and the right to have corrections made to administrative documents and other data concerning them ». Parlement européen, *Resolution on the Constitution of the European Union*, A3-0064/94, publié au Journal Officiel des Communautés européennes le 28 février 1994, disponible sur https://www.europarl.europa.eu/charter/docs/pdf/a3_0064_94_en_en.pdf (consulté en avril 2022) ; GONZÁLEZ FUSTER Gloria, GUTWIRTH Serge, « Opening up personal data protection : A conceptual controversy », *Computer Law & Security Review*, Volume 29, Issue 5, octobre 2013, p. 535.

[550] MAHIEU René, « The Right of Access of Personal Data : a Genealogy », *Technology and Regulation,* 20 août 2021, Vol 2021, p. 72.

[551] CJUE, 17 juillet 2014, *YS*, C-141/12 et C-372/12.

concernant la personne concernée est qualifiée de donnée à caractère personnel[552]. Dans un second temps, la CJUE limite le droit d'accès aux données à caractère personnel aux seuls objectifs poursuivis par les instruments protégeant celles-ci (en l'espèce, la directive 95/46/CE), en affirmant clairement que :

> « le fait d'étendre le droit d'accès du demandeur du titre de séjour à cette analyse juridique servirait, en réalité, non pas à l'objectif de cette directive consistant à garantir la protection du droit à la vie privée de ce demandeur à l'égard du traitement des données le concernant, mais celui de lui assurer un droit d'accès aux documents administratifs, lequel n'est toutefois pas visé par la directive 95/46 »[553].

L'interprétation de la CJUE des contours du droit d'accès à ses données à caractère personnel est ainsi intimement liée à une interprétation stricte de la notion de donnée à caractère personnel, qui a pour conséquence d'empêcher un contournement du droit d'accès aux données à caractère personnel à des enjeux dépassant ses objectifs. En effet, la solution de la CJUE dans l'arrêt YS embrasse pleinement l'interprétation de la notion de données à caractère personnel proposée par l'avocat général :

> « Une analyse juridique est le raisonnement qui sous-tend la réponse apportée à une question de droit. La réponse elle-même peut prendre la forme d'un avis, d'une opinion ou d'une décision (et peut donc être juridiquement contraignante ou pas). À l'exception des éléments factuels sur lesquels elle repose (dont certains peuvent être des données à caractère personnel), cette analyse contient l'explication de la réponse donnée. L'explication en elle-même n'est pas une information concernant une personne identifiée ou identifiable. Au mieux, elle peut être qualifiée d'information relative à l'interprétation et à l'application du droit pertinent au regard duquel la situation juridique d'une personne physique est appréciée et (éventuellement) décidée. Il est possible que des données à caractère personnel et d'autres éléments de fait alimentent le processus aboutissant à répondre à cette question, mais cela ne fait pas de l'analyse juridique elle-même une donnée à caractère personnel »[554].

259. Cette interprétation restrictive du droit d'accès peut être expliquée par la volonté du juge européen d'empêcher la protection des données à caractère personnel de devenir « la loi de tout » (*the law of everything*)[555]. Cependant, la doctrine se montre également critique de

---

[552] CJUE, C-141/12 et C-372/12, *op. cit.*, §48 concernant les données à caractère personnel relatives au demandeur du titre de séjour dans la minute ; CJUE, C-434/16, *op. cit.*, §46 concernant la qualification de données à caractère personnel des réponses écrites fournies lors d'un examen professionnel et des éventuelles annotations de l'examinateur relatives à ces réponses.

[553] CJUE, C-141/12 et C-372/12, *op. cit.*, §46.

[554] Conclusions de l'avocat général Mme Eleanor SHARPSTON, *YS et autres*, présentées le 12 décembre 2013, C-41/12 et C-372/12.

[555] PURTOVA Nadezhda, « The law of everything. Broad concept of personal data and future of EU data protection law », *Law Information and Technology*, Vol. 10, 2018, Issue 1, p. 41. L'utilisation du droit d'accès par les

l'interprétation proposée par la CJUE, dans la mesure où cette interprétation ne permet pas à la personne concernée de contrôler l'ensemble des conséquences ayant le potentiel d'affecter la personne concernée. Par exemple, une partie de la doctrine considère que la définition des données à caractère personnel devrait évoluer en parallèle de leur capacité à influencer la vie des personnes concernées[556]. Ainsi, l'objectif du droit d'accès de la personne concernée à ses données à caractère personnel semble limité par la CJUE à la protection du droit à la vie privée, alors même qu'il a été justement argumenté que le droit d'accès à ses données à caractère personnel ne se limite pas à un tel objectif et poursuit également le but de rééquilibrer l'asymétrie d'information entre le responsable de traitement et la personne concernée[557]. La jurisprudence de la CJUE doit néanmoins être interprétée comme une interprétation de la notion de données à caractère personnel et non comme une interprétation de l'intention de la personne concernée lors de sa demande d'accès. En effet, l'EDPB précise dans ses lignes directrices relatives au droit d'accès, que « les responsables de traitement ne doivent jamais se demander « pourquoi » la personne concernée demande l'accès à ses données, mais seulement « quel est l'objet » de sa requête […] et s'ils détiennent des données à caractère personnel relatives à cet individu »[558].

260. Ainsi, malgré des limites discutables et discutées, le droit d'accès à ses données à caractère personnel constitue un instrument permettant de renforcer le contrôle de la personne concernée et de compenser l'asymétrie d'information entre la personne concernée et le responsable de traitement. En ce qui concerne le consentement, la personne concernée autrice du consentement se voit dotée d'un outil lui permettant de vérifier que la réalité du traitement de données à caractère personnel correspond effectivement au référentiel selon lequel elle a consenti : le droit d'accès à ses données à caractère personnel constitue une voie d'évaluation du caractère éclairé du consentement. L'importance du droit d'accès à ses données à caractère personnel à la fois comme vecteur de transparence et comme outil d'évaluation de la réalité du

---

personnes concernées comme une voie d'accès aux autres droits est également refusée par les autorités de contrôle. Par exemple, le droit d'accès ne donne pas droit à l'édition d'un certificat d'emploi, v. HDPA, 30 juillet 2020, 23/2020.

556 PURTOVA Nadezhda, *op. cit.*,, p. 73 ; REMPELL Scott, « Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas », *Florida Journal of International Law*, 2006, 18, p. 830.

557 BROWER Evelien, BORGESIUS Frederik Zuiderveen, « Access to Personal Data and the Right to Good Governance during Asylum Procedures after the CJEU's YS. And M. and S. judgement (C-141/12 and C-372-12) », *European Journal of Migration and Law*, 17(2-3), p. 266 ; MAHIEU René, *op. cit.*, p. 72.

558 EDPB, *Guidelines 01/2022 on data subjects rights – Right of access, op. cit.*, p. 9. L'autorité de contrôle italien, la Garente per la protezione dei dati personali a d'ailleurs insisté sur le fait que la personne concernée n'est pas tenue de motiver sa demande d'accès. GPDP, 16 septembre 2021, 9704032.

traitement est dépendante de la capacité de la personne concernée à exercer ce droit. La personne concernée doit notamment connaître qu'elle est titulaire du droit d'accès à ses données à caractère personnel[559]. Les articles 13 et 14 du RGPD exigent en effet tous deux du responsable de traitement d'informer le responsable de traitement de l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel. Dès lors, l'insuffisance d'information sur le droit d'accès à ses données à caractère personnel est sanctionnée par les autorités de contrôle[560], notamment dans les cas où le traitement est « invisible » comme dans le cas de la vidéosurveillance[561].

261. Par conséquent, le consentement de la personne concernée se voit renforcer par sa capacité d'accéder aux informations *a priori* pour évaluer si elle souhaite donner son consentement, et *a posteriori* pour évaluer si la réalité du traitement correspond au référentiel sur lequel elle s'est appuyée pour donner son consentement. Néanmoins, il semble que la personne concernée ne puisse pas pleinement profiter de ces outils, tant ses interactions avec les responsables de traitement sont diverses et nombreuses : la lecture attentive des politiques de protection des données se révélerait trop chronophage[562], tout comme l'exercice du droit d'accès[563]. Se pose dès lors la question de savoir si la personne concernée a « vraiment la capacité d'assumer [l] e rôle » de contrôleur à la fois de ses données à caractère personnel et à

559

La connaissance générale des citoyens européens de leurs droits en ligne n'est d'ailleurs pas homogène dans l'Union européenne. Elle est très élevée dans certains pays nordiques (la Finlande, la Suède et les Pays-Bas présentent des taux de connaissance des droits en ligne de plus de 84 %), tandis qu'elle est très basse dans certains pays de l'Union européenne (l'Italie, la Roumanie et la Bulgarie présentent des taux de connaissance des droits en ligne inférieurs à 40 %). Commission européenne, *Digital Rights and Principles*, Special Eurobarometer 518, septembre-octobre 2021.

560

AEPD, PS-00315-2019, publiée le 14 février 2020 ; GPDP, 2 juillet 2020, 9445180 ; APD, 20 juillet 2020, Décision quant au fond 41/2020 ; APD, 28 juillet 2020, Décision quant au fond 39/2020 ; HDPA, 3 août 2020, 24/2020 ; AEPD, PS-00477-2019, *op. cit.* ; APD, 17 février 2021, Décision quant au fond 24/2021 ; AEPD, PS-00177-2021, publiée le 10 juin 2021.

561

AEPD, PS-00273-2019, publiée le 9 avril 2019 ; AEPD, PS-00397-2019, publiée le 4 juillet 2019 ; BVwG, 25 novembre 2019, W211 2210458-1/10 ; ANSPDCP, 4 août 2020, *Asociația de proprietari Bl. FC 5, orașul Năvodari, județul Constanța* ; AEPD, PS-00479-2019, publiée le 5 août 2020 ; AEPD, PS-00030-2020, publiée le 9 octobre 2020 ; AEPD, PS-00227-2020, publiée le 10 novembre 2020 ; AEPD, PS-00151-2020, publiée le 14 avril 2021 ; AEPD, PS-00377-2021, publiée le 18 octobre 2021 ; AEPD, PS-00224-2021, publiée le 13 janvier 2022..

562 MCDONALD Aleecia, FAITH CRANOR Lorrie, *op. cit.*, pp. 543-568 ; OBAR Jonathan A., « The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services », *Information, Communication & Society*, 2020, Volume 23, Issue 1, pp. 128-147.

563 L'accès chronophage de l'exercice des droits a créé un besoin sur le marché, résultant en la création de services proposant de déléguer l'exercice de ces droits à une société, chargée de l'exercer pour l'ensemble des responsables de traitement traitant les données des personnes concernées, v. par exemple Mine, https://saymine.com/. L'apparition de tels acteurs dans le domaine de la protection des données à caractère personnel pose des questions en matière de protection de la vie privée, de violation de confidentialité des données à caractère personnel et de cybersécurité.

la fois de la licéité et de la réalité des traitements de données à caractère personnel tels qu'annoncés par le responsable de traitement[564]. Plus encore, la question est de savoir si la personne concernée est véritablement le destinataire de l'information délivrée par le responsable de traitement, selon la réflexion engagée par Emmanuel Netter :

> « Si l'on admet l'idée, d'un pessimisme raisonnable, que l'utilisateur moyen ne fera pas grand-chose des informations qui lui sont adressées, il faut alors envisager l'hypothèse selon laquelle la transparence s'adresserait en réalité – ou de surcroît – à d'autres que lui. Qui sont ces autres ? »[565].

§2 – L'exhaustivité de l'information à des fins de contrôle par l'expert

262. Il vient d'être démontré que le destinataire premier de l'information délivrée par le responsable de traitement est la personne concernée afin qu'elle puisse à la fois consentir de manière éclairée au traitement de ses données et contrôler leur utilisation réelle une fois son consentement exprimé. La transparence est donc utile et nécessaire à la personne concernée qui, sensibilisée à la question de la protection des données à caractère personnel, souhaite se saisir de ces informations. Ainsi, « la transparence nécessite toujours des efforts de la part de ses destinataires, une volonté d'être informée »[566].

263. De plus, il peut être reproché au RGPD de vouloir concilier exhaustivité de l'information et accessibilité de celle-ci, alors même que ces objectifs semblent inconciliables. En effet, une information exhaustive est de nature contraire à l'accessibilité de l'information : si la structure de l'information multiniveaux est une solution satisfaisante afin de permettre à la personne concernée d'avoir en premier lieu, une vision d'ensemble des éléments nécessaires à l'exercice de son consentement, cette lecture reste un effort qui, isolé, est négligeable, mais devient colossal lorsqu'il est répété. Or, il s'agit bien là du cœur de l'absence de conciliation possible entre une information accessible et exhaustive.

264. Prenons l'exemple d'une navigation moyenne sur internet. Le rapport Digital 2021 France estime qu'un Français passe en moyenne 5 heures et 37 minutes de son temps par jour à naviguer sur internet[567]. Or, même la première information de premier niveau de certains acteurs reste colossale. Si l'on se réfère au classement des sites internet les plus visités en France

---

[564] EYNARD Jessica, « RGPD « empouvoirement » individuel : promesse tenue ou espoir déçu », *Revue des Affaires Européennes*, 2021/1, p. 25

[565] NETTER Emmanuel, 2020, *op. cit.*, p. 611.

[566] *Ibidem.*

[567] We are social, *Digital 2021* France, Special Report, p. 22, disponible sur https://wearesocial.com/fr/blog/2021/01/digital-2021-france/ (consulté en avril 2022).

en décembre 2020 selon SimilarWeb[568], lire le premier niveau d'information des politiques de confidentialité des dix sites les plus visités en France prendrait en moyenne deux heures et vingt minutes.

#	Site internet[569]	Nombre de mots de l'information premier niveau	Temps de lecture moyen évalué sur une base de 300 mots par minute	Temps moyen passé par visite[570]
1 2 4	Google.com Youtube.com Google.fr	6174	20 minutes et 34 secondes	11 minutes et 54 secondes 21 minutes et 14 secondes 8 minutes et 45 secondes
3	Facebook.com	5467	18 minutes et 13 secondes	9 minutes et 58 secondes
5	Amazon.fr	5509	18 minutes et 21 secondes	8 minutes et 10 secondes
6	Wikipedia.org	6835	22 minutes et 46 secondes	3 minutes et 59 secondes
7	Orange.fr	1429	4 minutes et 45 secondes	8 minutes et 50 secondes
8	Twitter.com	6808	22 minutes et 41 secondes	10 minutes et 50 secondes
9	Leboncoin.fr	5138	17 minutes et 7 secondes	11 minutes et 58 secondes
10	Live.com	4081	13 minutes et 36 secondes	8 minutes et 42 secondes

Figure 1 - Calcul du temps de lecture moyen des politiques de confidentialité premier niveau (comparé au temps moyenne passé par visite)

265. Il serait naïf de penser que le législateur européen n'a pas identifié cette difficulté lors de l'élaboration du RGPD. Au contraire, il semble que le législateur européen ait cherché à protéger doublement le consentement éclairé de la personne concernée. La première protection est celle qui est sus-étudiée : la personne concernée est dotée de moyens suffisants à l'exercice de son consentement éclairé, et peut contrôler de manière ex post la manière dont ses données à caractère personnel sont traitées par le responsable de traitement. La seconde est implicite : en exigeant du responsable de traitement de délivrer une information exhaustive, le législateur

[568] *Idem*, p. 33.
[569] Le classement des sites les plus visités en France a été établi par SimilarWeb sur la base du volume total de trafic en décembre 2020. *Ibidem.*
[570] Le temps moyen de visite par site internet a été calculé par SimilarWeb sur la base du volume total de trafic en décembre 2020. *Ibidem.*

européen permet à l'expert d'analyser la conformité au RGPD des responsables de traitement, informant indirectement la personne concernée. Ces experts sont en premier lieu les acteurs de la société civile spécialisés en protection des données à caractère personnel (A) et en second lieu, les autorités de contrôle (B).

A. Les acteurs de la société civile

266. Les acteurs de la société civile spécialisés en protection des données à caractère personnel permettent aux personnes concernées et aux responsables de traitement d'avoir accès à des analyses, informations et décisions sur la protection des données à caractère personnel afin, pour les premiers, de conserver le contrôle de leurs données à caractère personnel, pour les seconds, de se mettre en conformité avec le RGPD.

267. L'importance des acteurs de la société civile spécialisés en protection des données à caractère personnel a été notamment été mise en lumière par les arrêts Max Schrems, None of your business et La Quadrature du Net. Les arrêts Schrems sont peut-être les plus spectaculaires puisqu'ils ont abouti, à deux reprises, à l'annulation des décisions d'adéquation de la Commission européenne concernant les transferts de données vers les États-Unis[571]. Si la conséquence de ces arrêts est importante à la fois pour les citoyens européens et pour les entreprises traitant des données aux États-Unis, il est important de noter que les recours intentés ont dû faire l'objet d'une analyse juridique difficile, notamment en ce qui concerne la structure des dispositifs juridiques mis en place dans le cadre de la surveillance par les agences de sécurité américaines. Pour s'en convaincre, il suffit de se référer aux ressources engagées lors de l'affaire Schrems II : d'après *None of Your Business*, l'affaire a nécessité six semaines d'auditions, l'analyse de 45 000 pages de documents, pour une facture finale dépassant les deux millions d'euros[572].

268. La protection des données à caractère personnel dans le cadre du RGPD n'est pas le seul domaine relatif à la protection de la vie privée et des données à caractère personnel dans lequel l'engagement de la société civile est important et aboutit à une réflexion juridique renouvelée sur certaines dispositions, parfois confirmées, parfois infirmées. En effet, les associations de

---

571 CJUE, Gde ch., 6 octobre 2015, *Schrems*, C362/14 ; CJUE, Gde ch., 16 juillet 2020, *Facebook Ireland et Schrems*, C-311/18.

572 None of Your Business, « DPC ordered to pick up most of the legal bill of EU-US data transfer case », *noyb.eu*, 30 octobre 2020, disponible sur https://noyb.eu/en/dpc-ordered-pick-most-legal-bill-eu-us-data-transfer-case (consulté en avril 2022) ; NextInpact, « Privacy Shield : la CNIL irlandaise devrait payer la facture monstre des frais de Max Schrems », 2 novembre 2020, disponible sur https://www.nextinpact.com/lebrief/44457/privacy-shield-cnil-irlandaise-devrait-payer-facture-monstre-frais-max-schrems (consulté en avril 2022).

protection de la vie privée et des données à caractère personnel sont aussi très présentes sur les sujets relatifs à la surveillance étatique. Au niveau français, la Quadrature du Net a par exemple permis le réexamen de plusieurs dispositifs juridiques de surveillance par le Conseil constitutionnel, donnant par exemple l'occasion à ce dernier d'infirmer le dispositif de captation générale et indifférenciée des données à caractère personnel dans le cadre de la recherche, de la constatation et de la poursuite des infractions pénales[573] ou encore de confirmer l'exception au droit de la défense lorsque le Procureur de la République utilise de manière légale des dispositifs de surveillance classés secret défense[574].

269. L'implication d'acteurs de la société civile est d'autant plus importante que les systèmes de traitement des données à caractère personnel se complexifient à la fois au niveau de la technique informatique que de la technique juridique. La complexification des traitements de données à caractère personnel a créé un besoin d'analyse de ces traitements par des experts, qui sont généralement constitués soit de chercheurs, soit de professionnels de la protection des données à caractère personnel. En effet, les systèmes de plus en plus élaborés de traitement de données à caractère personnel ainsi que la présence de nombreux transferts de données à caractère personnel hors Union européenne complexifient l'application du RGPD, dont les définitions[575] et les principes[576] nécessitent une analyse juridique fine pour être appliqués aux systèmes les plus raffinés.

270. Les politiques de protection des données à caractère personnel peuvent dès lors constituer un instrument privilégié l'examen du public. De la même manière que les associations en matière de protection de la consommation, les politiques de protection des données vont se révéler être des outils d'examen des pratiques des responsables de traitement, examen à la fois de la réalité de leur discours et de leur positionnement quant à la protection des données à caractère personnel. Ces différentes analyses peuvent, à terme, fournir aux

---

573 Conseil constitutionnel, Décision n°2021-976/977 QPC du 25 février 2022.

574 Conseil constitutionnel, Décision n°2022-987 QPC du 8 avril 2022

575 L'exemple de la décision de l'APD concernant le *Transparency and Consent Framework* est particulièrement parlant, puisque malgré une définition large de la notion de données à caractère personnel, le raisonnement juridique concluant à la qualification de la TC string en tant que donnée à caractère personnel s'étale sur onze considérants. APD, Décision sur le fond 21/2022 du 2 février 2022.

576 La mise en demeure anonymisée de la CNIL relative à l'utilisation de l'outil Google Analytics implique notamment l'analyse des dispositions européennes et américaines de protection des données, ainsi que l'ensemble des mécanismes de transfert des données à caractère personnel vers les États-Unis. CNIL, 10 février 2022, « Utilisation de Google Analytics et transferts de données vers les États-Unis : la CNIL met en demeure un gestionnaire de site web », 10 février 2022, disponible sur https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure (consulté en avril 2022).

responsables de traitement et aux personnes concernées des informations précieuses renforçant leur protection des données à caractère personnel pour les premiers, renforçant leur capacité de donner leur consentement éclairé pour les seconds.

271. L'analyse de la réalité du discours des responsables de traitement est nécessaire au rééquilibrage de l'asymétrie d'information existante entre le responsable de traitement, détenteur de l'information, et la personne concernée, dont l'information se limite souvent à celles que le responsable de traitement accepte de divulguer. Le passage d'un système de déclaration administrative à un système d'*accountability* n'a fait que renforcer la nécessité pour la personne concernée d'avoir les moyens de « faire confiance » aux acteurs du marché européen du numérique (il s'agit, nous le rappelons, d'un des objectifs que la Commission cherche à atteindre, notamment à l'aide du RGPD). L'émission d'une politique de protection des données à caractère personnel à destination des personnes concernées constitue à la fois un droit à l'information de la personne concernée, mais également une obligation déclarative pour le responsable de traitement, à travers laquelle il engage sa responsabilité quant à sa véracité. En l'absence de contrôle préalable de véracité des informations délivrées par le responsable de traitement, il est probable que le marché européen soit en partie faussé par des politiques de confidentialité trompeuses ou mensongères. S'il s'agit initialement du rôle des autorités de contrôle et des autorités de justice de contrôler la véracité de ces politiques de confidentialité, la multiplication des acteurs du numérique a pour conséquence de complexifier cette mission, à un niveau herculéen. Les associations de protection de la vie privée et des données à caractère personnel constituent dès lors un complément de contrôle utile. L'association *None of Your Business* s'est par exemple lancée dans la lutte contre les *dark patterns* en matière de cookies[577]. L'association autrichienne a créé un système automatique d'évaluation des bannières de cookies et de création de recours juridiques, réexaminé par leurs membres, afin de repérer les *dark patterns* faussant la perception de la personne concernée des pratiques de traitement des données à caractère personnel réalisées par le responsable de traitement[578]. *None of Your Business* vérifie en particulier l'adéquation entre les cookies annoncés comme étant installés sur le terminal de l'utilisateur et ceux effectivement installés[579]. Leur action a entraîné le

[577] None of Your Business, « Noyb aims to end « cookie banner terror » and issues more than 500 GDPR complaints », 31 mai 2021, disponible sur https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints
[578] *Ibidem.*
[579] *Ibidem.*

changement des bannières de cookies de responsables de traitement, dont 42 % dans les 30 jours de la réception du projet de plainte de l'association[580].

Figure 2 - Exemple de résultat de l'action de Noyb[581]

Le consentement éclairé de la personne concernée se voit ainsi renforcé par l'information délivrée par les acteurs de la société civile, puis dans un deuxième temps par la stratégie de recours de ces acteurs, permettant la condamnation et la mise en conformité des responsables de traitement à l'obligation de transparence et aux différentes dispositions du Règlement.

272. En parallèle, les politiques de protection des données à caractère personnel fournissent des informations utiles à la personne concernée pour exercer son consentement. Or, ces informations ne sont pas toujours bien comprises par des personnes n'ayant ni le temps, ou les connaissances, ou encore les compétences de les comprendre. L'inadéquation du besoin d'être informé avec les solutions légales proposées pour répondre à ce besoin crée une place sur le marché pour des outils évaluateurs de la protection des données à caractère personnel des acteurs présents sur le marché européen. L'exemple du site internet PrivacyBoard est parlant. PrivacyBoard se propose de noter des responsables de traitement grâce à un « Privacy score » calculé à la suite d'un audit de celui-ci selon plusieurs critères : les violations de données, le processus relatif aux demandes d'accès aux données, l'étude d'impact, la formation des

[580] None of Your Business, « More Cookie Banners to go Second Wave of Complaints Underway », 4 mars 2022, disponible sur https://noyb.eu/en/more-cookie-banners-go-second-wave-complaints-underway
[581] *Ibidem.*

employés, la politique de sécurité, les mesures de sécurité, le cryptage des données, les restrictions d'accès, la réutilisation des données à caractère personnel, les cookies et la soumission ou non au Cloud Act et au FISA[582]. D'autres critères ont pu être utilisés par les organismes proposant une évaluation de la conformité au RGPD et de la protection de la vie privée des utilisateurs, par exemple le *tracking* des personnes concernées[583], l'accès et la qualité politiques de protection des données[584], la durée de conservation des données,[585] etc. Si une grande partie des « Privacy Score » révèlent *a minima* les critères utilisés dans leur évaluation, certains de ces outils sont assez peu transparents quant au calcul de ces scores[586].

273. Enfin, le chercheur est également un acteur privilégié en matière de protection des données à caractère personnel. À travers sa posture d'universitaire, le chercheur va pouvoir fournir des analyses scientifiques à destination de ses pairs, mais également développer des outils permettant aux personnes concernées d'exercer un choix éclairé, ou à la société civile de s'emparer de sujets permettant le renforcement du consentement des personnes concernées. Par exemple, des travaux de recherche ont utilisé les politiques de protection des données à caractère personnel publiées par les responsables de traitement pour en mesurer les effets sur les personnes concernées[587], leur qualité[588], pour créer des outils automatiques d'évaluation des politiques de protection des données,[589] etc. Le chercheur va également évaluer l'adéquation entre le discours du responsable de traitement, les attentes raisonnables de la personne concernée et la réalité des traitements de données à caractère personnel. Par exemple, une équipe de chercheurs a évalué la quantité de collecte de données à caractère personnel dans les formulaires avant la soumission du formulaire[590] : à travers l'outil développé dans ce cadre, les

---

[582] Par exemple, Visitor Analytics obtient un score de 100 %. Privacy board, https://www.privacyboard.co/software/visitor-analytics (consulté en avril 2022).

[583] Privacyscore, https://privacyscore.org/.

[584] Ranking Digital Rights, https://rankingdigitalrights.org/index2019/categories/privacy/.

[585] Privacy Rating, https://www.privacyrating.info/#/about.

[586] Privacy Monitor, https://www.privacymonitor.com/articles/privacy-guide/ ; Common sense, https://privacy.commonsense.org/resource/evaluation-questions.

[587] v. par exemple WU Kuang-Wen *et al.* « The effect of online privacy policy on consumer privacy concern and trust », *Computers in Human Behavior*, Volume 28, Issue 3, mai 2012, p. 889-897 ; GRIGGIO Carla F., « Caught in the Network : The Impact of WhatsApp's 2021 Privacy Policy Update on Users' Messaging App Ecosystems », *CHI'22*, New Orleans, 29 avril-5 mai 2022.

[588] V. par exemple MILLER Elizabeth *et al.*, « I Don't Know Why You Need My Data: A Case Study of Popular Social Media Privacy Policies », *CODASPY '22 : Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy*, avril 2022, pp. 340-342.

[589] V. par exemple ZAEEL Razieh Nokhbeh, « PrivacyCheck v3 : Empowering Users with Higher-Level Understanding of Privacy Policies », *WSDM '22 : Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining*, Février 2022, pp. 1593-1596.

[590] SENOL Asuman *et al.*, « Leaky Forms : A Study of Email and Password Exfiltration Before Form Submission », *USENIX Security'22*, 18 p.

personnes concernées acquièrent la capacité de détecter des traitements invisibles, dépassant leurs attentes raisonnables, et de choisir dès lors les responsables de traitement de leurs données à caractère personnel en étant davantage informées. De plus, le chercheur contribue au débat public autour de la protection des données à caractère personnel, discutant avec les pouvoirs publics chargés de son implémentation comme la CNIL[591], le CNNum[592], ou encore l'EDPB[593]. Les chercheurs vont également alimenter le débat public en prenant position à travers des tribunes publiées au sein de journaux médiatiques[594] ou scientifiques[595].

274. Les politiques de protection des données ne se limitent ainsi pas à leur rôle de déclaration des traitements de données à caractère personnel à destination des personnes concernées, mais constituent également un instrument de surveillance collective facilitée par les acteurs de la société civile. À ce rôle s'ajoute un rôle déclaratif dans le cadre de l'*accountability*, la politique de protection des données à caractère personnel jouant un rôle de démonstration de la conformité du responsable de traitement à la protection des données à caractère personnel.

B. L'autorité de contrôle

275. L'article 57 du RGPD confie la mission de contrôler l'application du RGPD aux autorités de contrôle. La CNIL est ainsi chargée de veiller à l'application du règlement par les responsables de traitement disposant d'un établissement en France ou traitant des données à

---

[591] La CNIL organise le 28 juin 2022 la première édition du *Privacy Research Day* dont l'objectif est de « renforcer les échanges entre les experts juridiques et techniques de la CNIL et les chercheurs en informatiques et en sciences humaines et sociales » et, pour la CNIL, d'envisager « plusieurs types de collaborations avec le monde de la recherche : participation à des projets de recherche, développement conjoint d'études, co-encadrement de doctorants, accueil de chercheurs en résidence… ». CNIL, « Évènement : la CNIL organise la première édition du Privacy Research Day, 18 février 2022, disponible sur https://www.cnil.fr/fr/evenement-la-cnil-organise-la-premiere-edition-du-privacy-research-day (consulté en avril 2022).

[592] Le Conseil national du numérique est composé de 17 membres, parmi lesquels des chercheurs. CNNUM, « Le Conseil », disponible sur https://cnnumerique.fr/le-conseil (consulté en avril 2022).

[593] L'EDPB soumet régulièrement ses lignes directrices à consultation publique. Par exemple, le professeur Zwenne de l'Université de Leiden a pu soumettre ses commentaires à propos des lignes directrices de l'EDPB relative au droit d'accès à ses données à caractère personnel. ZWENNE Gerrit-Jan, « Comments. EDPB Guidelines 01/2022 on Data Subject Access, version 1.0, adopted on 18 January 2022 », soumis le 9 mars 2022, disponible sur https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/ZWENNE_COMMENTS_on_EDPB-guidelines_01_2022_DSARs_DEF.pdf (consulté en avril 2022).

[594] V. par exemple ABITEBOUL Serge, DOWEK Gilles, « La propriété des données personnelles est une fausse bonne idée », *LeMonde.fr*, 5 février 2018, disponible sur https://www.lemonde.fr/idees/article/2018/02/05/la-propriete-des-donnees-personnelles-est-une-fausse-bonne-idee_5252158_3232.html (consulté en avril 2022) ; DALMONT Cyrille, « Données personnelles : pourquoi le RGPD est déjà dépassé », *LesEchos.fr*, 22 novembre 2019, disponible sur https://www.lesechos.fr/idees-debats/cercle/donnees-personnelles-pourquoi-le-rgpd-est-deja-depasse-1149930 (consulté en avril 2022).

[595] V. par exemple SPIEKERMANN Sarah *et al.* « Data protection in Europe – Academics are taking a position », *Computer Law & Security Review*, avril 2013, 29(2), pp. 180-184.

caractère personnel de personnes concernées résidant en France[596]. La CNIL contrôle les responsables de traitement sur la base des réclamations et signalements, mais également de sa propre initiative[597]. Il existe quatre formes de contrôle de la CNIL : le contrôle sur place, l'audition sur convocation, le contrôle en ligne et le contrôle sur pièce[598].

276. Si le contrôle sur place est privilégié, la CNIL a toutefois souvent recours au contrôle en ligne[599]. En effet, la part de contrôles en ligne représentait 34 % des contrôles effectués par la CNIL en 2020 (87 sur 247)[600] et 18 % des contrôles effectués en 2019 (53 sur 300)[601]. D'après la CNIL, « le contrôle en ligne vise prioritairement à obtenir copie d'informations (éléments techniques et juridiques) permettant d'évaluer les conditions dans lesquelles sont mis en œuvre les traitements »[602]. Dans ce cadre, la politique de confidentialité, et plus largement, les informations délivrées par le responsable de traitement à la personne concernée dans le cadre de l'obligation de transparence constituent le premier niveau de contrôle en ligne de la CNIL.

277. Dès lors, les informations délivrées par le responsable de traitement constituent un élément probant de l'*accountability* et de la conformité du responsable de traitement. En 2019, le manquement à l'obligation d'information constituait 14 % des décisions adoptées par les autorités de contrôle européennes[603]. Cependant, il serait difficile de considérer que les politiques de confidentialité sont essentiellement destinées aux autorités de contrôle, et ce à deux titres.

278. Premièrement, la démarche d'*accountability* ne saurait se résumer à l'aspect déclaratif de la politique de confidentialité. Au contraire, l'*accountability* est un concept « protéiforme » qui sous-entend une approche globale se traduisant « par une réflexion destinée à identifier la meilleure organisation possible et évaluer de manière efficace et proactive les modalités d'identification et de prise en compte des risques liés à la mise en œuvre des traitements, pour ensuite déterminer les mesures et actions à engager »[604]. Dès lors, la politique de confidentialité

---

[596] CNIL, « Comment se passe un contrôle de la CNIL », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/comment-se-passe-un-controle-de-la-cnil
[597] *Ibidem.*
[598] *Ibidem.*
[599] CNIL, « Mission 4 – Contrôler et sanctionner », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/mission-4-controler-et-sanctionner.
[600] CNIL, Rapport d'activité, 2020, La Documentation française, p. 7.
[601] CNIL, Rapport d'activité, 2019, La Documentation française, p. 3.
[602] CNIL, *Charte des contrôles de la CNIL*, version du 5 août 2020, p. 12.
[603] ARMINGAUD Claude-Etienne, BOURNY Marianne, « Surveiller et punir à l'aune du RGPD : l'harmonisation à l'épreuve de la diversité européenne », *Revue Lamy Droit de l'Immatériel*, n° 163, 1er octobre 2019.
[604] METALLINOS Nathalie, « Accoutability – Le principe d'accountability : des formalités préalables aux études d'impact sur la vie privée (EIVP) », *Communication Commerce électronique*, n°4, avril 2018, dossier 11.

n'est qu'une composante de la démarche d'a*ccountability* puisque le responsable de traitement devra démontrer qu'il a mis en œuvre des processus, mesures organisationnelles et techniques, audits et sensibilisation pour que la politique de confidentialité délivrée soit non seulement conforme au RGPD, mais reflète également la réalité des traitements de données à caractère personnel qu'il met en place.

279. Deuxièmement, comme il l'a été rappelé précédemment, les autorités de contrôle n'évaluent pas les politiques de confidentialité de manière déconnectée de la personne concernée. Au contraire, les autorités de contrôle évaluent les politiques de confidentialité selon le référentiel de la personne concernée qui doit être capable d'exercer ses droits[605] et de comprendre les opérations de traitement mises en place par le responsable de traitement[606].

280. Ainsi, le destinataire premier et principal de l'information délivrée par le responsable de traitement est la personne concernée. Si l'autorité de contrôle peut se saisir de la politique de confidentialité pour exercer son contrôle, notamment en ligne, la politique de confidentialité ne constitue qu'un premier niveau de ce contrôle, les instruments privilégiés de la démonstration de la conformité au RGPD étant le registre de traitement et le programme de management des données à caractère personnel. Dès lors, l'obligation de transparence ne peut se comprendre que comme un instrument de contrôle du traitement des données à caractère personnel dont est dotée la personne concernée, afin notamment de contrôler la réalité du traitement avec son référentiel de consentement. Ce contrôle de la réalité du traitement peut s'exercer soit de manière individuelle, à travers la lecture de politiques de confidentialité ou encore de l'exercice par la personne concernée de son droit d'accès, soit de manière collective, à travers les analyses et l'activisme de la société civile, informant la personne concernée de la

---

[605] Tietosuojavaltuutetun toimisto, 26 mai 2020, 8393/161/2019 ; DPC, 20 août 2021, Whatsapp Ireland Limited - IN-18-12-2

[606] CE, 19 juin 2020, n°420810 ; CNIL, Délibération de la formation restreinte n° SAN-2020-018 du 8 décembre 2020 concernant la société NESTOR SAS ; CNIL, Délibération de la formation restreinte SAN-2020-008 du 18 novembre 2020 concernant la société Carrefour France ; CNIL, Délibération de la formation restreinte SAN-2020-009 du 18 novembre 2020 concernant la société Carrefour Banque ; CNIL, Délibération de la formation restreinte n° SAN-2019-010 du 21 novembre 2019 concernant la société Futura Internationale ; CNIL, Délibération n°2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » (demande d'avis n°20008032) ; Tietosuojavaltuutetun toimisto, 26 mai 2020, 8393/161/2019 ; GPDP, 16 décembre 2021, 9735672 ; EPDB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65 (1) (a), adoptée le 28 juillet 2021 ; DPC, 20 août 2021, Whatsapp Ireland Limited - IN-18-12-2 ; Datatilsynet, 9 novembre 2020, 20/01949 (PVN-2020-13) ; APD, 13 novembre 2020, Décision quant au fond 73/2020 ; APD, 20 juillet 2020, Décision quant au fond 41/2020.

réalité des pratiques des personnes concernées et lui permettant ainsi d'exercer son consentement dans un environnement conforme au RGPD et à son référentiel de consentement.

281. L'obligation de transparence est alors la modalité privilégiée du caractère éclairé du consentement de la personne concernée. Elle ne saurait cependant suffire à assurer la réalité du consentement, qui doit effectivement et véritablement coïncider avec la volonté de la personne concernée.

282. Conclusion de Section. – La recherche de l'exhaustivité de l'information permet au législateur européen de protéger le consentement éclairé de la personne concernée directement et indirectement. De manière directe, la personne concernée se voit délivrer l'ensemble des informations nécessaires à sa prise de décision et au contrôle du traitement de ses données à caractère personnel. Ainsi, dans une logique d'*empowerement*, la personne concernée peut être active de sa propre protection et vérifier à tout moment l'adéquation du traitement avec son référentiel de consentement. De manière indirecte, la personne concernée est accompagnée dans son contrôle par l'expert, qui pourra, grâce à l'ensemble des informations délivrées par le responsable de traitement, alerter la personne concernée de toute anomalie dans la mise en œuvre des traitements.

Conclusion du Chapitre 2

283. Les conditions matérielles attachées à l'obligation d'information jouent un rôle essentiel dans la validité du consentement. En effet, le consentement éclairé est intrinsèquement lié à la connaissance par son émetteur de l'ensemble des informations nécessaires à sa prise de décision.

284. Les enjeux de la définition des conditions matérielles attachées à l'obligation d'information dépassent le simple respect du RGPD. En effet, cet effort de définition s'inscrit dans l'ensemble de la philosophie européenne traversant la protection des données à caractère personnel. Ainsi, un consentement suffisamment informé – et donc éclairé – permet à la fois de protéger la personne concernée en lui octroyant le contrôle de ses données à caractère personnel et de garantir le bon fonctionnement du marché numérique, selon l'objectif annoncé de la Commission européenne d'accroître la confiance dans le marché par le respect des droits humains sur ce marché et notamment, de la protection des données à caractère personnel.

285. En pratique, les conditions matérielles permettent aux personnes concernées d'exercer leur consentement en ayant une connaissance suffisante des traitements de données à caractère personnel leur permettant de comparer la réalité estimée de ces traitements avec leur référentiel de décision. Cette comparaison est garantie logiquement au moment de l'émission du consentement, par la délivrance d'informations préalables à l'acte de consentir, mais également durant toute la durée du consentement, à travers le contrôle exercé par la personne concernée ou par l'expert.

Conclusion du Titre 1

286. La réalité du caractère éclairé du consentement de la personne concernée se concrétise par la consécration de la transparence comme principe central et exigeant au sein du RGPD. Ce faisant, le législateur européen a opéré une double évolution du principe de transparence, à la fois formel et matériel.

287. Le renforcement formel du principe de transparence se matérialise en un véritable droit à l'information. La philosophie du droit à l'information s'explique aisément par l'asymétrie d'information manifeste entre le responsable de traitement et la personne concernée. Les pratiques des responsables de traitement sous l'égide de la directive 95/46/CE ont permis de révéler la nécessité d'équilibrer la relation entre le responsable de traitement et la personne concernée en matière de connaissance, ce qui constitue un prérequis de la logique d'*empowerement* poursuivi par le règlement. Dès lors, sous le régime du RGPD, la délivrance de l'information à la personne concernée ne suffit plus à satisfaire l'obligation de transparence : la nature de droit inverse le processus d'évaluation du principe de transparence qui s'analyse désormais du point de vue de la personne concernée. Ainsi, un traitement est suffisamment transparent lorsque la personne concernée peut accéder à l'information. La transparence nécessite alors des efforts importants de la part du responsable de traitement qui doit rendre l'information accessible à la fois physiquement et intellectuellement. La transparence, et par extension, le consentement éclairé s'évalue ainsi par la capacité de la personne concernée de trouver l'information et de la comprendre sans effort.

288. Le renforcement matériel du principe de transparence se matérialise quant à lui dans la divulgation d'informations suffisantes pour permettre à la personne concernée de faire un choix éclairé. La garantie d'un choix éclairé est essentielle pour permettre à la personne concernée d'avoir le contrôle de ses données à caractère personnel, mais également pour permettre le bon fonctionnement du marché en limitant les éléments d'irrationalité. Placée au centre de la protection de ses données à caractère personnel, la personne concernée se voit octroyer les moyens d'exercer un contrôle sur les traitements de données à caractère personnel opérés par le responsable de traitement au moment de l'émission de son consentement, mais également durant toute la durée de son consentement. Accompagnée dans son contrôle par l'expert qui pourra l'alerter ou l'indemniser, la personne concernée atteint un niveau de connaissance satisfaisant à l'émission d'un consentement éclairé.

289. Ce constat se doit d'être nuancé. En effet, le législateur a manqué l'occasion de créer des « incitants »[607] législatifs permettant une pratique plus inclusive de l'accessibilité de l'information : le RGPD ne protège pas suffisamment certaines populations vulnérables, et il est regrettable que le législateur n'ait pas poussé sa réflexion sur les méthodes de délivrance de l'information. De même, l'interprétation des conditions matérielles n'est pas établie en matière de consentement de la personne concernée, oscillant entre un cœur d'information *a priori* nécessaire à l'émission du consentement et l'analyse casuistique du référentiel de la personne concernée.

290. Malgré ces nuances, le législateur a substantiellement contribué à permettre à la personne concernée de mieux s'informer avant sa prise de décision. Afin de garantir la réalité du consentement de la personne concernée, les dispositions renforçant le caractère éclairé du consentement ont été accompagnées de garanties visant à préserver la liberté de consentement de la personne concernée.

607
Groupe de travail « Article 29 », WP259 rev. 01, p. 15.

TITRE 2 – LE RENFORCEMENT DU CONSENTEMENT LIBRE

291. Selon le Groupe de travail « Article 29 », le consentement suppose une manifestation de volonté libre et « l'adjectif « libre » implique un choix et un contrôle réel pour les personnes concernées »[608]. Ainsi, la liberté au sens de l'exigence d'un consentement « libre » par le RGPD[609] se traduit d'après le Groupe de travail « Article 29 » comme une liberté de choix de la personne concernée et suppose, dès lors, un effort de protection de ce choix par le Règlement.

292. La question du choix a été un sujet largement traité en philosophie. Déjà dans l'Antiquité, Platon affirmait que le choix délibéré (la *proaïrésis*) distinguait l'homme des autres êtres[610]. Le choix, et la liberté de choix, a fait l'objet de « débats passionnés » puisque la question fait appel d'une part à des théories déterministes diverses et d'autre part à des théories se fondant sur les notions de liberté humaine et de libre arbitre[611]. Le droit a fait le choix pragmatique de poser la liberté humaine comme principe, car les « systèmes juridiques […], soucieux d'efficacité dans leurs menaces et sanctions, seraient embarrassés par la liberté imprévisible »[612]. La conception moderne de la responsabilité, associant la matérialité de l'acte au caractère volontaire de l'action en est l'illustration la plus flagrante dans la mesure puisqu'en conséquence, « un élément important de la reconnaissance contemporaine de la responsabilité d'une personne (ou au contraire du déni de sa responsabilité) est l'existence (ou l'absence) d'un *choix* volontaire de sa part »[613]. Dans la conception juridique, le libre arbitre, ou liberté de la volonté, s'impose alors comme une prémisse de l'application des règles juridiques de l'individu, puisqu'elle se définit comme « la capacité de former soi-même ses intentions d'action »[614].

---

[608] Groupe de travail « Article 29 », WP259 rev. 01, p. 6.
[609] RGPD, 27 avril 2016, Article 4(2)(11).
[610] ZIELINSKI Agata, « Le libre choix. De l'autonomie rêvée à l'attention aux capacités », *Gérontologie et société,* 2009/4, vol. 32, n°131, p. 11.
[611] MORANGE Jean, « Liberté », in ALLAND Denis, RIALS Stéphane (dir.), *Dictionnaire de la culture juridique,* Paris, Quadridge/Lamy-Puf, 2003, p. 945.
[612] SEVE René, *Philosophie et théorie du droit,* Paris, Dalloz, 2e ed., 2017, pp. 69-70.
[613] GUILLARME Bertrand, « Usages de la Responsabilité », *Revue française de science politique,* 2008/6, vol. 58, p. 873.
[614] ESFELD Michaël, *La philosophie de l'esprit – Une introduction aux débats contemporains*, Paris, Armand Colin, 2020, 3e ed., 256 p.

293. La notion de choix se rapproche également de la notion de décision. Si la littérature scientifique semble parfois ne pas s'encombrer de la distinction entre choix et décision[615], utilisant ces termes comme synonymes, le choix et la décision peuvent être distingués chronologiquement, le choix résultant de la décision. Un premier indice d'une telle différence se trouve dans l'étymologie de chacun de ces termes. Le terme « décision » est emprunté au latin classique *decisio* qui signifie « action de trancher une question débattue »[616]. Le terme « choisir » semble quant à lui provenir de l'ancien français *coisir* signifiant « distinguer, voir distinctement »[617]. Ainsi, le choix intervient au moment de la comparaison entre différentes options, quand la décision désigne plus largement l'ensemble du processus permettant de trancher une question : la décision intervient à un moment où la question reste « débattue », ambiguë et implique de réfléchir à chacune des options. Cette distinction se confirme par la recherche en neuropsychologie. Selon Jeffrey D. Schall, le choix implique de pouvoir être expliqué par la préférence d'une option en vue d'atteindre un but déterminé[618]. Ainsi, « alors que le choix fait référence à l'engagement final en faveur d'une alternative, la décision fait référence à la délibération précédente sur les alternatives »[619]. Dès lors, une des différences entre le choix et la décision est que le choix peut s'anticiper quand la décision ne s'anticipe pas et « semble simplement se produire »[620].

294. Le RGPD définit le consentement comme « toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne accepte, par une déclaration ou un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement »[621]. Le consentement est donc bien le résultat d'un choix puisqu'il porte sur un objet déterminé (les options sont ainsi identifiées) et ce choix peut être anticipé dans la mesure où il intervient à un moment déterminé pendant lequel la personne concernée devra effectuer une action (une déclaration ou un acte positif équivoque). Par conséquent, en protégeant un consentement libre, spécifique et explicite, le RGPD protège le choix de la personne concernée,

---

615 Voir par exemple L'HAIDON Olivier, PARASCHIV Corina, « Choix individuel et décision fondée sur l'expérience », *Revue économique*, 2009/4, vol. 60, pp. 949-978 ; VIDAILLET Bénédicte, D'ESTAINTOT Véronique, ABECASSIS Philippe (dir.), *La décision. Une approche pluridisciplinaire des processus de choix*, De Boek Supérieur, Collection Méthodes & Recherches, 2015, 304 pages.

616 CNRTL, « Décision », CNRTL.fr, *Étymologie*, disponible sur https://www.cnrtl.fr/etymologie/decision (consulté en décembre 2020).

617 CNRTL, « Choisir », CNRTL.fr, *Étymologie*, disponible sur https://www.cnrtl.fr/etymologie/decision (consulté en décembre 2020).

618 SCHALL Jeffrey D., « Neural Basis of Deciding, Choosing and Acting », Nature Review Neuroscience, 2001, 2, pp. 33-34.

619 *Idem*, p. 34.

620 *Ibidem*.

621 RGPD, 27 avril 2016, Article 4 (11).

en obligeant le responsable de traitement d'offrir de réelles alternatives (libre), qui pourront être identifiées (spécifiques) et anticipées (explicites) par la personne concernée.

295. Une fois la personne concernée informée sur le choix qui lui est offert, encore faut-il s'assurer que ce choix puisse être effectué librement. La notion de consentement libre est ainsi intimement liée à d'autres notions philosophico-juridiques telles que l'autonomie de la volonté ou encore le libre arbitre. Ces notions vont parfois se confronter au caractère protectionniste de la protection des droits de l'Homme, avec comme interrogation principale la question de savoir s'il faut protéger l'individu contre lui-même, et si oui, jusqu'à où cette protection peut se confronter au le libre arbitre de l'individu.

296. La jurisprudence de la Cour européenne des droits de l'Homme est à cet égard intéressante dans la mesure où elle montre une évolution dans la philosophie européenne de la protection des droits de l'Homme. La CEDH s'est en effet intéressée à la question de la transformation de l'illégal en légal par l'effet du consentement dans le domaine pénal. Confrontée à la question de la pénalisation des pratiques sadomasochistes, la Cour avait d'abord adopté une posture protectionniste lors de l'arrêt *Laskey, Jaggard et Brown c. Royaume-Uni*[622]. La question était de savoir si des actes pouvant relever de l'article 3 de la CEDH (l'interdiction de la torture et des traitements inhumains et dégradants[623]) devaient être sanctionnés lorsque la victime était consentante. Dans sa posture protectionniste, la Cour de Strasbourg avait alors considéré que l'État était libre de fixer un « niveau de dommage que la loi doit tolérer lorsque la victime est consentante »[624].

297. En 2005, la Cour opère un revirement de jurisprudence à l'occasion de son arrêt fondamental *K. A. et A. D. c. Belgique,* en affirmant que « le droit pénal ne peut, en principe, intervenir dans le domaine des pratiques sexuelles consenties qui relèvent du libre arbitre des individus »[625]. Ainsi, tout le raisonnement de la Cour s'inverse : si, dans l'arrêt *Laskey*, l'objectif de protection des individus contre les dommages corporels prévalait du consentement de l'individu, l'arrêt *K. A. et A. D.* érige le libre arbitre – et donc la capacité de consentir à des actes de violence à son égard – comme principe dont les exceptions doivent relever de la stricte nécessité et doivent, par conséquent, être justifiées par l'existence de « raisons particulièrement graves »[626]. Ainsi, comme le relève Michel Levinet, dans cette perspective, l'État « ne peut

[622] CEDH, 19 février 1997, *Laskey et autres c. Royaume-Uni*, req. 21627/93 ; 21628/93 ; 21974/93.
[623] Convention européenne de sauvegarde des droits de l'Homme, Article 3.
[624] CEDH, *Laskey et autres c. Royaume-Uni, op. cit.*, §44.
[625] CEDH, 17 février 2005, *K. A. et A. D. c. Belgique*, req. 42758/98 et 45558/99, §84.
[626] *Ibidem.*

intervenir que de manière tout à fait exceptionnelle face à ce type de pratiques, […] *a priori* son intervention est illégitime »[627]. De plus, l'affaire *K. A. et A. D.* a été l'occasion de confirmer que l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme protège l'autonomie personnelle en tant que composante du « droit à l'épanouissement personnel »[628], solution qui avait déjà été esquissée par la Cour lors de l'arrêt *Pretty c. Royaume-Uni*[629].

298. En matière de consentement en matière de droits de l'Homme, l'affaire *K. A. et A. D.* doit notamment son retentissement à la consécration du pouvoir transformateur du consentement de l'illégal au légal de faits qui, « examinés sur le terrain de l'article 3 [de la Conv. EDH], seraient, à n'en pas douter, qualifiés d'actes de torture »[630]. La Cour européenne des droits de l'Homme s'est certes refusée à examiner les faits sous le prisme de l'article 3, mais elle consacre en pratique, au prisme de l'article 8, l'exception de la victime consentante à propos du seul article de la Convention ne permettant aucune ingérence.

299. En matière de protection des données à caractère personnel, le pouvoir transformateur du consentement de l'illégal au légal est consacré par la consécration du consentement comme base légale pouvant fonder le traitement de données à caractère personnel. Pourtant, le consentement au traitement de ses données à caractère personnel n'a pas toujours été consacré. En France, le consentement en tant que base légale justifiant le traitement des données à caractère personnel n'apparaît que lors de la transposition de la directive 95/46/CE en 2004. Dans son rapport à l'Assemblée nationale sur le projet de loi de transposition de la directive, Gérard Gouzes envisage clairement le consentement comme une « disposition protectrice », au « caractère extrêmement restrictif »[631]. Dans la même lignée, le rapport au Sénat d'Alex Türk interprète le projet de loi comme posant « le principe selon lequel le consentement des personnes concernées par un traitement de données à caractère personnel est nécessaire »[632].

---

[627] FABRE-MAGNAN Muriel *et al.,* « Controverse sur l'autonomie personnelle et la liberté du consentement », *Droits*, 2008/2, n°48.

[628] « L'article 8 de la Convention protège le droit à l'épanouissement personnel, que ce soit sous la forme du développement personnel […] ou sous l'aspect de l'autonomie personnelle qui reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8 ». CEDH, 17 février 2005, *K. A. et A. D. c. Belgique, op. cit.,* §83.

[629] « Bien qu'il n'ait été établi dans aucune affaire antérieure que l'article 8 de la Convention comporte un droit à l'autodétermination en tant que tel, la Cour considère que la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8 ». CEDH, 29 avril 2002, *Pretty c. Royaume-Uni*, req. 2346/02.

[630]FABRE-MAGNAN Muriel *et al., op. cit.*.

[631] GOUZES Gérard, *op. cit.*.

[632] TÜRK Alex, *Rapport fait au nom de la commission des Lois constitutionnelles, de la législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant*

300. Le poids du consentement dans la protection des données à caractère personnel a entraîné la réflexion sur la qualité du consentement. En plus du caractère éclairé du consentement sus-étudié, le législateur a aussi eu à cœur de faire correspondre le consentement de la personne concernée à sa volonté : l'exercice du consentement doit ainsi inclure l'exercice d'un choix libre. Pour atteindre cet objectif, le législateur a, d'une part, isolé le consentement d'autres considérations pour permettre à la personne concernée d'exercer son consentement uniquement sur le traitement de ses données à caractère personnel (Chapitre 1) et, d'autre part, visibilisé le consentement en lui attribuant des limites spatio-temporelles (Chapitre 2).

la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Rapport au Sénat n°218, Annexe au procès-verbal de la séance du 19 mars 2003.

CHAPITRE 1 – UN CONSENTEMENT ISOLÉ DE CONTRAINTES EXTERNES À SON OBJET

301. En physique, l'isolation se définit comme le « fait de s'opposer au passage du courant électrique, de la chaleur ou des vibrations sonores »[633]. L'isolation est un procédé permettant de protéger un matériau ou un espace déterminé d'une menace extérieure pouvant l'affecter. En matière de données à caractère personnel, l'analogie se vérifie puisque le consentement va être isolé de considérations externes à celui-ci afin de s'opposer à l'influence de paramètres extérieurs au choix.

302. Lorsqu'il s'agit des choix opérés par la personne concernée face à un responsable de traitement, l'un des constats opérés est que la personne concernée se voit souvent offrir un choix « sur une base de à prendre ou à laisser »[634]. Dès lors, le consentement de la personne était invariablement lié au choix d'utiliser ou non un service ou de visiter un site internet donné. L'offre liant le consentement au traitement de ses données à caractère personnel à la possibilité de profiter d'un service ou de visiter un site internet a été une des raisons identifiées justifiant l'attitude des internautes ne lisant pas les politiques de confidentialités des sites qu'ils visitaient[635]. Ainsi, les personnes concernées ressentaient le sentiment de ne pas pouvoir exercer un réel choix sur le traitement de leurs données à caractère personnel, ce qui, par lassitude, entraînait un abandon du contrôle de leurs données.

303. Cette logique du tout-ou-rien s'additionnait à l'inexistence du pouvoir de négociation de la personne concernée sur le contenu de la politique de confidentialité et résultait en l'impossibilité d'exercer un consentement sur le traitement de ses données à caractère personnel *per se.* Le RGPD a ainsi corrigé cette faiblesse du consentement, d'abord en déconditionnant ce dernier d'autres considérations (Section 1), puis en interdisant l'utilisation du consentement dans le cadre d'une relation déséquilibrée entre le responsable de traitement et la personne concernée en défaveur de cette dernière (Section 2).

---

633 CNRTL, « Isolation », *CNRTL.fr,* Lexicographie, disponible sur https://www.cnrtl.fr/definition/isolation (consulté en février 2021).

634 « *on a take-it-or-leave-it basis* ». PLAUT Victoria. C., BARTLETT Robert P., « Blind consent? A social psychological investigation of non-readership of click-through agreements », *Law and Human Behavior*, 2012, 36(4), p. 298.

635 PLAUT Victoria. C., BARTLETT Robert P., *op. cit.*, pp. 293–311.

Section 1 – Le caractère non conditionné du consentement

304. Le RGPD propose une interprétation stricte de la notion de liberté du consentement, instituant une présomption de consentement non libre « si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement bien que celui-ci ne soit pas nécessaire à une telle exécution »[636]. Le consentement, déconditionné de l'ensemble des autres bases légales fondant le traitement des données à caractère personnel[637], est surtout renforcé par le fait d'être déconditionné de l'exécution d'un contrat, dont le consentement ne sera réputé libre que pour ce qui est nécessaire à une telle exécution.

305. Ainsi, le RGPD resserre la marge d'interprétation de la liberté du consentement en refusant que le consentement et le contrat ne puissent être « fusionnés et amalgamés »[638], ce qui renforce le contrôle de la personne concernée sur ses données à caractère personnel (§1). Une telle évolution est loin d'être anecdotique dans la mesure où elle permet d'évaluer la validité du consentement en fonction du contexte dans lequel le responsable de traitement en effectue la demande, engageant dès lors la responsabilité de ce dernier dans les modalités de collecte du consentement (§2).

§1 – Le principe de la distinction entre consentement contractuel et consentement RGPD

306. La distinction entre la base légale du contrat (le consentement contractuel) et le consentement au traitement de ses données à caractère personnel (le consentement RGPD) s'inscrit dans la volonté de renforcer la liberté du consentement de la personne concernée, et par extension, le contrôle qu'elle détient sur ses données à caractère personnel. Si les notions de consentement contractuel et de consentement RGPD s'accordent sur certaines conditions de validité, notamment le caractère libre et éclairé du consentement, la distinction opérée par le RGPD se révèle nécessaire. En effet, le caractère libre et éclairement du consentement contractuel et du consentement RGPD ne se confondent pas du fait qu'ils s'appliquent à des objets différents qui ne nécessitent pas le même degré de protection de l'émetteur du consentement (A). De plus, la nature particulière de l'économie des données à caractère

[636] RGPD, 27 avril 2016, considérant 43.
[637] Voir notamment HDPA, 30 juillet 2019, 26/2019; HDPA, *Summary of Hellenic DPA's Decision No 26/2019* disponible sur https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF
[638] EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/579*, *op. cit.*, p. 11.

personnel a rendu nécessaire la visibilisation des contrats d'adhésion *a priori* gratuits, ce qui protège la personne concernée dans son rôle de consommateur (B).

A. L'essence de la distinction entre consentement contractuel et consentement RGPD

307. Comprendre la distinction entre consentement contractuel et consentement RGPD est essentiel dans la mesure où cette approche est spécifique à la protection des données à caractère personnel et ne correspond pas parfaitement à la définition de droit commun de la notion de consentement. Or, le consentement est une notion couramment rencontrée dans les études de droit, quelle que soit la spécialité. Souvent envisagée dans le cadre contractuel[639], la notion de consentement est aussi analysée en dehors de ce cadre dans des domaines tels que la procédure pénale[640] ou encore le droit médical[641]. L'approche spécifique de la protection des données à caractère personnel réside dans la nécessité d'opérer une distinction entre le consentement contractuel au sens strict[642] , et le consentement RGPD.

308. La distinction entre consentement contractuel et consentement RGPD découle principalement de son article 6 qui liste les bases juridiques fondant la licéité des traitements de données à caractère personnel. Ainsi, le RGPD distingue la situation où « la personne concernée a consenti au traitement de ses données à caractère personne pour une ou plusieurs finalités spécifiques » (article 6(1)(a)) de la situation où « 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 celui-ci » (article 6(1)(b)). Cette distinction n'est pas source de redondance puisque ces deux conditions de licéité n'ont pas les mêmes conséquences juridiques. Par exemple, l'article 9 autorise les traitements de données sensibles fondés sur le consentement, mais pas ceux fondés sur le contrat[643].

309. Le RGPD inclut explicitement la distinction entre consentement contractuel et consentement RGPD à la démarche de renforcement du consentement libre. Le considérant 43 établit une présomption de consentement non libre si le consentement contractuel et le consentement RGPD sont confondus. De même, l'article 7, qui s'attache à définir les conditions applicables au consentement, alerte le responsable de traitement sur la nécessité de ne pas

---

639 v. STORCK Michel, *op. cit.*
640 v. AMBROISE-CASTÉROT Coralie, « Aveu », *Répertoire de droit pénal et de procédure pénale*, avril 2020.
641 v. MALLET ÉRIC, « Consentement à procréation », JCl. Notarial Formulaire, Fasc. 10, 01/03/2010 (dernière mise à jour : 08/10/2019).
642 Le consentement contractuel sera entendu comme le consentement correspondant exactement à l'objet du contrat. Le consentement à un traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution d'un contrat sera ainsi considéré comme un consentement extracontractuel.
643 RGPD, 27 avril 2016, Article 9 ; Groupe de travail « Article 29 », WP259 rév. 01, *op. cit.*, p. 22.

amalgamer les deux notions. L'article 7(4) dispose en effet qu'au « moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat ».

310. La définition du consentement proposée par l'article 4(11) du RGPD ne définit ainsi que le consentement RGPD. Ainsi, le consentement contractuel répond à la définition de droit commun proposé par le droit civil national quand le consentement RGPD se définit comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ». À titre de comparaison, en droit français, le consentement au contrat doit être donné de manière libre et éclairé, de telle manière qu'aucun vice du consentement – l'erreur, la violence et le dol – ne corrompe la volonté contractuelle des cocontractants[644]. La validité du consentement éclairé ne décrit pas la même réalité en matière de consentement contractuel et de consentement RGPD : la validité du consentement contractuel n'est évaluée qu'au regard de l'existence d'un vice du consentement ; la validité du consentement RGPD est évaluée au regard des éléments de définition inscrits à l'article 4(11) du RGPD.

311. Cette différence de régime juridique est justifiée par la différence de situation de l'émetteur du consentement. Dans le cadre du consentement contractuel, le traitement de données à caractère personnel est une condition nécessaire à l'exécution d'une obligation du responsable de traitement née du contrat conclu entre le responsable de traitement et la personne concernée. La personne concernée et le responsable de traitement sont alors réputés être sur un pied d'égalité en vertu de la présomption d'égalité des cocontractants[645]. Dans le cadre du consentement RGPD, le traitement de données à caractère personnel ne repose que sur l'accord de la personne concernée, voire son autorisation. Dès lors, le RGPD isole le consentement du bénéfice pouvant résulter de celui-ci, dans la mesure où ce dernier ne constitue pas une obligation du responsable de traitement. Au contraire, dans le cadre du consentement RGPD, le traitement de données à caractère personnel s'inscrit plutôt dans le cadre d'un avantage

[644] DISSAUX Nicolas, « Contrat : formation – Détermination des conditions », *Répertoire de droit civil*, avril 2017, actualisé en avril 2022, §126-127.
[645] L'égalité entre les cocontractants n'exclut cependant pas la possibilité pour le législateur de garantir cette égalité par des textes protégeant la partie la plus vulnérable. LAURIN Yves, « L'enjeu européen d'un bicentenaire », *D.*, 2004, p. 883.

conféré au responsable de traitement du fait de l'autorisation de traitement des données à caractère personnel. La distinction devient ainsi plus claire : le consentement contractuel est le consentement qui ne peut être isolé d'une obligation du responsable de traitement envers la personne concernée. Le premier relèvera du régime relatif au droit des contrats, le second du régime spécifique de la protection des données à caractère personnel.

312. Le besoin de distinguer le consentement contractuel et le consentement RGPD est le résultat d'une réflexion initiée dans le cadre du contentieux. Ainsi, la question s'était déjà posée sous l'égide de la directive 95/46/CE, notamment à propos de la nature d'une navigation internet. La distinction précédemment décrite avait par exemple été consacrée par la Cour d'appel de Paris qui avait jugé en 2012 que « le simple fait de se rendre sur un site internet afin de consulter celui-ci sans encore présenter une quelconque demande, telles une commande ou une réservation, ne saurait engager l'internaute dans des liens contractuels avec la société propriétaire du site »[646]. La réflexion sur les contours du contrat en matière de navigation internet, objets connectés et plus largement, de traitements de données à caractère personnel met en exergue la nécessité d'adapter la notion de consentement à la nature de l'objet du consentement.

313. Plus précisément, ces réflexions font naître la nécessité de s'intéresser plus précisément à la notion de consentement afin de saisir les enjeux convergents et divergents des consentements contractuel et extracontractuel. Présent dans le langage courant, le mot « consentement » présente des sens différents selon le point de vue intellectuel adopté. Dans le sens courant, le consentement signifie à la fois l'« action de consentir » et le « résultat de cette action »[647]. Cette définition a du sens puisque le juriste manipulera les deux notions dans un ordre chronologique, s'intéressant à l'action de consentir lorsqu'il évaluera la validité du consentement, puis au résultat de cette action lorsqu'il se penchera sur les conséquences de celui-ci. Cependant, le résultat dépendant entièrement de l'action, l'étude de l'action semble suffire à tracer les contours du consentement. Ainsi, il suffit de s'intéresser à l'action de consentir, c'est-à-dire à l'action de « se prononcer en faveur de l'accomplissement d'un projet,

[646] Cour d'appel de Paris, pôle 5, ch. 2, 23 mars 2012.
[647] « Consentement », *CNRTL.fr*, disponible sur https://www.cnrtl.fr/definition/consentement (consulté en juillet 2019).

d'un acte, etc. »[648] ou, plus étymologiquement, l'action d'« être d'accord avec »[649]. La définition est peu précise, mais pose les jalons d'un acte de volonté interne.

314. La définition philosophique permet d'apporter plus de précision en nuançant l'intensité de l'acte. En effet, « se prononcer en faveur » et « être d'accord avec » ne témoignent pas de la même force de volonté. Le consentement serait ainsi un « acte de volonté par lequel on décide ou même on déclare expressément qu'on ne s'oppose pas à une action déterminée dont l'initiative est prise par autrui »[650]. Une première divergence s'esquisse alors entre le consentement contractuel et le consentement RGPD. Si ce dernier semble correspondre à l'acception philosophique du consentement, le consentement contractuel, quant à lui, s'en éloigne. Cette divergence découle du bénéfice attaché au consentement : si le consentement RGPD « marque, dans l'ordre de la pensée comme dans celui de l'action, une nuance de réserve, ou du moins une tendance primitive à refuser »[651], c'est parce qu'il n'est pas attaché à une démarche contractuelle et ne fait pas intervenir spontanément l'appât d'un bénéfice pour la personne concernée. Cette dernière est chronologiquement d'abord confrontée au sacrifice de ses données à caractère personnel puis au bénéfice qui peut en résulter. Au contraire, lors du consentement contractuel, le consentement est intrinsèquement lié au bénéfice promis par le contrat : la personne concernée ne sacrifie ses données qu'en raison de la projection du bénéfice qu'il obtiendra du fait du contrat. Ainsi, le consentement contractuel correspond à la définition juridique classique du consentement, c'est-à-dire « dans la création d'un acte juridique, [l']acceptation par une partie de la proposition faite à l'autre »[652].

315. L'étude du consentement contractuel découle dès lors d'une logique contractuelle lorsque le consentement RGPD relève quant à lui d'une logique autonomiste. Il semble octroyer à la personne concernée un pouvoir plus important puisqu'elle réfléchit en priorité sous le prisme de son sacrifice et non de son bénéfice. Le pouvoir de la personne concernée sur la gestion de ses données à caractère personnel consiste en effet en la correspondance la plus exacte entre la manifestation de la volonté et le consentement donné. En effet, internet est un espace oligopolistique[653] : de ce fait, la personne concernée aurait pu être déresponsabilisée du

---

[648] « Consentir », *CNRTL.fr*, Lexicographie, disponible sur https://www.cnrtl.fr/definition/consentir (consulté en juillet 2019).
[649] Consentir provient du latin *consentire* qui signifie « être d'accord avec ». *Ibidem.*
[650] LALANDE André, *op. cit.*, p. 177.
[651] *Ibidem.*
[652] DEBARD Thierry, GUINCHARD Serge, *op. cit.*, p. 272.
[653] Pour une vision globale de la structure oligopolistique d'internet et de la dominance de la publicité sur cet espace, v. SMYRNAIOS Nikos, *Internet Oligopoly. The Corporate Takeover of Our Digital World*, Bingley,

fait du pouvoir trop important des acteurs privés[654]. Or, l'esprit du RGPD a été au contraire de rééquilibrer les pouvoirs de la personne concernée en protégeant son consentement, garantissant ainsi que ce dernier corresponde effectivement à la manifestation de volonté de la personne concernée afin de « garantir aux individus le contrôle de leurs données à caractère personnel »[655]. Cette interprétation est confirmée par l'explication proposée par le Groupe « Article 29 » quant aux enjeux de la distinction entre consentement contractuel et consentement au traitement des données à caractère personnel :

> « Dès lors que la législation sur la protection des données vise à protéger les droits fondamentaux, le contrôle d'un individu sur ses données à caractère personnel est considéré comme essentiel, et il semble évident que le consentement au traitement de données à caractère personnel non nécessaire ne peut être considéré comme une condition sine qua non de l'exécution d'un contrat ou de la fourniture d'un service »[656].

316. En explicitant le lien entre le consentement contractuel et le bénéfice lié à l'exécution du contrat, le RGPD autonomise le consentement produit de l'unique volonté de la personne concernée du consentement contractuel. Cette démarche a aussi permis de « visibiliser » les contrats nécessitant le traitement de données à caractère personnel, remédiant à l'invisibilisation de ces contrats du fait de leur apparente gratuité.

B. L'enjeu sous-jacent de « visibilisation » des contrats invisibles

317. La sortie du consentement de la logique contractuelle est aussi importante pour la protection des données à caractère personnel en raison de la présence importante de la « culture de la gratuité » sur internet. Cette culture est d'autant plus forte qu'elle est présente depuis la création du réseau, comme en témoigne l'idéologie des « pionniers » d'internet[657] dont

---

Emerald Publishing, 2018, 174 p. ; pour comprendre les effets de la structure oligopolistique d'internet sur le droit de la concurrence et l'exercice du droit à la vie privée par les personnes concernées, v. TAYLOR Curtis, LIAD Wagman, « Consumer Privacy in Oligopolistic Markets : Winners, Losers and Welfare », *International Journal of Industrial Organization*, vol. 34, mai 2014, pp. 80-84.

[654] L'importance du pouvoir des acteurs privés sur Internet a d'ailleurs poussé le ministre américain de la Justice à ouvrir « des investigations sur les pratiques anticoncurrentielles et quasi monopolistiques de certaines multinationales », visant, entre autres, à « déterminer si ces entreprises ont eu recours à des pratiques « ayant réduit la concurrence, empêché l'innovation ou affecté les consommateurs ». Le Monde, « Les géants du web sont-ils devenus trop puissants ? Les États-Unis ouvrent une enquête », *LeMonde.fr*, Économie, Vie en ligne, 23 juillet 2019, disponible sur https://www.lemonde.fr/economie/article/2019/07/23/ouverture-d-une-enquete-antitrust-sur-les-societes-high-tech_5492664_3234.html (consulté en juillet 2019).

[655] « Ensuring that individuals are in control of their personal data ». Commission européenne, *Impact Assessment*, SEC/2012/0072 final, *op. cit*. Bien que la notion de contrôle ne soit pas associée directement à la notion de consentement, le RGPD affirme tout de même que « les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant ». RGPD, 27 avril 2016, considérant 7.

[656] Groupe de travail « Article 29 », WP259 rév. 01, *op. cit.*, p. 9.

[657] PROULX Serge, GOLDENBERG Anne, « Internet et la culture de la gratuité », *Revue du MAUSS*, 2010/1 (n° 35), pp. 503-517, disponible sur https://www.cairn.info/revue-du-mauss-2010-1-page-503.htm.

l'expression la plus libertaire vient probablement de la déclaration d'indépendance du cyberespace, qui affirme :

> « Vos notions juridiques de propriété, d'expression, d'identité, de mouvement et de contexte ne s'appliquent pas à nous. Elles se fondent sur la matière. Ici, il n'y a pas de matière ».

Cette culture de la gratuité a conduit à « invisibiliser » les contrats présents sur Internet, ou du moins d'invisibiliser le caractère synallagmatique de ces contrats. Serge Proulx et Anne Goldenberg expliquent « l'ambivalence de la gratuité » par la définition commune associée à ce terme[658], associée à l'absence de contrepartie pécuniaire ou même l'absence de compensation. Ainsi, selon ces auteurs, « la gratuité rassemblerait trois dimensions constitutives : réalisé avec un sentiment de plaisir, sans recherche de contrepartie, ce qui est gratuit serait fait sans but déterminé, constituant une fin en soi ; ne cherchant à servir à rien »[659].

318. La gratuité pouvait ainsi invisibiliser le caractère synallagmatique des contrats puisque le contrat gratuit est par essence unilatéral. Cette vision contractuelle de la gratuité du contrat est bien inscrite dans le Code civil français dont l'article 1107 ne conçoit pas de contrat synallagmatique à titre gratuit « puisque celui qui procure un avantage à l'autre ne doit ni attendre une contrepartie ni recevoir une contrepartie »[660]. D'ailleurs, la nouvelle rédaction du Code civil ne laisse que peu de place aux contrats gratuits puisque désormais un contrat est qualifié d'onéreux à la fois sur le critère de la réception d'une contrepartie, mais aussi sur l'intention des parties de recevoir une contrepartie de l'autre[661]. Le caractère gratuit ne peut donc pas s'appliquer à l'ensemble des services gratuits sur internet, dans la mesure où la gratuité apparente de ces contrats est compensée par un avantage réciproque : le traitement de données à caractère personnel à des fins onéreuses. Ainsi, la gratuité des services sur internet semble invisibiliser le caractère synallagmatique de ces contrats. De plus, la nature d'internet favorisant les décisions immédiates, le contrat devient lui-même invisible puisque, comme le remarquent Gérard Haas, Stéphane Astier et Paul Benelli, « les conditions générales – de vente ou de service – constituent en effet les contrats les plus souvent conclus à l'heure du numérique et pourtant les plus invisibles »[662].

319. D'ailleurs, de récents développements jurisprudentiels ont confirmé l'absence de caractère gratuit des services offerts en contrepartie de données à caractère personnel. À ce

---

[658] *Ibidem.*
[659] *Ibidem.*
[660] LATINA Mathias, « Contrats : généralités Civ. », *Répertoire de droit civil*, Paris, Dalloz, §216.
[661] LATINA Mathias, *op. cit.*, §215.
[662] HAAS Gérard *et al.*, « Le nouveau droit des obligations à l'épreuve de la pratique – L'impact de la réforme du droit des obligations sur les contrats « digitaux », *Revues des Juristes de Sciences Po*, n°13, mars 2017, p. 7.

propos, le raisonnement du Tribunal de Grande Instance (TGI) de Paris est intéressant : prenant acte de la fourniture du service Google+ à titre gratuit, la Cour remarque cependant que la société Google commercialise les données fournies par l'utilisateur lors de l'inscription et de l'utilisation du service[663]. Le tribunal conclut :

> « Ainsi donc, un service sans paiement monétaire ne pouvant être pour autant considéré comme un service entièrement gratuit, la fourniture de données collectées gratuitement puis exploitées et valorisées par la société GOOGLE doit s'analyser en un « avantage » au sens de l'article 1107 du Code civil, qui constitue la contrepartie de celui qu'elle procure à un utilisateur, de sorte que le contrat conclu avec la société GOOGLE est un contrat à titre onéreux et non un contrat à titre gratuit »[664].

320. Ainsi, la gratuité affichée des services proposés par Google correspondait uniquement à l'absence de contrepartie pécuniaire. L'adage désormais célèbre « si c'est gratuit, c'est que vous êtes le produit » traduit l'absence de gratuité des services proposés sur internet par les exploitants de données à caractère personnel en raison de la valorisation de ces données. La distinction entre consentement contractuel et consentement au traitement de ses données à caractère personnel proposée par le RGPD permet d'effacer la notion de gratuité au profit du degré d'autorisation de ses données à caractère personnel qu'il souhaite accorder au responsable de traitement. La personne concernée, peu apte à distinguer les traitements essentiels à l'exécution d'un contrat des traitements à caractère personnel au bénéfice du responsable de traitement, se voit dès lors protégée par la visibilisation des contrats synallagmatiques.

321. La personne concernée est d'autant plus protégée qu'il revient au responsable de traitement de distinguer les traitements essentiels à l'exécution du contrat des traitements qui relèvent du consentement RGPD. Cette distinction peut s'avérer compliquée économiquement, tant le *business model* des acteurs du numérique s'est appuyé sur les revenus publicitaires pour proposer des contenus gratuits. Il n'est dès lors pas étonnant de constater que les acteurs dont les revenus dépendent des revenus publicitaires s'évertuent à limiter la présomption de non-liberté du consentement lorsque le traitement des données à caractère personnel n'est pas essentiel à l'exécution du contrat. L'exemple des *cookie walls* est particulièrement parlant. Face aux lignes directrices de la CNIL relatives aux cookies qui excluait la possibilité de consentir librement à un *cookie paywall*[665], une action avait été portée en justice afin d'en demander

---

[663] TGI Paris, 12 février 2019, Union Fédérale des consommateurs – Que choisir c. Société Google Inc., 14/07224.
[664] *Ibidem.*
[665] Un cookie paywall conditionne l'accès à un site internet soit au consentement à l'installation de cookies sur le terminal de la personne concernée, soit au paiement d'une somme d'argent souvent sous la forme d'un abonnement mensuel.

l'annulation par l'association des agences-conseils en communication, la fédération du e-commerce et de la vente à distance, le groupement des éditeurs de contenus et services en ligne, l'Interactive Advertising Bureau France, la Mobile Marketing Association France, le syndicat communication directe de la data à la logistique, le syndicat des régies internet, l'union des entreprises de conseil et d'achat médiat et l'union des marques[666]. Ces acteurs ont en commun de se reposer sur un modèle économique qui se fondait sur la gratuité perçue du contenu par la personne concernée en échange de l'installation de cookies sur son terminal. Malgré une décision en défaveur d'une interprétation stricte de protection de l'autonomie de la personne concernée, le *cookie paywall* a le mérite de visibiliser l'aspect économique de l'installation de *cookies* sur le terminal de la personne concernée.

322. Désormais, la personne concernée peut distinguer les traitements de données à caractère personnel nécessaire à la fourniture du service qu'il souhaite utiliser des traitements de données à caractère personnel accessoires, permettant à l'exploitant du service d'obtenir d'autres avantages (exploitation commerciale des données, suivi des visites d'un site internet, etc.). La responsabilité de cette distinction revient alors au responsable de traitement.

§2 – Les modalités de la distinction entre consentement contractuel et consentement au traitement de ses données à caractère personnel

323. La distinction entre le consentement contractuel et le consentement au traitement de ses données à caractère personnel a des conséquences sur les obligations du responsable de traitement. Selon le Comité européen à la protection des données, le législateur a fait le choix de souligner « la conditionnalité en tant que présomption de l'absence de liberté de consentement »[667], créant ainsi une forte incitation pour le responsable de traitement de déconditionnaliser le consentement (A). En pratique, cette distinction s'articule autour de la notion de préjudice du refus de consentir (B).

A. L'incitation forte de déconditionnaliser le consentement

324. L'interprétation restrictive des situations relevant de la base juridique contractuelle a pour conséquence logique l'élargissement des situations dans lesquelles le responsable de traitement a pour obligation de déconditionnaliser le consentement.

---

[666] CE, 10e et 9e ch. réunies, 19 juin 2020, *Association des agences-conseil et a.*, n°434684.
[667] EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, op. cit.*, p. 12.

325. Si l'existence de deux bases juridiques différentes pour le consentement contractuel et le consentement RGPD était déjà présente dans le projet initial de la Commission[668], l'obligation de séparer le consentement au traitement de ses données du consentement contractuel n'est apparue qu'au cours des négociations tripartites. Dès son premier rapport sur le projet de règlement, la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) a ajouté que « l'exécution d'un contrat ou la délivrance d'un service ne devait pas être conditionnée au consentement sur un traitement de données qui n'est pas nécessaire à l'exécution du contrat ou à la délivrance du service »[669]. L'obligation de distinguer le consentement contractuel du consentement au traitement de ses données non nécessaire à l'exécution du contrat ou à la fourniture d'un service apparaît ainsi dès la première lecture du Parlement[670] et du Conseil[671]. De plus, en raison du « principe général de responsabilité omniprésent dans le RGPD »[672], la charge de la preuve du déconditionnement du consentement revient au responsable de traitement. Les modalités de la distinction entre le consentement contractuel et le consentement RGPD revêtent donc un enjeu majeur pour le responsable du traitement dans la mesure où il lui revient d'apprécier si le consentement est conditionné ou non à l'exécution d'un contrat, appréciation qui pourra faire l'objet d'un recours par la personne concernée ou encore évaluée par une autorité de contrôle ou un tribunal[673].

326. La distinction opérée par le responsable de traitement conditionne la validité du consentement de la personne concernée. En effet, l'article 7(4) du RGPD requiert du responsable de traitement de « tenir le plus grand compte de la question de savoir […] si

---

668 Commission européenne, COM(2012) 11 final, *op. cit.*, Article 6.

669 « *the execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service* » [traduction libre]. Parlement européen, Commission LIBE, *Committee report tabled for plenary, 1st reading/single reading*, A7-0402/2013.

670 « *The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1), point (b)* ». Parlement européen, *European Parliament legislative resolution of 12 March 2014 on 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 the free movement of such data (General Data Protection Regulation*), Procédure legislative ordinaire : première lecture, Strasbourg, 12 mars 2014, COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

671 « When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract ». Conseil des ministres, *Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*), adoptee le 8 avril 2016, ST 5419 2016 REV 1.

672 EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, op. cit.*, p. 13.

673 Voir Groupe de travail « Article 29 », *Avis 06/2014 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,* adopté le 9 avril 2014, WP 217, p. 15.

l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement » lors de sa collecte. L'EDPB, dans son interprétation de l'article 7 (4) du RGPD, confirme bien que le responsable de traitement doit, dans la majorité des cas, déconditionnaliser le consentement est à la charge du responsable de traitement :

> « La locution « tenir le plus grand compte » utilisée à l'article 7, paragraphe 4, suggère que le responsable du traitement doit être particulièrement prudent lorsqu'un contrat (qui pourrait inclure la fourniture d'un service) intègre une sollicitation de consentement au traitement de données à caractère personnel »[674].

L'interprétation de l'EDPB s'inscrit dans la réflexion qu'elle avait déjà initiée au sein du G29 lors de son avis sur la notion d'intérêt légitime en 2014. Ainsi, depuis la directive 95/46/CE, le G29 propose une interprétation stricte de la base contractuelle en tant que fondement du traitement des données à caractère personnel. Le G29 s'opposait ainsi à une pratique courante des responsables de traitement qui consistait à inclure des traitements de données à caractère personnel au sein de contrats longs et difficiles à lire, afin d'annihiler le pouvoir de négociation de la personne concernée. Le G29 précisait ainsi :

> « La disposition doit être interprétée de façon restrictive et ne couvre pas les situations dans lesquelles le traitement n'est pas véritablement *nécessaire* à l'exécution d'un contrat, mais plutôt imposé unilatéralement à la personne concernée par le responsable du traitement. Le fait qu'un certain traitement de données soit couvert par un contrat ne signifie pas automatiquement que le traitement soit nécessaire à son exécution […]. Même si ces activités de traitement sont expressément mentionnées en petits caractères dans le contrat, elles n'en deviennent pas pour autant « nécessaires » à l'exécution de ce dernier »[675].

327. L'interprétation restrictive de la base contractuelle impose ainsi au responsable de traitement de « toujours se demander dans quelle mesure les données sont « nécessaires » à l'exécution d'un contrat ou seulement recueillies à l'occasion de celui-ci »[676] : la première hypothèse relève du régime de l'article 7 (b) du RGPD, la base contractuelle, tandis que la seconde relève du régime de l'article 7 (a) du RGPD, c'est-à-dire du consentement. D'ailleurs, l'interprétation est si restrictive que la base juridique contractuelle ne s'appliquera ni aux « diverses actions déclenchées par le non-respect du contrat ni quelque autre incident dans son exécution » : ces dernières situations relèveront de la base juridique de l'intérêt légitime[677]. Quant aux relations précontractuelles, celles-ci relèveront de la base juridique du contrat

---

[674] EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, op. cit.,* p. 12.
[675] Groupe de travail « Article 29 », WP 259 rev. 01, *op. cit.*, p. 9.
[676] DEBET Anne, « Le consentement dans le RGPD : rôle et définition », Étude, *Communication Commerce électronique*, n°4, avril 2018, dossier 9, disponible sur Lexis 360.
[677] Groupe de travail « Article 29 », WP 260 rev. 01, *op. cit.*, p. 19.

uniquement s'il s'agit de démarches « accomplies à la demande de la personne concernée, plutôt qu'à l'initiative du responsable du traitement ou d'un tiers »[678]. Dès lors, l'interprétation restrictive de la base légale contractuelle réserve le consentement au contrat à ce qui est nécessaire à l'objet du contrat (généralement, la fourniture d'un bien ou d'un service) plutôt qu'au contenu du contrat.

328. La frontière entre les bases légales du consentement et du contrat a fait l'objet d'un contentieux au niveau des juridictions françaises, en particulier dans le domaine du e-commerce. La CNIL a ainsi considéré l'inadéquation de la base légale du contrat à la conservation de certaines données précédemment considérées par le responsable de traitement comme relevant de sa relation précontractuelle avec la personne concernée. En effet, par sa délibération du 6 septembre 2018[679], la CNIL a précisé que la conservation du numéro de carte bancaire d'un client pour faciliter un éventuel paiement ultérieur (la procédure d'achat « en un clic ») relevait non pas de la base juridique de l'exécution d'un contrat, mais de celle du consentement[680]. La CNIL justifie sa position en affirmant qu'un tel traitement « va au-delà de l'exécution du contrat conclu », ce traitement constituant « une option indépendante de l'acte initial ayant conduit à la collecte des données bancaires »[681]. L'autorité de contrôle a toutefois consacré une exception : le cas où la personne concernée a souscrit un abonnement donnant accès à des prestations additionnelles, dans la mesure où un tel fait « peut traduire l'intention du client de s'inscrire dans une relation commerciale régulière »[682].

329. Cette recommandation reprend la jurisprudence antérieure de la CNIL qui avait eu l'occasion de se prononcer à deux reprises sur la question. En 2012, l'autorité de contrôle française a condamné la pratique de la société Fnac Direct consistant à conserver les coordonnées bancaires des clients à la suite d'un achat en vue de faciliter les achats ultérieurs sur les fondements de l'exécution d'un contrat et de l'intérêt légitime[683]. D'une part, la CNIL avait refusé le fondement contractuel parce que la finalité de la conservation des coordonnées bancaires allait au-delà de l'exécution du contrat de vente initial, la conclusion d'achats ultérieurs éventuels étant tout à fait indépendante de la vente initiale[684]. D'autre part, la CNIL

---

[678] Voir Groupe de travail « Article 29 », WP 260 rev. 01, *op. cit.*, p. 20.
[679] CNIL, 6 septembre 2018, Délibération n°2018-303 portant adoption d'une recommandation concernant le traitement de données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance et abrogeant la délibération n°2017-222 du 20 juillet 2017.
[680] *Idem*, §2.5.
[681] *Ibidem.*
[682] *Ibidem.*
[683] CNIL, 19 juillet 2012, Délibération de la formation restreinte n°2012-214 portant avertissement à l'encontre de la société X.
[684] *Ibidem.*

avait rejeté le fondement de l'intérêt légitime. Si l'autorité administrative a reconnu que la société pouvait légitimement invoquer comme intérêt légitime l'intérêt commercial visant à « faciliter la réalisation d'un ou de plusieurs paiements successifs dans la durée »[685], elle a cependant considéré que la balance entre les intérêts poursuivis par la société et ceux des personnes concernées ne permet pas la conservation des données bancaires. En effet, en raison de la « sensibilité toute particulière » des coordonnées bancaires, leur conservation « doit être entourée de garanties renforcées »[686]. La CNIL avait alors laissé entendre que la demande de consentement était l'une des garanties renforcées obligatoires en matière de conservation des données bancaires[687].

330. La recommandation de la CNIL a été contestée devant le Conseil d'État par la société Cdiscount[688]. La société contestait l'interprétation de la CNIL en ce qu'elle réservait la base légale contractuelle aux seules conservations de données bancaires dans le cadre d'une souscription à un abonnement donnant accès à des prestations additionnelles. [689] En l'espèce, la société Cdiscount souhaitait l'autorisation de « la conservation des numéros de cartes bancaires pour les clients non abonnés, mais dont la récurrence des achats laisse supposer qu'ils peuvent raisonnablement s'attendre à ce que leurs données bancaires soient conservées pour simplifier leurs achats ultérieurs »[690]. La société Cdiscount avait précédemment notamment été mise en demeure en 2016 en raison d'un manquement à l'obligation de recueillir le consentement des personnes à la conservation de leurs coordonnées bancaires[691]. La CNIL avait alors conclu que l'intérêt légitime de la société ne pouvait prévaloir sur les intérêts des personnes concernées. D'une part, la légitimité même de l'intérêt de la société avait été remise en question par la CNIL qui affirmait alors que les achats postérieurs « ne sont qu'hypothétiques et conduisent à conserver des données bancaires au-delà du délai nécessaire à la finalité initiale de leur collecte, à savoir un achat en ligne »[692]. D'autre part, un tel intérêt ne pouvait prévaloir sur l'intérêt des personnes concernées à « renforcer leur contrôle » sur leurs informations bancaires, étant donné les risques importants que font courir les traitements de ces données à la personne concernée[693].

---

[685] *Ibidem.*
[686] *Ibidem.*
[687] *Ibidem.*
[688] CE, 10e et 9e ch. réunies, 10 décembre 2020, n°429571.
[689] *Ibidem*.
[690] *Idem*, n°429571, §2.
[691] CNIL, 26 septembre 2016, *Décision n°2016-083 mettant en demeure la société X.*
[692] *Ibidem.*
[693] CNIL, 26 septembre 2016, *Décision n°2016-083 mettant en demeure la société X.*

331. Dans son arrêt du 10 décembre 2020, le Conseil d'État a eu à se prononcer à la fois sur l'adéquation de la base juridique de l'exécution du contrat et sur l'adéquation de la base juridique de l'intérêt légitime. La base juridique de l'exécution contractuelle sera rapidement rejetée puisque le Conseil d'État se contentera de rappeler que « s'agissant de l'exécution d'un contrat auquel la personne concernée est partie, la conservation du numéro de carte bancaire ne saurait se justifier une fois ce contrat exécuté »[694]. Ainsi, la conservation du numéro de carte de paiement en vue d'achats postérieurs éventuels se dissocie sans difficulté de l'achat initial, même récurrent.

En ce qui concerne l'intérêt légitime, le Conseil d'État rejette la possibilité de fonder la conservation des numéros de carte bancaire pour deux raisons. Premièrement, tout comme la CNIL, la juridiction administrative considère que l'intérêt légitime commercial du responsable de traitement « ne saurait prévaloir sur l'intérêt des clients de protéger ces données, compte tenu de la sensibilité de ces informations bancaires et des préjudices susceptibles de résulter pour eux de leur captation et d'une utilisation détournée ». Si le Conseil d'État justifie comme la CNIL, l'absence de prévalence de l'intérêt commercial de facilitation des achats ultérieurs sur l'intérêt des personnes concernées à protéger des données présentant un caractère sensible – au sens de données présentant un risque de préjudice important et non au sens de l'article 9 du RGPD –, le Conseil d'État ne qualifie pas le consentement de « garantie renforcée »[695]. Deuxièmement, le Conseil d'État vérifie la concordance entre la réalité du traitement et les attentes raisonnables de la personne concernée, vérification suggérée à la fois par le considérant 47 du RGPD et par le G29 depuis son avis 06/2014 sur la notion d'intérêt légitime[696]. En l'espèce, le critère des attentes raisonnables de la personne concernée n'était pas rempli puisque le Conseil d'État constate que « de nombreux clients qui utilisent des sites de commerce en ligne en vue de réaliser des achats ponctuels ne peuvent raisonnablement s'attendre à ce que les entreprises concernées conservent de telles données sans leur consentement »[697].

332. Cependant, l'approche du Conseil d'État « implique une appréciation au cas par cas »[698], ce qui est cohérent avec son approche prohibant la CNIL de déduire du règlement une « interdiction générale et absolue »[699]. Ainsi, si la base juridique de l'exécution du contrat est

---

[694] CE, n°429571, *op. cit.*, §8.
[695] *Ibidem*, §9.
[696] Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 3.
[697] CE, n°429571, *op. cit.*, §9.
[698] BELKACEM Nacima, « Bases légales (RGPD) des traitements portant sur la conservation des numéros de cartes bancaires dans le secteur de la vente de biens ou la fourniture de services à distance », *Communication Commerce électronique*, n°3, mars 2021, comm. 24.
[699] CE, 10e et 9e ch. réunies, 19 juin 2020, *Association des agences-conseil et a.*, n°434684.

définitivement exclue de la conservation des données bancaires en vue d'achats futurs, l'intérêt légitime doit faire l'objet d'une analyse *in concreto* mettant en balance les intérêts du responsable de traitement et les intérêts de la personne concernée. Le Conseil d'État s'assure en effet de ne pas interpréter le RGPD au-delà de la présomption de consentement non libre posée par le considérant 43 du règlement, et s'interdit ainsi d'y voir une interdiction générale de conditionnalité du consentement à l'exécution du contrat. Dans cette démarche de prudence, il vérifiera la conditionnalité du consentement à l'égard de l'exécution du contrat (et des intérêts légitimes résultant de l'exécution du contrat), puis effectuera une interprétation casuistique de la liberté du consentement en prenant en compte le fait qu'il soit conditionné à l'exécution du contrat.

333. Cette analyse casuistique est effectuée en analysant de manière précise la liberté du consentement au regard du service concerné. À cet égard, le déconditionnement du consentement au traitement à caractère personnel de l'exécution d'un contrat doit être évalué au niveau du service offert par le responsable de traitement et non au niveau de l'ensemble du marché. Ainsi, le Comité européen à la protection des données précise que :

> « le consentement ne peut pas être considéré comme donné librement si un responsable du traitement avance qu'il existe un choix entre son service comprenant le consentement à l'utilisation de données à caractère personnel à des fins complémentaires et un service équivalent proposé par un autre responsable du traitement. Dans un tel cas, la liberté de choix dépendrait de ce que d'autres acteurs du marché font et du point et du point de savoir de si la personne concernée trouve les services de l'autre responsable du traitement réellement équivalents »[700].

334. La doctrine de la CNIL a également rejeté la possibilité d'évaluer la nécessité à l'exécution d'un contrat du point de vue du modèle économique du responsable de traitement. En 2016, La CNIL a condamné la société Facebook Inc., qui, en l'espèce, fondait le traitement des données à caractère personnel des adhérents à son réseau social à des fins de publicité ciblée sur la base juridique de l'exécution du contrat, arguant que « la combinaison des données à des fins de publicité est nécessaire à l'exécution contractuelle, et plus particulièrement à l'offre de services gratuits aux utilisateurs »[701]. L'argument n'a pas convaincu la formation restreinte de la CNIL qui, bien que précisant qu'elle ne s'opposait ni au modèle économique du réseau ni à la possibilité de recourir à la publicité ciblée, a toutefois conclu que « la combinaison des données des utilisateurs à des fins de ciblage publicitaire ne correspond ni à l'objet principal du

[700] EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, op. cit.*, p. 13.
[701] CNIL Délibération de la formation restreinte SAN-2017-006 du 27 avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés X et Y

contrat ni aux attentes raisonnables des utilisateurs quant à l'exécution de la convention conclue lors de l'inscription au service »[702]. Ainsi, le caractère nécessaire de la publicité ciblée pour le modèle économique du réseau social est inopérant à la qualification de nécessaire à l'exécution du contrat.

La nécessité à l'exécution du contrat ne s'évalue dès lors que du point de vue de l'objet du contrat et des attentes raisonnables de la personne concernée. En l'espèce, Anne Debet relève avec raison que « la nécessité contractuelle n'est en fait examinée que du côté de la prestation fournie à l'internaute (l'accès à un réseau social) et jamais du côté de celle que l'internaute fournit en contrepartie »[703]. La même solution est envisagée par le Groupe de travail « Article 29 » dans ses lignes directrices sur le consentement[704]. Cette solution constitue une évolution dans la position des autorités de contrôle. En 2008, le Groupe de travail « Article 29 » avait en effet affirmé que les moteurs de recherche pouvaient fonder les traitements aux fins de publicité comportementale sur la base contractuelle[705] et « la CNIL n'avait pas jugé nécessaire de soulever la question, dans son rapport de 2009 sur la publicité en ligne »[706]. Cette évolution est concomitante aux réflexions relatives à la liberté du consentement de l'individu face aux modèles économiques propres à la société numérique. Ainsi, le modèle économique fondé sur la publicité ciblée n'est pas rejeté, mais la publicité ciblée obligatoire à la fourniture d'un bien ou service est interdite au nom du consentement libre de la personne concernée.

335. Il résulte des indications et décisions de la CNIL, du Conseil d'État, de l'EDPB et du G29 que le traitement de données à caractère personnel non nécessaire à l'exécution du contrat ne peut pas relever de la base juridique du contrat, et relève souvent de celle du consentement RGPD. L'interprétation stricte de la notion de nécessaire à l'exécution du contrat limite

---

[702] *Ibidem.*

[703] DEBET Anne, « Réseaux sociaux – Facebook condamné à une sanction pécuniaire de 150 000 euros par la CNIL », *Communication Commerce électronique*, juillet 2019,°7-8, comm. 67.

[704] À propos d'une application mobile d'éditions de photos, le Groupe de travail « Article 29 » affirme que « ni la géolocalisation, ni la publicité comportementale en ligne ne sont nécessaires à la fourniture de services d'édition de photos et toutes deux dépassent de ce fait la fourniture du service de base proposé ». Groupe de travail « Article 29 », *Lignes directrices sur le consentement au sens du règlement 2016/679*, *op. cit.*, p. 6.

[705] « les fournisseurs de moteurs de recherche qui souhaitent proposer de la publicité personnalisée afin d'accroître leurs recettes peuvent trouver une raison au traitement légitime de certaines données à caractère personnel à l'article 7 (a) de la directive (consentement) ou à l'article 7 (b) de la directive (exécution d'un contrat), mais il est difficile de trouver une raison légitime à cette pratique pour les utilisateurs qui ne se sont pas spécifiquement inscrits en prenant connaissance de certaines informations sur la finalité du traitement ». Groupe de travail « Article 29 », *Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche*, adopté le 4 avril 2008, WP 148 p. 20.

[706] DEBET Anne, *op. cit.*, dossier 9. En effet, la CNIL se contente à renvoyer le lecteur vers l'Avis 1/2008 du Groupe de travail « Article 29 » sur les aspects de la protection des données liés aux moteurs de recherche. Voir PEYRAT Bernard, « La publicité ciblée en ligne », *Communication présentée en séance plénière*, CNIL, 5 février 2009, p. 29.

substantiellement la possibilité de se fonder sur la base légale du contrat, dans la mesure où la nécessité est évaluée uniquement du point de vue de l'objet du contrat – généralement, la fourniture d'un bien ou d'un service –, et que la base légale du contrat ne s'applique aux mesures contractuelles que sous certaines conditions restrictives. Une telle interprétation renforce le caractère libre du consentement de la personne concernée, qui ne se voit pas obligée de consentir à un traitement de données à caractère personnel pour obtenir la fourniture d'un bien ou d'un service indépendant à ce traitement. Cette interprétation stricte du contrat s'inscrit dans le principe de la « véritable liberté de »[707] promue par le RGPD permettant à la personne concernée de consentir ou de refuser de consentir au traitement de données à caractère personnel « sans subir de préjudice »[708].

B. La notion de préjudice comme objet de discordes doctrinales

336. L'article 7 du RGPD sur les conditions applicables au consentement n'envisage la liberté du consentement que par rapport à son éventuel conditionnement avec l'exécution d'un contrat[709]. L'utilisation des termes « entre autres » indique cependant que d'autres paramètres doivent être pris en compte lors de l'évaluation de la liberté de consentement de la personne concernée. Un élément essentiel d'interprétation de la liberté du consentement de la personne concernée est en effet délivré par le considérant 42, qui énonce le principe selon lequel

> « Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée de dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice ».

337. La liberté du consentement va donc être évaluée par la présence ou non d'un préjudice pour la personne concernée en cas de refus de consentement au traitement de ses données à caractère personnel. Ce préjudice peut être, entre autres, constitué par l'engendrement de frais pour la personne concernée, par un désavantage évident pour ceux qui retirent leur consentement, par l'amoindrissement de la qualité du service ou par « la tromperie, l'intimidation, la coercition ou toute conséquence négative importante »[710]. Par exemple, un responsable de traitement qui fait dépendre l'accès d'un bâtiment au traitement des données à

[707] RGPD, 27 avril 2016, considérant 42.
[708] *Ibidem.*
[709] RGPD, 27 avril 2016, article 7(4).
[710] Groupe de travail « Article 29 », WP 259 rev. 01, pp. 14-15.

caractère personnel de la personne concernée souhaitant y accéder, comme la prise de sa température, constitue un préjudice en défaveur de la personne concernée[711].

338. *A contrario*, dans le cas où le couplage du consentement est attaché à un « incitant »[712], et non à la fourniture d'un service en particulier, le consentement pourrait être considéré comme libre. Le G29 donne l'exemple de réductions générales offertes aux personnes concernées dont la collecte de données sur leurs préférences permet à l'enseigne les émettant d'adapter l'offre aux préférences de la personne concernée, sur la base de son consentement[713]. Dans ce cas de figure, si le retrait du consentement n'entraîne que la perte de l'incitant (la personne concernée recevra toujours des réductions, mais non personnalisées) alors il n'y a pas de préjudice et le consentement peut être évalué comme ayant été librement donné. En revanche, les polices d'assurance de *pay as you drive*, modulant le prix de la prime d'assurance à un suivi et une évaluation de la conduite à l'aide d'un boîtier connecté ne peuvent pas se fonder sur le consentement puisque cette base légale ne permettrait pas au responsable de « « maintenir la licéité » tout au long du cycle de vie du traitement »[714]. Le couplage entre le traitement de données à caractère personnel et la fourniture de service relève donc de l'article 6(1)(b) du RGPD, soit l'exécution d'un contrat auquel la personne concernée est partie[715].

339. L'absence de définition de la notion de préjudice par le législateur européen a engendré un point de discorde quant à son interprétation parmi les juristes spécialisés en protection des données à caractère personnel. La définition juridique est en effet très large puisqu'elle se confond avec la notion de « dommage […] subi par une personne par le fait d'un tiers »[716]. Dès lors, ni la définition juridique ni le RGPD ne permettent de déterminer le référentiel d'évaluation du préjudice de la personne concernée en matière de refus ou retrait du consentement au traitement de ses données à caractère personnel. Le silence de la CJUE, dont une interprétation de la notion de préjudice avait été attendue lors de son arrêt *Planet 49*, a par ailleurs privé le droit européen de la protection des données à caractère personnel d'une interprétation unifiée de la notion de préjudice. En effet, si l'arrêt *Planet 49* confirme

---

[711] APD, « Prise de température dans le cadre de la lutte contre le Covid-19 », mis à jour le 4 février 2021, disponible sur https://www.autoriteprotectiondonnees.be/citoyen/themes/covid-19/prise-de-temperature (consulté en décembre 2021).
[712] Groupe de travail « Article 29 », WP 259 rev. 01, p. 15.
[713] *Ibidem.*
[714] PERRAY Romain, « Données à caractère personnel. – Bases juridiques applicables aux traitements de données à caractère personnel. Traitement reposant sur le consentement préalable de la personne concernée. Dispositions générales », *JurisClasseur Communication*, Fasc. 932-71, 7 décembre 2020, §114.
[715] CNIL, « Véhicules connectés et données personnelles », *Pack de conformité*, octobre 2017, p. 24.
[716] GUINCHARD Serge, DEBARD Thierry, *op. cit.*, p. 807.

l'application du RGPD au consentement à l'installation des cookies[717], elle ne règle pas pour autant la question de savoir si la pratique des *cookie walls* et *cookie paywalls* constitue une pratique autorisée au regard du RGPD[718].

340. L'exemple du consentement aux cookies constitue alors un point de discorde entre autorités de protection, juridictions et législateur. La CNIL, l'autorité de contrôle néerlandaise, le Contrôleur européen de protection des données et le Comité européen de protection des données ont proposé une interprétation stricte du RGPD, considérant qu'un *cookie wall* est constitutif d'un préjudice du fait du refus ou du retrait de consentement[719]. Ce courant est suivi par une partie de la doctrine qui s'appuie sur l'opinion publique plutôt hostile aux *cookie walls,* les avis précités des autorités de contrôle, ou encore l'incompatibilité des *cookie walls* avec la définition du consentement proposée par le RGPD[720].

341. Le Conseil d'État récuse cette position en 2020, considérant qu'en affirmant que « la validité du consentement est soumise à la condition que la personne concernée ne subisse pas d'inconvénient majeur en cas d'absence ou de retrait de son consentement, un tel inconvénient majeur pouvant consister, selon elle, dans l'impossibilité d'accéder à un site internet, en raison de la pratique des « *cookie walls* », la CNIL a excédé ses pouvoirs « en déduisant une telle interdiction de la seule exigence d'un consentement libre »[721]. Le raisonnement du Conseil d'État apparaît *a priori* décevant tant il déplace le débat de la définition du préjudice à l'étendue des pouvoirs de l'autorité de contrôle. Les conclusions du rapporteur public M. Alexandre Lallet[722] sont pourtant révélatrices du débat sur la nature du préjudice et sur la place accordée au considérant 42 dans l'évaluation de la liberté du consentement.

---

[717] CJUE, Gde ch ., 1er octobre 2019, Planet49 GmbH, C-673/17.

[718] On voit d'ailleurs de plus en plus fleurir ces modèles économiques, par exemple sur www.jeuxvideo.com,

[719] EDPB, Déclaration du comité européen de la protection des données sur la révision de la directive ePrivacy et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques, p. 4 ; CNIL, Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs), Article 2 ; AP, « Hoe legt de AP de juridische normen rond cookiewalls uit? », disponible sur https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_ap_cookiewalls.pdf (consulté en décembre 2021).

[720] ZUIDERVEEN BORGESIUS Frederik J. *et al.*, « Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation », *European Data Protection Law Review,* Volume 3, Issue 3, pp. 353-368; COTON Fanny, RUELLE Victoria, « The end of third-party cookies: nothing but smoke and mirrors if the RTB winner takes it all? », *in* JACQUEMIN Hervé (dir.), *Time to Reshape the Digital Society*, Bruxelles, Larcier, 2021, pp. 214-217 ; GÉROT Mathilde, « Le renforcement des droits des personnes sur leurs données à caractère personnel – Aspects de droit interne », *Revue de droit international d'Assas,* 2019, n°2.

[721] CE, n°434684, *op. cit.*,§10.

[722] LALLET Alexandre, Conclusions, n°434684, *op. cit.*.

342. La difficulté d'interprétation des règles relatives aux *cookie walls* provient d'abord de la nécessaire articulation entre la directive *e-privacy* et le RGPD. L'interprétation des dispositions de la directive à la lumière du règlement ne semble cependant pas poser de réelles difficultés puisque d'une part, elle résulte de la volonté du législateur[723], et d'autre part, elle ne semble pas poser de difficulté pour les avocats généraux à la CJUE[724]. Les complications résultent plutôt de l'articulation entre d'une part le considérant 25 de la directive *e-privacy* et le considérant 42 du RGPD. En effet, le considérant 25 de la directive s'oppose clairement à une prohibition générale et absolue des *cookie walls*, disposant que :

> « L'accès au contenu d'un site spécifique peut être, toutefois, subordonné au fait d'accepter, en pleine connaissance de cause, l'installation d'un témoin de connexion ou d'un dispositif analogue, si celui-ci est utilisé à des fins légitimes ».

Les conclusions du rapporteur Alexandre Lallet visent à démontrer l'importance de ce considérant dans le régime juridique relatif aux cookies. L'étude des travaux préparatoires à la transposition en droit national de la directive révèle en effet le rejet, en 2004, par le législateur français, de l'interdiction générale et absolue des *cookie walls*, notamment à travers le rapport présenté devant le Sénat par Alex Türk[725]. De plus, la modification de la directive *e-privacy* par la directive 2009/136/CE n'a pas procédé à la suppression du considérant 25 de la directive *e-privacy* alors même qu'elle y insère des dispositions relatives à la liberté du consentement en matière de dépôt de cookies[726]. Cependant, cette interprétation est discutable : si le rapporteur public démontre avec succès que le législateur n'a pas voulu en 2004 et 2009 interdire de manière générale et absolue les *cookie walls*, il peut être considéré qu'en matière d'interprétation de la directive à la lumière du Règlement le curseur doive se placer plutôt au niveau de la volonté du législateur en 2016. Ainsi, seul l'argument selon lequel le Parlement européen n'a pas *in fine* réussi à voter l'interdiction générale et absolue des *cookie walls* proposée lors des négociations relatives au RGPD est le seul élément pouvant relever de la volonté du législateur[727].

---

[723] RGPD, 27 avril 2016, considérant 173.
[724] Conclusions de l'avocat général M. Marciej SZPUNAR, *Planet 49 GmbH*, présentées le 21 mars 2019, C-673/17.
[725] TÜRK Alex, *op. cit.*, Annexe au procès-verbal de la séance du 19 mars 2003 ; LALLET Alexandre, Conclusions, n°434684, *op. cit*.
[726] 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 ; LALLET Alexandre, Conclusions, n°434684, *op. cit.*
[727] LALLET Alexandre, Conclusions, n°434684, *op. cit*.

343. Il est également regrettable que certaines discussions sur les *cookie walls* se focalisent sur le considérant 25 de la directive *e- privacy* et l'article 7(4) du RGPD, sans s'intéresser à la notion de préjudice de la personne concernée pourtant insérée au considérant 42 du RGPD[728]. Pourtant, l'interprétation de la notion de préjudice est justement le point de discorde qui requiert du législateur, des autorités de contrôle et des juridictions de procéder à l'articulation entre la directive *e-privacy* et le RGPD. Ainsi, les débats qui se focalisent sur la question des *cookie walls* et *cookie paywalls* sont centralisés autour de l'évaluation du préjudice et du référentiel d'évaluation choisi. Dans ce cadre, comme le remarque justement Alexandre Lallet dans ses conclusions, l'évaluation du préjudice peut soit s'évaluer du point de vue de l'accès de la personne concernée à un site en particulier, ou du point de vue de l'accès de la personne concernée à un service[729]. La première solution relève de la solution proposée par la CNIL et le Comité européen de protection des données. La seconde, adoptée par le Conseil d'État, révèle les ambitions européennes actuelles en matière de régulation des *cookie walls.*

344. Les conclusions du rapporteur public Alexandre Lallet et la solution proposée par la Cour de cassation italienne proposent toutes deux d'évaluer la liberté de la personne concernée au regard du caractère indispensable et non fongible du site concerné[730]. Ainsi, la liberté de consentir de la personne concernée n'est plus évaluée au regard de sa capacité à accéder à un site internet particulier, mais au regard de « la nature du besoin que l'utilisateur cherche à satisfaire et, surtout, dans l'existence, la disponibilité et l'accessibilité d'alternatives raisonnables permettant d'atteindre un résultat équivalent »[731]. Ainsi, la Cour de cassation italienne rejette l'existence d'un préjudice lorsque le *cookie wall* est mis en place sur un service d'information générale dès lors que les informations sont facilement à obtenir par d'autres moyens (qui peuvent être payants, ou provenir de publications imprimées) : l'existence d'alternatives au service recherché exclut le caractère préjudiciable du *cookie wall*[732].

345. L'existence d'alternatives peut être évaluée au regard de la concurrence dans son ensemble. Dans l'ensemble des situations, l'utilisation de *cookie walls* serait strictement

[728] La Cour de cassation italienne ne se réfère à aucun moment au considérant 42 du RGPD. Cour de cassation italienne, Cass Civ., 17278/2018, *op. cit.*. On regrettera également l'occasion manquée de l'Avocat général Marciej Szpunar de préciser une interprétation harmonisée de la notion de préjudice au sens du considérant 42 du RGPD. Conclusions de l'avocat général M. Marciej SZPUNAR, *op. cit.*.
[729] LALLET Alexandre, Conclusions, n°434684, *op. cit*.
[730] LALLET Alexandre, Conclusions, n°434684, *op. cit*.; Cour de cassation italienne, Cass Civ., 17278/2018, *op. cit.*
[731] LALLET Alexandre, Conclusions, n°434684, *op. cit*.
[732] Cour de cassation italienne, Cass Civ., 17278/2018, *op. cit.*

interdite s'agissant de services administratifs et plus largement des services du secteur public[733] en raison du « monopole de l'administration et [de] l'absence d'équivalence ergonomique du déplacement au « guichet » »[734]. Le G29 prend à ce titre l'exemple de la législation suédoise qui considère que la personne concernée refusant de donner son consentement doit choisir un prestataire de service différent, sauf pour « certains services relevant du secteur public, sur lesquels l'utilisateur pourrait être considéré comme ayant peu de possibilités, voire comme n'ayant pas d'autre possibilité que de recourir à ce service »[735]. Dans ce cadre, le préjudice de la personne concernée se confond avec le préjudice du consommateur sur le marché : le préjudice de la personne concernée naît de l'absence d'alternative au service recherché, du fait de la nature administrative du service, de la nature novatrice ou rare du service ou de la position dominante d'un acteur sur le marché[736].

346. L'existence d'alternatives peut être également évaluée au regard du fournisseur de service. Le G29 avait proposé en 2013 une interprétation du considérant 25 du terme « contenu d'un site spécifique », qui appliquait le terme « spécifique » non pas au site, mais au contenu[737]. Dès lors, le G29 considère dans son document de travail que « les sites web ne devraient pas subordonner « l'accès général » au site à l'acceptation, par l'utilisateur, de tous les cookies et qu'ils ne peuvent limiter que certains contenus si l'utilisateur ne donne pas son consentement pour les cookies »[738]. L'accès au site internet se conçoit alors à la manière d'un jeu *free-to-play* où la fonctionnalité principale n'est pas subordonnée à l'acceptation des cookies, mais les services complémentaires le sont. Le mandat de négociation de l'Union européenne s'inscrit cependant dans une ligne légèrement différente[739]. L'existence d'alternative s'évalue également au niveau du fournisseur de service, mais également au niveau global du site internet. Le couplage entre l'accès à un site internet et le dépôt de cookies est alors permis à la condition

[733] Groupe de travail « Article 19 », *Document de travail 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies*, adopté le 2 octobre 2013, 1676/13/FR, WP 208, p. 7.
[734] LALLET Alexandre, Conclusions, n°434684, *op. cit*.
[735] Groupe de travail « Article 19 », WP 208, nbp 9.
[736] Le mandat de négociation adopté par le Conseil de l'Union européenne dispose en son considérant 20aaaa que le couplage entre le dépôt de cookies pour des finalités additionnelles et l'accès au site est accepté en l'absence d'un déséquilibre manifeste entre la personne concernée et le fournisseur de service, du fait de la nature administrative du service, de la présence de peu ou pas d'alternatives au service ou en cas de position dominante du fournisseur de service. Conseil de l'Union européenne, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications – Mandate for negociations with EP*, Bruxelles, 10 février 2021, 2017/0003(COD), considérant 20 aaaa.
[737] Groupe de travail « Article 19 », WP 208, p. 6.
[738] *Ibidem.*
[739] Conseil de l'Union européenne, 2017/0003(COD), *op. cit.*, considérant 20 aaaa.

que le fournisseur de service propose une alternative à ce couplage[740]. Il s'agirait d'une légitimation du modèle *cookies-or-pay* déjà présente en nombre sur le marché numérique, l'alternative au couplage cookies-services se matérialisant dans le paiement d'une somme d'argent déterminée.

Figure 3 - Banières de paywall d'Allociné et Marmiton

347. Ainsi, la pratique des *cookie walls* n'est pas encadrée de manière satisfaisante puisque sa légalité même est contestée et relève d'une jurisprudence l'autorisant sur une base casuistique et non-générale. L'absence de cadre juridique autour de la question des *cookie walls* est dénoncée par la CNIL et l'EDPB, qui ont tous deux appelé le législateur à préciser le cadre juridique des *cookie paywalls* dans le futur règlement *e-privacy*[741]. Pour pallier l'absence de

[740] *Ibidem.*
[741] EDPB, *Déclaration du comité européen de la protection des données sur la révision de la directive ePrivacy et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques*, 25 mai 2018 ; EDPB, *Response to the letter of 13 July 2020 from News Media Europe and others regarding cookie* walls,

cadre juridique précis, la CNIL a commencé un travail de définition des critères d'évaluation des *cookie walls* vis-à-vis de la liberté de consentement de la personne concernée « dans l'attente d'une législation ou d'un positionnement de la Cour de justice de l'Union européenne »[742]. La solution proposée par la CNIL reprend le raisonnement du rapporteur public M. Alexandre Lallet afin de proposer une interprétation du préjudice au regard du caractère indispensable et non fongible du contenu ou service concerné. Ainsi, la CNIL interprète la notion de préjudice comme invitant les éditeurs de site internet à proposer aux personnes concernées, en plus d'un accès au site conditionné au consentement, une alternative réelle et équitable permettant à celles-ci d'accéder au contenu ou au service proposé par le site internet sans avoir à consentir au traitement de leurs données à caractère personnel[743]. L'alternative doit alors remplir deux conditions cumulatives : être réelle et équitable.

348. La réalité de l'alternative s'évalue en fonction du besoin de la personne concernée, en fonction de l'état du marché au moment de la demande de consentement. Ainsi, si l'éditeur du site internet a l'exclusivité sur les contenus ou services proposés (ce qui est souvent le cas des services administratifs par exemple), ou s'il n'existe « que peu ou pas d'alternative au service », la CNIL considère qu'il n'y a pas de véritable choix dans la mesure où la personne concernée sera contrainte d'accepter le traitement de ses données à caractère personnel pour satisfaire ce besoin[744].

349. L'adéquation de l'alternative, quant à elle, s'évalue en fonction de son caractère raisonnable. Les *cookies walls* se sont avant tout développés pour des raisons économiques, les éditeurs compensant le caractère « gratuit » de leur contenu et service par l'exploitation payante des données à caractère personnel des personnes concernées. Cependant, la CNIL avertit que « cette contrepartie monétaire ne doit toutefois pas être de nature à priver les internautes d'un véritable choix »[745]. L'interprétation du caractère raisonnable de la contrepartie monétaire sera alors importante pour déterminer la liberté de consentement de la personne concernée lorsqu'elle est confrontée à un *cookie paywall*. Deux interprétations peuvent ainsi concourir : celle de la valeur raisonnable perçue par la personne concernée et celle de la valeur raisonnable compensatoire.

---

19 novembre 2020 ; CNIL, « Cookie walls : la CNIL publie des premiers critères d'évaluation », *CNIL.fr*, 16 mai 2022, disponible sur https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookie-walls/la-cnil-publie-des-premiers-criteres-devaluation (consulté en juin 2022).

[742] CNIL, « Cookie walls … », *op. cit.*

[743] *Ibidem.*

[744] *Ibidem.*

[745] *Ibidem.*

Dans la première interprétation, le caractère raisonnable de la contrepartie monétaire est évalué vis-à-vis de la valeur perçue par la personne concernée, ce qui peut relever d'un faisceau d'indices incluant par exemple la valeur facturée pour le même service non numérique, la valeur du contenu sur le marché, le caractère indispensable ou non du service, ou encore le caractère habituellement gratuit ou non du service. Dans ce cadre, l'interprétation est éminemment casuistique, ce qui permet d'évaluer le caractère raisonnable de la contrepartie monétaire du point de vue de la personne concernée. Cependant, une telle interprétation fait peser sur la responsabilité du responsable de traitement de déterminer une valeur qu'il estime raisonnable pour la personne concernée. Ainsi, la valeur perçue par la personne concernée permet de se placer du côté de l'évaluation de la valeur par la personne concernée, mais la mise en œuvre d'un tel principe est susceptible d'être source de difficulté d'une part pour les responsables de traitement devant évaluer cette valeur, et d'autre part pour les personnes concernées si les responsables de traitement ont un pouvoir important sur le marché dans lequel s'inscrit le service concerné.

Dans la seconde interprétation, le caractère raisonnable de la contrepartie monétaire est évalué vis-à-vis de la valeur réelle de l'exploitation des données à caractère personnel pour financer le service. Dans ce cadre, le responsable de traitement présente deux offres réellement équivalentes : une offre impliquant des traitements de données à caractère personnel afin de rémunérer le service concerné, et une offre pécuniaire, évaluée comme une compensation de la perte de gain du fait du refus de traitement des données à caractère personnel. Cette interprétation se rapprocherait de l'approche adoptée par l'État de Californie dans le CCPA, dont la section 1798.125 (b) (1) indique :

> « A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data.»[746]

L'avantage d'une telle interprétation est qu'elle apporte une sécurité juridique satisfaisante aux responsables de traitement dans la mise en œuvre du principe de la contrepartie monétaire raisonnable. Il est vrai qu'une telle interprétation impliquerait probablement l'existence d'un contentieux quant au calcul de la valeur réelle de l'exploitation des données à caractère personnel pour un service. Néanmoins, le caractère raisonnable de la contrepartie monétaire

[746] *California Consumer Privacy Act*, Section 1798.125 (b) (1).

résulterait d'une méthodologie mathématique, plus certaine que l'interprétation par faisceau d'indices. Le caractère libre du consentement serait dès lors évalué en fonction de la « perte » de valeur estimée pour le responsable de traitement du fait de proposer un service gratuit. La pratique paraît *a priori* satisfaisante, même si l'on peut regretter l'inversement de la logique du RGPD selon laquelle les traitements sont interdits, sauf si une base légale les autorise. Dans la logique de la contrepartie compensatrice d'une perte de valeur du responsable de traitement, l'interprétation de la liberté du consentement de la personne concernée relève plus d'une logique de marché que d'une logique de droits fondamentaux, puisque le responsable de traitement dispose ainsi d'une sorte de « droit d'exploitation » des données à caractère personnel lors de l'utilisation de son service, dont le refus emporte compensation.

Ainsi, l'interprétation de la liberté de consentement du *cookie paywall* semble être une solution efficace permettant de respecter au mieux la liberté de consentement de la personne concernée dans une logique de marché désormais confirmée par le Conseil d'État. Cette solution pourrait à terme s'imposer puisque la consécration du *cookie paywall* semble être engagée dans les négociations relatives au Règlement *ePrivacy*[747].

350. En conclusion, la conditionnalité du consentement fait l'objet d'interprétations divergentes en matière de dépôt de cookies sur le terminal d'un utilisateur. Avancée du règlement en matière de protection du consentement, le découplage du consentement aux données à caractère personnel rencontre des difficultés à s'adapter au modèle économique fondé sur le ciblage publicitaire[748]. La notion de préjudice au refus ou au retrait du consentement est alors centrale pour procéder à l'évaluation de la liberté du consentement. Notamment, la question du *cookie paywall* met à mal la notion de préjudice au refus de consentement, dont l'interprétation n'est pas évaluée au niveau du service concerné, mais semble être évaluée au niveau de l'ensemble du marché.

351. Conclusion de section. – Le couplage du consentement aux cookies à l'accès d'un site internet est, dans ce cadre, un cas particulier qui relève à la fois du RGPD et de la directive *ePrivacy*, cette dernière s'interprétant comme une *lex specialis* qui crée un régime spécifique au dépôt de cookies sur le terminal de l'utilisateur. Il reste cependant au législateur européen de déterminer, à l'issue du dialogue tripartite, l'ampleur de ce régime afin de l'adapter d'une part au modèle économique des fournisseurs de service tout en veillant à ne pas créer un régime neutralisant la liberté de consentement garanti par le RGPD. La liberté de consentement semble

[747] Conseil de l'Union européenne, 2017/0003(COD), *op. cit.,* considérant 20 aaaa
[748] Ce point sera développé en Partie II.

ainsi être évaluée du point de vue du pouvoir économique de la personne concernée sur le marché du service auquel elle souhaite accéder. Le législateur européen a également consacré dans le RGPD l'évaluation du pouvoir de la personne concernée vis-à-vis du responsable de traitement en dehors de rapports strictement économiques, s'intéressant à l'existence ou non d'une hiérarchie entre la personne concernée et le responsable de traitement.

Section 2 – Le déséquilibre manifeste entre la personne concernée et le responsable de traitement

352. La notion de déséquilibre manifeste n'était pas présente dans la directive 95/46/CE. Elle fait son apparition dans le RGPD, au considérant 43 qui dispose :

> « Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable de traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière ».

353. Seule occurrence de la notion de déséquilibre manifeste, le considérant 43 ne définit pas cette notion autrement que par la référence à des « circonstances » et à la particularité de la situation. Définir les contours de la notion de déséquilibre manifeste semble à ce titre nécessaire à l'analyse de la protection de la liberté de consentement de la personne concernée (§1). En pratique, la notion de déséquilibre manifeste risque de se rencontrer lorsqu'il existe un lien de subordination entre la personne concernée et le responsable de traitement (§2).

§1 – La notion de déséquilibre manifeste

354. La notion de déséquilibre manifeste semble résulter d'une analyse de la relation entre la personne concernée et le responsable de traitement, qui prend en compte la nature de la relation, le contexte dans lequel s'établit la relation ainsi que toutes « circonstances ». Le RGPD ne définit cependant pas la nature du déséquilibre entre la personne concernée et le responsable de traitement (A). De plus, la notion de manifeste est indicatrice du degré de contrôle du RGPD sur la liberté de consentement, en ce qui concerne la relation entre le responsable de traitement et la personne concernée (B).

A. Le déséquilibre

355. La seule occurrence du terme « déséquilibre » dans le lexique des termes juridiques concerne la notion de déséquilibre significatif rencontrée en droit civil et en droit des affaires[749]. Le déséquilibre significatif se définit comme une « situation de disproportion sensible entre les droits et obligations des parties à un contrat en défaveur de la partie faible »[750]. Pourtant, la protection du plus vulnérable est parfois décrite comme « une des missions traditionnelles du

[749] DEBARD Thierry, GUINCHARD Serge, *op. cit.*, p. 361.
[750] *Ibidem.*

droit »[751]. L'identification de la vulnérabilité du sujet du droit dans l'exercice de ses droits est symptomatique de « l'ordre public de protection » vers lequel tend le droit[752]. La prise en compte de la vulnérabilité dans le droit dépasse le « postulat volontariste » selon lequel les contractants sont égaux en droits et en devoirs pour prendre en considération l'inégalité des cocontractants et le déséquilibre structurel du contrat[753].

356. Le déséquilibre se conçoit dès lors dans le cadre d'une relation entre le fort et le faible, dans la perspective souvent citée de Henri Lacordaire :

> « Entre le fort et le faible, entre le riche et le pauvre, entre le maître et le serviteur, c'est la liberté qui opprime, et la loi qui affranchit »[754]

La citation fort connue pointe du doigt la question de la nature du déséquilibre : il peut être déséquilibre de pouvoir, entre le fort et le faible, déséquilibre de richesses entre le riche et le pauvre, déséquilibre de statut entre le maître et le serviteur. Les vulnérabilités sont donc diverses et variées, et il convient de déterminer avec plus de précision quelles vulnérabilités sont envisagées dans le RGPD.

357. Les formes de vulnérabilités sont généralement catégorisées en fonction de leur origine, séparant la « vulnérabilité subjective » (aussi rencontrée sous les appellations de « vulnérabilité personnelle » ou de « vulnérabilité endogène ») de la « vulnérabilité objective » (aussi rencontrée sous les appellations de « vulnérabilité du fait des choses » ou « vulnérabilité réelle »)[755]. La vulnérabilité subjective est inhérente au sujet de droit : la vulnérabilité a pour origine la maladie ou la constitution physique (handicaps, enfants, personnes âgées, etc.)[756]. La vulnérabilité objective est quant à elle inhérente à la situation dans laquelle se trouve le sujet de

---

[751] DUPICHOT Philippe, GRIMALDI Cyril, VERNIÈRES Christophe, « Avant-propos », *in* Association Henri Capitant, *Vulnérabilité*, Bruxelles, Bruylant, 2020, p. 5.

[752] LE GAC-PECH Sophie, « De la personne vulnérable au contractant vulnérable », *in* LE GAC-PECH Sophie, *Les droits du contractant vulnérable*, Bruxelles, Larcier, 2016, p. 11 ; REVET Thierry, « Rapport de synthèse », *in* Association Henri Capitant, *Vulnérabilité*, Bruxelles, Bruylant, 2020, p. 11.

[753] LE GAC-PECH Sophie, *Les droits du contractant vulnérable*, Bruxelles, Larcier, 2016, p. 9.

[754] LACORDAIRE Henri, *Conférences de Notre-Dame de Paris*, Tome III, 52e conférence, *Du double travail de l'homme*, 16 avril 1848.

[755] AUBRY Hélène, « L'apport du droit de la consommation » *in* LE GAC-PECH Sophie, *Les droits du contractant vulnérable*, Bruxelles, Larcier, 2016, p. 33 ; POULLET Yves, « Numérique, droit et vulnérabilités », *in* MATHIEU Géraldine *et al.* (dir.), *L'étranger, la veuve et l'orphelin. Le droit protège-t-il les plus faibles ?*, Liber Amicorum Jacques Fierens, Bruxelles, Larcier, 2020, p. 420 ; CANNARSA Michel, « Chapitre 4 – Les consommateurs aussi ont des sentiments ! Quels effets sur leur patrimoine ? », *in* VIOLET Franck, *Personne et Patrimoine*, Bruxelles, Bruylant, 2015, p. 109.

[756] AUBRY Hélène, « L'apport du droit de la consommation » *in* LE GAC-PECH Sophie, *Les droits du contractant vulnérable*, Bruxelles, Larcier, 2016, p. 33 ; POULLET Yves, « Numérique, droit et vulnérabilités », *in* MATHIEU Géraldine *et al.* (dir.), *L'étranger, la veuve et l'orphelin. Le droit protège-t-il les plus faibles ?*,Liber Amicorum Jacques Fierens, Bruxelles, Larcier, 2020, p. 420 ; CANNARSA Michel, « Chapitre 4 – Les consommateurs aussi ont des sentiments ! Quels effets sur leur patrimoine ? », *in* VIOLET Franck, *Personne et Patrimoine*, Bruxelles, Bruylant, 2015, p. 109.

droit, qu'il s'agisse d'une situation de pouvoir, d'une situation économique ou d'une situation sociale[757]. Si la vulnérabilité subjective est traditionnellement envisagée sous l'angle du droit des personnes[758], la vulnérabilité objective est souvent rencontrée en droit des contrats, en droit de la consommation, ou encore en droit des étrangers.

358. En ce qui concerne le RGPD, la vulnérabilité subjective fait l'objet d'une autre protection, plus spécifique à la capacité de la personne concernée, qui se traduit dans le RGPD par un régime spécifique dédiée aux enfants, une interprétation particulière des dispositions relatives à certains principes dédiée aux personnes vulnérables (sus-étudiées) et au régime juridique national relatif aux personnes en situation de vulnérabilité (en matière de consentement, il s'agira des dispositions relatives aux sauvegardes de justices, curatelles et tutelles par exemple). De plus, la référence aux « circonstances de cette situation particulière » semble confirmer que le « déséquilibre manifeste » doit s'évaluer en matière de vulnérabilité objective, dans le cadre de la relation entre le responsable de traitement et la personne concernée. La lecture des contributions du G29 permet de préciser ce qui pourrait être évalué au compte de la vulnérabilité objective : le G29 discute des conséquences du déséquilibre économique entre les grandes entreprises et les consommateurs[759], du déséquilibre de pouvoir et de choix entre l'employé et l'employeur[760], de la faiblesse relationnelle du salarié, de l'étudiant ou encore du patient[761]. Le champ d'application du déséquilibre manifeste semble relever donc de deux catégories : le déséquilibre des relations économiques et le déséquilibre du fait d'un lien de subordination (autorité publique-citoyen, employeur-employé, étudiant-système éducatif, patient-médecin).

359. En ce qui concerne la protection de la réalité du consentement, le droit de l'Union européenne se focalise principalement sur la relation entre l'employeur et l'employé. Il est en effet établi depuis l'arrêt *Pfieffer* que « le travailleur doit être considéré comme la partie faible au contrat de travail, de sorte qu'il est nécessaire d'empêcher que l'employeur dispose de la faculté de circonvenir la volonté du cocontractant ou de lui imposer une restriction de ses droits »[762]. Le RGPD est également sensible au déséquilibre de la relation entre le citoyen et l'autorité publique. Le consentement du citoyen sera alors protégé des conséquences que

---

[757] AUBRY Hélène, *op. cit.* p. 420 ; CANNARSA Michel, *op. cit.*, p. 109.
[758] AUBRY Hélène, *op. cit.*, p. 33
[759] Groupe de travail « Article 29 », *Opinion 03/2013 on purpose limitation*, adopté le 2 avril 2013, 00569/13/EN, WP 203, p. 49.
[760] Groupe de travail « Article 29 », WP 203, *op. cit.*, p. 56
[761] Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 45.
[762] CJCE, Gde Ch., 5 octobre 2004, *Pfieiffer e.a.*, C-397/01 à C-403/01, §82 ; CJUE, 5e ch., 17 mars 2021, *Academia de Studii Economice din Bucureşti*, C-585/19.

l'autorité publique peut lui attacher, à l'image des différents avis sur la compatibilité de la base légale du consentement avec les applications de suivi dans le cadre de la lutte contre le Covid-19[763]. Le déséquilibre peut dès lors résulter soit d'un déséquilibre économique, soit d'un déséquilibre de pouvoir.

360. La protection de la partie faible dans le cadre d'un déséquilibre économique est largement prise en compte par le droit. Par exemple, le devoir de sollicitude de la Commission a été interprété de manière favorable à la femme enceinte dont l'accouchement est imminent, en raison de sa vulnérabilité économique[764]. De même, les dispositions relatives aux relations entre le voyageur et le service de transport sont évaluées en faveur du voyageur[765], expressément désigné comme la partie faible du contrat par le législateur européen[766]. L'interprétation *in* favorem de la partie faible va également se retrouver dans des situations où la vulnérabilité de la personne concernée résulte du déséquilibre de ses connaissances avec son interlocuteur, par exemple l'accédant face au professionnel[767]. En matière de droit de la consommation, l'interprétation en faveur du consommateur est d'ailleurs consacrée et systématisée au sein du Code civil[768]. Le législateur va parfois plus loin en consacrant législativement un régime plus favorable à la partie faible, par exemple en l'assujettissant à des règles de compétence juridictionnelles plus favorables à ses intérêts.[769]

361. Par conséquent, il semble que le consentement soit *a priori* protégé lorsqu'il existe un lien de subordination ou de pouvoir entre la partie faible et la partie forte. La vulnérabilité économique fera quant à elle l'objet d'une protection *a posteriori* de l'équilibre de l'accord entre la partie faible et la partie forte. Dès lors, le consentement libre au sein du RGPD semble

---

[763] CNIL, Délibération n°2020-046 du 24 avril 2020, *op. cit.* ; EDPB, 21 avril 2020, *op. cit.*

[764] Tribunal de la fonction publique de l'Union européenne, 19 juillet 2016, Oprena / Commission européenne, F-67/15.

[765] V. par exemple CJUE, 4e ch., 2 septembre 2021, *Irish Ferries Ltd*, C-570/19, §51 ; CJUE, 5e ch., 7 novembre 2019, *Kanyeba*, C-349/18 à C-351/18, §50 ; CJUE, 1er ch., 22 novembre 2012, *Westbahn Management GmH*, C-136/11, §34.

[766] Règlement (CE) 1371/2007 du Parlement européen et du Conseil du 23 octobre 2007 sur les droits et obligations des voyageurs ferroviaires, considérant 3 ; Règlement (UE) 1177/2010 du Parlement européen et du Conseil du 24 novembre 2010 concernant les droits des passagers voyageant par mer ou par voie de navigation intérieure et modifiant le règlement (CE) n°2006/2004, considérant 2 ;

[767] BROCHE Christophe, « La protection de la partie faible à l'épreuve des contrats de construction », *in* CLARET Hélène *et al.* (dir.), *Les rapports entre le droit de la protection des consommateurs et les autres branches du droit*, Presses Universitaire Savoie Mont-Blanc, 2020, disponible sur hal.

[768] LAGADEC Alain, *De l'interprétation des clauses contractuelles à la qualification du* contrat, Thèse pour obtenir le grade de docteur en droit, soutenue le 12 avril 2017, Université de Toulon, p. 74

[769] Règlement (UE) 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, considérant (18) ; CJUE, 3e ch., 20 mai 2021, *CNP*, C-913/19 ; Règlement (CE) 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I), considérant (23) ; CJUE, 1er ch., 15 juillet 2021, *DG, EH*, C-152/10 et C-218/20.

être protégé du déséquilibre résultant de l'existence d'un lien de subordination ou de pouvoir entre la personne concernée et le responsable de traitement. Cependant, le seul lien de subordination ou de pouvoir n'est pas suffisant à exclure la liberté du consentement de la personne concernée : encore faut-il démontrer que le déséquilibre entre la personne concernée et le responsable de traitement est manifeste.

B. La notion de « manifeste »

362. Le terme « manifeste » se définit par ce « qui est de toute évidence », « qui ne peut être contesté dans sa nature ou son existence »[770]. Si le manifeste se définit par l'évidence, son saisissement par le juriste semble pourtant relever d'un caractère « mystique » tant il se sent confronté face à « une notion insaisissable »[771]. La thèse de Clovis Callet nous apporte cependant des éléments de précision de la notion : plus que l'évidence, le caractère manifeste s'entend parfois de la démonstration facile (plus précisément, de ce qui apparaît certain « au terme d'un examen simple et relativement rapide »)[772], et le plus souvent, de la certitude, autrement dit, l'inexistence d'un doute[773]. Appliqué à la protection des données à caractère personnel telle qu'établie par le RGPD, le caractère manifeste du déséquilibre permet de préciser le sens et la portée du considérant 43 du RGPD.

363. Premièrement, le déséquilibre manifeste signifie que le déséquilibre ne doit pas être révélé par un examen minutieux de l'autorité de contrôle et du juge. L'hypothèse la plus simple est celle de l'existence d'un lien de subordination ou de pouvoir, dont la certitude découle du droit (contrat de travail, prérogatives de puissance publique, etc.). Dans ce cadre, le juge peut *a priori* choisir « entre le blanc et le noir, le oui et le non »[774], le droit lui fournissant une preuve certaine d'un déséquilibre de pouvoir entre la personne concernée et le responsable de traitement. Une telle interprétation manichéenne ne semble cependant pas suffisante, tant du point de vue de la protection de la personne concernée que de celui de l'interprétation de la notion par le G29. Du point de vue de la personne concernée d'abord, une interprétation si stricte du caractère manifeste limiterait sa protection aux hypothèses de déséquilibres de

---

[770] CNRTL, « Manifeste », *CNRTL.fr*, Lexicographie, https://www.cnrtl.fr/definition/manifeste
[771] CALLET Clovis, *Le sérieux et le manifeste en droit judiciaire privé. Contribution à une étude de la certitude en droit*, Thèse pour obtenir le grade de docteur en droit sous la direction de CHÉROT Jean-Yves et PUTMAN Emmanuel, Université d'Aix-Marseille, 2015, telle que réécrite après la soutenance et mise à jour au 20 février 2021, p. 5.
[772] *Idem*, p. 6.
[773] *Idem*, p. 80.
[774] RIGAUX François, « Le juge, arbitre de la certitude du droit », *in* MACKAAY Ejan (dir.), *Les certitudes du droit*, p. 21.

pouvoir formels au détriment des hypothèses de déséquilibres réels. Le point de vue du G29 sur la notion de « déséquilibre manifeste » se comprend non seulement des éléments dont la certitude découle du droit, mais également des éléments de tromperie, intimidation, coercition, conséquences négatives, contrainte, pression ou incapacité[775]. Ainsi, la certitude ne porte pas sur l'existence de la cause de déséquilibre, mais sur le fait que l'existence du fait démontré déséquilibre de manière certaine la relation entre la personne concernée et le responsable de traitement au point que la personne concernée ne peut pas consentir de manière libre.

364. Deuxièmement, le déséquilibre manifeste signifie que le législateur n'a pas voulu réguler l'ensemble des situations dans lesquelles il existe un déséquilibre entre la personne concernée et le responsable de traitement. En effet, la logique d'*empowerment* fait de la personne concernée un réel acteur de sa protection des données à caractère personnel, et le protège déjà de nombreuses hypothèses de conditionnement de son consentement, notamment à travers la notion de préjudice sus étudiée. Le contrôle que le RGPD revendique accorder aux personnes concernées leur permet de rester libres en cas de déséquilibre peu important. La solution contraire se révélerait d'autant plus problématique que l'autre objectif du règlement est de permettre « le libre flux des données personnelles » au sein du marché intérieur[776]. Une vision trop stricte du déséquilibre n'aurait probablement pas permis à « l'économie numérique de se développer dans l'ensemble du marché intérieur »[777].

365. S'il est facile de démontrer que l'existence d'un lien de subordination ou d'un déséquilibre des pouvoirs déséquilibre de façon manifeste la relation entre la personne concernée et le responsable de traitement, tel n'est pas le cas du déséquilibre économique. Cela ne signifie pas que tous les déséquilibres économiques seront exclus de la notion de déséquilibre manifeste. Il existe des situations où le pouvoir économique d'un acteur sera si grand sur le marché qu'il en résultera un déséquilibre manifeste : il s'agit probablement des situations de mise à mal de la concurrence telles que l'existence d'une position dominante ou d'un monopole. Le mandat du Conseil de l'Union européenne quant aux négociations relatives au Règlement *ePrivacy* ainsi que la prise de position de la CNIL en matière de *cookie walls* semblent conforter cette interprétation puisque le déséquilibre manifeste entre le responsable de traitement est défini par le fait qu'il n'existe peu ou pas d'alternative au service, notamment du fait de la

[775] EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/579*, *op. cit.*, p. 11.
[776] RGPD, 27 avril 2016, considérant 3.
[777] RGPD, 27 avril 2016, considérant 7.

position dominante d'un fournisseur de service[778]. Dès lors, l'interprétation relative à l'existence d'un déséquilibre manifeste relève d'une application *in concreto* du RGPD lors de l'examen de la réalité du consentement.

§2 – Le déséquilibre manifeste en pratique

366. Le déséquilibre manifeste entre la personne concernée et le responsable de traitement s'évalue en fonction des conséquences que ce déséquilibre entraîne en matière de liberté de consentement de la personne concernée. Les travaux de l'EPBD ont ainsi rapidement affirmé que ces rapports de force doivent être interprétés de manière large, afin d'englober l'ensemble des situations de tromperie, intimidation et coercition, conséquences négatives importantes, éléments de contraintes, de pression, ou d'incapacité d'exercer un véritable choix[779]. Dans un même temps, le RGPD s'efforce d'accorder à la personne concernée suffisamment de pouvoir pour considérer la relation entre la personne concernée et le responsable de traitement suffisamment équilibrée pour garantir la liberté du consentement.

367. Ce double mouvement explique la focalisation du RGPD sur des situations où la personne concernée subit un lien de subordination avec le responsable de traitement, ce qui la place dans une situation particulièrement déséquilibrée avec ce dernier. Cependant, poursuivant sa logique d'*empowerment* et de refus d'infantiliser la personne concernée, le législateur n'a pas émis une interdiction absolue de recourir au consentement pour l'autorité publique et l'employeur. C'est ainsi que, dans une logique d'*accountability*, l'autorité publique (A) et l'employeur (B) doivent déterminer, traitement par traitement, la liberté de consentement dont dispose la personne concernée.

A. L'autorité publique

368. Du fait de la relation verticale existante entre le citoyen et l'administration, le RGPD protège la liberté de consentement de la personne concernée en invitant à adopter une diligence particulière lors de l'utilisation du consentement pour fonder un traitement de données à caractère personnel effectué par une autorité publique. En effet, le considérant 43 du RGPD dispose :

---

[778] Conseil de l'Union européenne, 2017/0003(COD), *op. cit.,* considérant (20aaaa) ; CNIL, « Cookie walls : la CNIL publie des premiers critères d'évaluation », *CNIL.fr*, 16 mai 2022, disponible sur https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookie-walls/la-cnil-publie-des-premiers-criteres-devaluation (consulté en juin 2022).

[779] EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/579*, *op. cit.,* p. 11.

> « Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable de traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière ».

Ainsi, souvent, le consentement ne sera pas la base juridique la plus appropriée pour le traitement de données par une autorité publique dans la mesure où le considérant 42 crée une présomption d'absence de liberté du consentement lorsque « la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice ».

369. Prenons l'exemple d'un centre de santé proposé par David Conerady et Aloïs Ramel dans Le Courrier des maires[780] : en fondant la collecte de données à caractère personnel sur le consentement, alors il ne sera pas possible de disposer d'information nécessaire à la prestation de soins. Dès lors, le recueil de données devant conditionner la prise en charge de la personne, la question du consentement se traduira par la question suivante : « voulez-vous être soigné ? Auquel cas, il faut consentir à la transmission de vos données »[781]. Il est évident que la personne concernée n'est ici pas en mesure de refuser son consentement sans subir de préjudice. Le Conseil d'État a suivi le même raisonnement à propos de l'installation de caméras thermiques à l'entrée d'un lycée en considérant que « la circonstance que l'accès des enfants à l'école soit subordonné à l'acceptation de l'utilisation de la prise de température par caméra thermique exclut en tout état de cause que le consentement puisse être regardé comme libre »[782].

370. Dès lors, l'autorité publique doit faire d'autant plus attention à respecter l'esprit initial de la base juridique du consentement : le consentement est un « dernier recours » [783], applicable lorsqu'aucune autre base juridique n'est applicable. La CNIL considère d'ailleurs que « dans la majorité des cas, les collectivités n'auront pas à recueillir le consentement »[784]. Il peut cependant exister des cas pour lesquels le consentement sera approprié : le G29 énonce à ce titre les exemples de l'inscription à une liste d'adresses électroniques permettant de s'informer

---

[780] CONERADY David, RAMEL Aloïs, « RGPD et consentement, un malentendu handicapant pour les acteurs publics », *Le Courrier des maires*, nos 335-336, juin-juillet 2019, p. 37.
[781] *Ibidem.*
[782] Conseil d'État, ordonnance, 26 juin 2020, Caméra*s thermiques à Lisses*, n°441065, §24.
[783] CONERADY David, RAMEL Aloïs, *op. cit.*, p. 37.
[784] CNIL, *Guide de sensibilisation au RGPD pour les collectivités* territoriales, p. 9, disponible sur https://www.cnil.fr/sites/default/files/atoms/files/cnil-guide-collectivite-territoriale.pdf

sur l'état d'avancement de travaux d'entretien de la voirie ou du consentement des étudiants pour utiliser leurs photographies dans une revue[785].

371. La question s'est posée récemment à propos des applications de localisation et recherche de contact dans le cadre de la lutte contre la Covid-19. Le Comité européen a invité les autorités publiques à ne pas confondre le caractère volontaire de l'installation de l'application par la personne concernée sur son terminal avec le consentement au titre du RGPD, la base juridique la plus appropriée en l'espèce étant l'exécution d'une mission d'intérêt public [786]. Cette position semble être la plus idoine à la situation puisqu'il « est certain que le caractère notamment libre de celui-ci serait difficile à caractériser dans un contexte anxiogène de pandémie mondiale »[787].

372. Il est cependant regrettable que la distinction entre le caractère volontaire de l'installation d'une application et la base juridique du consentement ne soit pas encore claire au sein du paysage juridique français. Les propos de Marie-Laure Denis à propos des applications de recherche de contacts dans le cadre de la pandémie sont particulièrement révélateurs : la présidente de la CNIL avait considéré que ces applications devaient reposer « sur le volontariat, c'est-à-dire le consentement libre et éclairé » [788].

Le Conseil d'État ne semble pas plus enclin à opérer une distinction entre utilisation volontaire d'un service ou d'une application et pertinence de la base juridique du consentement pour traiter les données à caractère personnel concernées. Dans l'affaire concernant la mise en place d'Alicem, un outil d'authentification utilisant la reconnaissance faciale, le Conseil d'État a en effet jugé :

> « Les téléservices accessibles via l'application « Alicem » l'étaient également, à la date du décret attaqué, à travers le dispositif FranceConnect, dont l'utilisation ne présuppose pas le consentement à un traitement de reconnaissance faciale. Dès lors que les usagers qui ne consentiraient pas au traitement prévu dans le cadre de la création d'un compte Alicem peuvent accéder en ligne, grâce à un identifiant unique, à l'ensemble des téléservices proposés, ils ne sauraient être regardés comme subissant un préjudice au sens du règlement général sur la protection des données précité »[789].

---

[785] Groupe de travail « Article 29 », *Lignes directrices sur le consentement au sens du règlement 2016/679, op. cit.*, p. 7.
[786] EDPB, *Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19, op. cit.*, p. 8.
[787] GAVANON Isabelle, LE MAREC Valentin, « Application de contact tracing : « un choix individuel gage de responsabilité collective » encadré par le CEPD », *Dalloz actualité*, 21 avril 2020.
[788] DENIS Marie-Laure, « Coronavirus : « Les applications de « contact tracing » appellent à une vigilance particulière », *LeMonde.fr*, Pixels, 5 avril 2020, disponible sur https://www.lemonde.fr/pixels/article/2020/04/05/coronavirus-les-applications-de-contact-tracing-appellent-a-une-vigilance-particuliere_6035639_4408996.html
[789] Conseil d'État, n°432656, *op. cit.*

373. La confusion entre l'utilisation volontaire et le consentement libre est problématique dans la mesure où elle confond l'utilisation du service avec le consentement au traitement de ses données à caractère personnel. Une telle interprétation a notamment été dénoncée par Émilie Debaets comme « un moyen de contournement d'une légalité plus stricte »[790], résultant de deux incohérences dans le raisonnement juridique. Premièrement, le Conseil d'État inverse la présomption du RGPD en interprétant *a contrario* le considérant 42. En effet, la présomption d'absence de liberté de consentement en cas de préjudice résultant du refus de consentement est interprétée par le Conseil d'État comme « une toute autre présomption : celle d'un consentement libre en l'absence de préjudice »[791]. Deuxièmement, le Conseil d'État apprécie la liberté du consentement « à la date du décret attaqué », c'est-à-dire sans inscrire le projet Alicem dans le projet pourtant annoncé par le gouvernement :

> « Alicem est une solution en « avance de phase », qui accompagnera la mise en place progressive de nouveaux téléservices nécessitant une authentification plus sécurisée qu'un « identifiant / mot de passe »[792].

L'autrice en déduit logiquement que le raisonnement du Conseil d'État est « paradoxal » dans la mesure où il ne prend pas en compte le préjudice futur, qui peut pourtant être anticipé de la communication du gouvernement[793]. Elle en conclut très justement que « libre aujourd'hui, le consentement ne le sera donc plus nécessairement demain lorsque de tels services seront mis en place »[794]. Ainsi, une solution pérenne serait d'autoriser Alicem à se fonder sur la base légale du consentement que si l'État propose une alternative à la reconnaissance faciale en tant qu'authentification très sécurisée aux téléservices concernés. Une autre solution, plus réaliste, serait de fonder Alicem non pas sur le consentement, mais sur l'intérêt public, ce qui impliquerait de réserver l'authentification Alicem aux seuls services nécessitant une authentification très sécurisée.

374. La confusion entre l'utilisation volontaire et la liberté du consentement est d'autant plus problématique qu'elle a eu lieu pour des traitements de données sensibles, qu'il s'agisse de données relatives à la santé ou de données biométriques. Or, puisqu'il s'agit de données pouvant générer des discriminations diverses ou de données « indélébiles » (la particularité des données

---

[790] DEBAETS Émilie, « À propos des dérives actuelles du consentement en matière de protection des données, *AJDA*, 2021, p. 346.
[791] *Ibidem.*
[792] Ministère de l'intérieur, « Alicem, la première solution d'identité numérique régalienne sécurisée », *L'actu du ministère*, 12 février 2020, disponible sur https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee
[793] DEBAETS Émilie, *op. cit.*, p. 346.
[794] *Ibidem.*

biométriques étant leur unicité et donc, la capacité de reconnaître un individu particulier), la liberté du consentement de la personne concernée aurait dû faire l'objet d'un examen plus minutieux au regard des conséquences attachées à leur éventuel traitement, voire à leur éventuelle fuite. Ces réflexions sont pourtant présentes au sein du débat public puisque par exemple, les lignes directrices développées par le Comité consultatif de la Convention 108 du Conseil de l'Europe ont affirmé qu'en « règle générale, le consentement ne devrait pas être le fondement juridique utilisé pour la reconnaissance faciale effectuée par les autorités publiques compte tenu du déséquilibre des pouvoirs entre les personnes concernées et ces autorités »[795].

375. Par conséquent, du fait du pouvoir hiérarchique entre l'autorité publique et la personne concernée, il n'est pas rare que la base légale du consentement ne soit pas appropriée aux traitements mis en place par l'autorité publique, et ce, à plusieurs titres. Premièrement, l'autorité publique ne peut pas se fonder sur le consentement lorsqu'elle met en place un traitement relevant de missions pour lesquelles elle dispose de prérogatives de puissance publique. Il serait en effet impossible de fonder les traitements de données à caractère personnel aux fins de recherche de fraude fiscale sur le consentement. Deuxièmement, l'autorité publique ne peut pas se fonder sur le consentement lorsque ce consentement est subordonné à un service dont elle est la seule ou l'une des rares exploitantes. Ainsi, il n'est pas imaginable de faire dépendre le traitement des données à caractère personnel dans le cadre d'un service public (par exemple, un abonnement aux transports en commun) sur la base du consentement. Enfin, l'autorité publique ne peut pas se fonder sur le consentement lorsque le traitement de données à caractère personnel relève d'une pression sociale ou peut engendrer un préjudice futur. Ces situations, dont les sources ne relèvent pas de l'évidence contrairement à leurs conséquences, doivent faire l'objet d'une prudence minutieuse de la part de l'autorité publique lors de la mise en place de ses traitements. Les exemples des applications de tracking de Covid-19 qui ont d'abord été adoptées sur la base d'une « utilisation volontaire » ne pouvaient ainsi pas relever de la liberté de consentement dans la mesure où non seulement la personne concernée pouvait ressentir une pression sociale au téléchargement de l'application, mais l'application a par la suite également facilité l'accès à certains lieux pour des raisons de santé publique grâce à l'émission simplifiée du pass sanitaire.

[795] Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), *Lignes directrices sur la reconnaissance faciale*, 28 janvier 2021, p. 5.

376. Ainsi, la liberté du consentement semble être protégée de façon satisfaisante par la notion de « déséquilibre manifeste » établie par le RGPD vis-à-vis de l'autorité publique, pour autant que son interprétation reste fidèle à l'esprit et à la lettre du règlement. La notion de « déséquilibre manifeste » vise également directement une autre relation de subordination en défaveur de la personne concernée : la relation entre l'employeur et l'employé.

B. L'employeur

377. Le considérant 42 du RGPD indique qu'il existe des situations dans lesquelles la personne concernée ne peut pas être considérée comme disposant d'une « véritable liberté de choix », qui résultent notamment d'un déséquilibre manifeste entre la personne concernée et le responsable de traitement. Dans ses lignes directrices sur le consentement, le G29 affirme explicitement qu'un tel déséquilibre peut avoir lieu « dans le cadre des relations de travail […] au vu de la dépendance résultant de la relation employeur/employé »[796], ce qui a été réaffirmé par la jurisprudence[797].

378. Le G29 avait déjà mis en exergue cette dépendance dans son avis de 2011 sur la définition du consentement, considérant que cette dépendance peut pousser la personne concerner à « craindre d'être traitée différemment si elle n'accepte pas le traitement de ses données »[798]. Dès lors, l'adéquation du consentement dans la relation employeur/employé est « peu probable »[799]. Dans son avis de 2001 sur les traitements de données à caractère personnel dans le milieu professionnel, le G29 a insisté sur le fait qu'un traitement fondé sur le consentement alors même que son refus ferait perdre au travailleur une opportunité d'emploi ne peut pas être libre[800]. Cependant, comme pour les autorités publiques, le G29 précise que « cela ne signifie toutefois pas que les employeurs ne peuvent jamais avoir recours au consentement en tant que base juridique pour le traitement des données »[801].

379. Il convient dès lors, en l'absence de précisions supplémentaires par le G29, de chercher les conditions de licéité du consentement dans la relation employeur/employé. À la lecture de la jurisprudence relative à la question de l'adéquation de la base juridique du consentement

---

[796] Groupe de travail « Article 29 », *Lignes directrices sur le consentement au sens du règlement 2016/679, op. cit.*, p. 7.
[797] V. par exemple HDPA, *Summary of Hellenic DPA's Decision No 26/2019, op. cit.*
[798] Groupe de travail « Article 29 », WP 18, *op. cit.*, p. 14
[799] Groupe de travail « Article 29 », WP 259 rev. 01, p. 8.
[800] Groupe de travail « Article 29 », *Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel*, adopté le 13 septembre 2001, WP 48, p. 32.
[801] Groupe de travail « Article 29 », WP 259 rev. 01, p. 8

dans la relation entre l'employeur et l'employé, il est possible d'identifier trois critères conditionnant le caractère libre du consentement dans les relations professionnelles.

380. Premièrement, le déséquilibre manifeste dans la relation verticale entre l'employeur et l'employé peut provenir du couplage du consentement avec d'autres bases juridiques rendant le traitement des données à caractère personnel obligatoire en vue d'autres finalités. Ces finalités peuvent être liées par exemple à l'exécution du contrat de travail ou encore à une obligation légale. Par exemple, la collecte du numéro de sécurité sociale de l'employé par l'employeur ne peut pas être fondée sur le consentement, car elle résulte d'une obligation légale à la charge de l'employeur. En 2019, l'autorité de contrôle grecque a rendu un arrêt intéressant à ce sujet, condamnant une société pour avoir utilisé comme base juridique le consentement alors que le traitement était fondé sur une obligation légale. Le choix inapproprié de base légale fondant le traitement de données à caractère personnel a notamment entraîné des conséquences en ce qui concerne le principe de transparence en raison de la fausse impression de voir ses données à caractère personnel traitées sur la base juridique du consentement alors qu'elles sont traitées sur une autre base juridique qui n'est pas portée à la connaissance des employés[802]. En effet, un employé aurait pu penser pouvoir exercer son droit de retirer son consentement quand la base juridique de l'obligation légale ne permet évidemment pas un tel retrait.

381. Deuxièmement, même en l'absence de couplage explicite, l'employeur doit veiller à ce que « la personne concernée soit en mesure de refuser de donner son consentement à son employeur concernant le traitement de ses données sans craindre ou encourir des conséquences négatives à ce refus »[803]. Le préjudice peut être réel (par exemple, une sanction professionnelle), mais aussi imaginé par le salarié, ce que le G29 souligne en affirmant que dans de nombreux cas, le salarié peut « se sentir obligé de consentir »[804]. Cette situation résulte du lien de subordination entre l'employeur et le salarié : à ce propos, l'autorité de contrôle britannique rappelle que « puisque les employés sont dépendants de l'entreprise pour leurs moyens de subsistance, ils peuvent se sentir obligés de consentir puisqu'ils ne veulent pas prendre le risque de perdre leur travail ou être perçus comme difficiles ou ayant quelque chose à cacher »[805]. Le sentiment de « se sentir obligé de consentir » a pour conséquence que le consentement ne peut être qu'une base juridique « exceptionnelle » pour les traitements de données à caractère

---

[802] HDPA, *Summary of Hellenic DPA's Decision No 26/2019*, *op. cit.*

[803] Groupe de travail « Article 29 », WP 259 rev. 01, *op. cit.*, p. 7 ; Cette règle a notamment été rappelée par l'autorité de protection des données belge, v. APD, 9 novembre 2020, n°72/2020, §31.

[804] Groupe de travail « Article 29 », WP 259 rev. 01, *op. cit.*, p. 8.

[805] ICO, « When is consent appropriate? », *Consent,* disponible sur https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/

personnel dans le milieu professionnel[806] : il existe donc une présomption d'absence de liberté du consentement du salarié sans sa relation avec l'employeur. L'autorité de protection des données néerlandaise a ainsi condamné une entreprise ayant utilisé le consentement pour fonder la collecte des empreintes digitales de ses employés. En effet, l'autorité de contrôle a rappelé la présomption de l'absence de liberté du consentement du salarié en raison de leur lien de dépendance avec leur employeur, et a démontré qu'en l'espèce, les employés croyaient que ce traitement était requis[807].

382. Troisièmement, l'autorité de protection des données belges a considéré qu'à « titre exceptionnel, un travailleur peut valablement consentir au traitement de données de la part de son employeur, lorsque ce dernier ne retire aucun avantage du traitement », car, dans cette situation, « le déséquilibre de pouvoir entre les parties ne risque donc pas de vicier le consentement »[808]. Ainsi, dans la mesure où si le consentement ne confère aucun avantage à l'employeur, il est possible de considérer que l'employé ne ressentira aucun sentiment de contrainte à l'égard de l'acceptation du traitement de données à caractère personnel.

383. Le déséquilibre manifeste entre l'employeur et l'employé ne semble pas créer de difficultés particulières dans l'interprétation de la liberté de consentement au sens du RGPD. En effet, la protection du travailleur est une question largement traitée par le droit de l'Union européenne, et la protection de la liberté de consentement de l'employé face à son employeur semble constituer un prolongement logique de la protection du travailleur.

384. Conclusion de section. – La notion de déséquilibre manifeste semble protéger efficacement la liberté de consentement de la personne concernée. Compromis entre la logique protectrice et la logique d'*empowerement*, l'adjectif manifeste permet de réserver le consentement aux situations de déséquilibres suffisamment peu importants pour ne pas relever de l'évidence, quand les situations de déséquilibres manifestes relèvent quant à eux soit d'autres bases légales de traitement, soit de l'interdiction. La confusion entre l'adoption volontaire d'un service et le consentement libre de la personne concernée se pose ainsi comme la seule ombre sur le tableau de la liberté du consentement RGPD, qui gagnerait à faire l'objet d'une interprétation clarificatrice de la CJUE.

---

[806] Groupe de travail « Article 29 » sur la protection des données, *Opinion 2/2017 on data processing at work*, adoptées le 8 juin 2017, WP 249, p. 23.

[807] AP, « Company fined for processing employees' fingerprint data", 30 avril 2020, disponible sur https://autoriteitpersoonsgegevens.nl/en/news/company-fined-processing-employees%E2%80%99-fingerprint-data

[808] APD, 9 novembre 2020, Décision quant au fond 72/2020, §32.

Conclusion du Chapitre 1

385. L'isolation du consentement de considérations économiques, qu'elles soient économiques ou hiérarchiques, permet de protéger la liberté du consentement de contraintes externes pouvant influencer la personne concernée au-delà de l'acceptable. L'isolation du consentement relève ainsi de la philosophie des vices du consentement, mais sa mise en œuvre relève de régimes plus protecteurs prenant en compte la place défavorable de la personne concernée dans sa relation avec le responsable de traitement.

386. Certes, l'isolation du consentement fait l'objet d'incertitudes législatives et jurisprudentielles que le législateur ou juge européen se doit d'adresser afin de mettre fin à des pratiques qui aujourd'hui relèvent plus de la zone grise du consentement que du respect de la lettre et de l'esprit du RGPD. Cependant, l'isolation externe du consentement de la personne concernée a permis de renforcer le caractère libre de celui-ci, mettant fin à des pratiques contestées lors du régime de la directive 95/46/CE.

387. Le bilan de cette directive a également poussé le législateur à protéger la liberté du consentement en délimitant les frontières de celui-ci, afin que l'objet du consentement corresponde à l'objet de la manifestation de volonté de la personne concernée.

CHAPITRE 2 – UN CONSENTEMENT DÉLIMITÉ

388. La notion de consentement libre est une notion très étudiée en droit civil. Selon Philippe le Tourneau, qualifier le consentement de libre revient à le qualifier de « réel »[809]. L'ancien article 1109 du Code civil définissait négativement le consentement libre, comme un consentement exempt de vices[810] :

> « Il n'y a point de consentement valable, si le consentement n'a été donné que par erreur, ou s'il a été extorqué par violence ou surpris par le dol ».

389. La définition est cependant plus restrictive en matière de protection des données à caractère personnel puisqu'elle exclut de son champ le consentement contractuel. Le consentement libre se définit ainsi comme un « choix sans contrainte ni influence »[811]. Le RGPD s'attache à définir le consentement dans son considérant 42 :

> « Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice ».

Dans cette définition se retrouve l'idée que le contraire de la liberté est la contrainte, qu'il s'agisse de notre liberté politique (« un choix sans contrainte ») ou de notre liberté métaphysique (« un choix sans influence »)[812].

390. La relation entre la liberté et la capacité de pouvoir accepter et refuser une proposition a longuement été traitée en philosophie. Dès l'Antiquité grecque, Épictète définit l'homme libre comme l'homme qui, par sa volonté, ne désire que ce qui dépend de lui-même[813]. Plus tard, Descartes affirmera avec plus de force la relation entre la liberté et le pouvoir de dire non, puisque, selon lui, la liberté est la capacité de la volonté de faire un choix absurde (c'est-à-dire un choix contre la raison)[814] :

> « À tel point que, lorsqu'une raison très évidente nous porte d'un côté, bien que moralement parlant, nous ne puissions guère choisir le parti contraire, absolument parlant, néanmoins, nous le pouvons. Car il nous est toujours loisible de nous retenir de poursuivre un bien clairement

---

[809] LE TOURNEAU Philippe, « Formation de la vente », *in* LE TOURNEAU Philippe (dir.), *Droit de la Responsabilité et des contrats 2021/2022*, Dalloz Action, 12e édition, 2020, p. 2016.
[810] *Ibidem/*
[811] FÉRAL-SCHUHL Christiane, *Cyberdroit. Le droit à l'épreuve de l'Internet*, Praxis Dalloz, 8e édition, 2020, p. 96.
[812] Voir la définition proposée par MORANA Cyril, OUDIN ÉRIC, *Petite Philosophie des grandes idées – La liberté*, Paris, Eyrolles, 2010, p. 11.
[813] « Que tout homme donc, qui veuille être libre, ne veuille et ne fuie rien de tout ce qui dépend des autres, sinon il sera esclave nécessairement ». Epictète, *Manuel*, XIV.
[814] MORANA Cyril, OUDIN ÉRIC, *op. cit.*, pp. 49-50.

> connu et d'admettre une vérité évidente, pourvu que nous pensions que c'est un bien d'affirmer par là notre libre arbitre »[815].

391. La liberté de pouvoir dire non se module également dans le temps. Dans son ouvrage *Du contrat social*, Jean-Jacques Rousseau affirmait qu'il « est absurde que la volonté se donne des chaînes pour l'avenir ». Bien intégrée dans le droit, l'on retrouve cette liberté de « pouvoir changer d'avis » dans la sanction des engagements perpétuels[816]. Or, cette liberté de changer d'avis doit se concilier avec la nature du consentement, puisque ce dernier oblige son auteur. Une telle conciliation est effectuée au sein du RGPD à travers le caractère temporaire du consentement (Section 1).

392. De plus, si la liberté de pouvoir dire non implique de pouvoir prendre des décisions les plus absurdes correspondant à la volonté, encore faut-il que l'objet du consentement soit suffisamment délimité pour que la personne concernée sache qu'elle est en train de consentir à un traitement de données à caractère personnel, lui-même clairement identifié (Section 2).

---

[815] Descartes, *Lettre au Père Mesland du 9 février 1945.*

[816] Sur le principe de prohibition des engagements perpétuels, v. CHANTEPIE Gaël « Contrats : effets – rayonnement du contrat », *Répertoire de droit civil*, §147-151.

Section 1 – Le caractère temporaire du consentement

393. La prohibition des engagements perpétuels constitue l'un des points de rupture de la Révolution française avec le régime féodal, au nom de la « préservation de la liberté de celui qui s'engageait, liberté évidemment méconnue par une situation créant des conditions proches d'une soumission personnelle, non pas à temps, mais bien à vie »[817]. La lecture de l'article 1780 du Code civil comme source de la prohibition des engagements perpétuels était cependant source de débats doctrinaux à propos de l'existence réelle d'un tel principe en droit des contrats[818]. La réforme du 10 février 2016 a finalement tranché le débat en consacrant législativement la sanction des engagements perpétuels à travers l'insertion de l'article 1210 dans e nouveau Code civil[819]. L'interdiction des engagements perpétuels s'inscrit dans la volonté de garantir la liberté individuelle puisqu'elle permet d'interdire des « contrats si longs qu'ils entravent *de facto* sinon *de jure* la liberté du cocontractant »[820]. L'interdiction de tels contrats a fait l'objet de différentes sanctions. Dans un premier temps, le contrat créant un engagement perpétuel a été strictement sanctionné par la nullité absolue du contrat[821]. La réforme de 2016 a opté quant à elle pour l'application du régime du contrat indéterminé en consacrant une faculté de résiliation unilatérale[822].

394. La philosophie de ces sanctions se retrouve dans le RGPD à travers une double protection de la personne concernée contre l'engagement perpétuel au traitement de ses données à caractère personnel. Premièrement, le RGPD interdit au responsable de traitement de conserver les données à caractère personnel au-delà de ce qui est nécessaire au regard des finalités du traitement (§1). Deuxièmement, le RGPD offre à la personne concernée la possibilité de se retirer à tout moment de son engagement à travers le retrait du consentement (§2).

§1 – La limitation des durées de conservation des données

395. Le principe de limitation des durées de conservation des données est établi par l'article 5(1)(e) du RGPD qui dispose que les données à caractère personnel doivent être

---

[817] LIBCHABER Rémy, « Réflexions sur les engagements perpétuels et la durée des sociétés », *Rev. Sociétés*, 1995, n°3, p. 437
[818] FABRE Marie, « Réflexions sur la sanction des engagements perpétuels après la réforme du 10 février 2016 », *D.*, 2020, p. 1189.
[819] *Ibidem*.
[820] LICARI François-Xavier, « Contrat. – Durée du Contrat, *JurisClasseur Civil Code*, 28 février 2017, §5.
[821] LICARI François-Xavier, *op. cit.*, §5 ; FABRE Marie, *op. cit.*, p. 1189.
[822] CHANTEPIE Gaël, *op. cit.*, §147-151.

> « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistes dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) »

396. L'article 5(1)(e) est ainsi construit en deux parties. Premièrement, le RGPD crée un principe général de limitation de la conservation dont les contours sont dessinés à travers les principes de nécessité et de proportionnalité. Deuxièmement, le RGPD concilie le principe général de limitation de la conservation avec des intérêts d'archivage particuliers qui doivent être mis en balance avec la garantie des droits et libertés de la personne concernée.

397. Le principe de limitation de la conservation crée à la charge du responsable de traitement l'obligation de déterminer la durée de conservation des données en fonction des finalités du traitement, et de détruire ou anonymiser celles-ci à l'issue de la durée choisie[823]. La CNIL distingue trois phrases dans le cycle de vie d'une donnée : l'utilisation courante (ou base active), l'archivage intermédiaire et l'archivage définitif. L'utilisation courante correspond à l'utilisation de la donnée à caractère personnel pour la finalité du traitement, l'archivage intermédiaire correspond à la conservation de la donnée à caractère personnel qui ne correspond plus à la finalité du traitement, mais dont la conservation répond à un intérêt administratif (principalement à titre de preuve en cas de contentieux) ou à une obligation légale et enfin l'archivage définitif correspond à la conservation des données dans le cadre d'une dérogation à la limite de la conservation[824].

398. La détermination de la durée de la conservation en base active n'est pas une tâche aisée pour le responsable de traitement. Si dans certains cas la durée de conservation est fixée par voie législative, dans la plupart des situations, la durée de conservation des données devra être fixée par le responsable de traitement. Les autorités de contrôle se sont donc naturellement saisies du sujet afin de fournir aux responsables de traitement des indications quant à la durée de conservation des données durant les différentes phases de leur cycle de vie.

399. Déterminer la durée de conservation des données nécessite un travail de recherche juridique par le responsable de traitement. Il devra en premier lieu rechercher s'il existe un texte

---

[823] DE TERWANGNE Cécile, ROSIER Karen (dir.), *op. cit.*, pp. 12-13.
[824] CNIL, *Guide pratique. Les durées de conservation*, juillet 2020, p. 4.

imposant une durée de conservation pour le traitement[825], ce qui nécessite un effort important pour les responsables de traitement traitant les données à caractère personnel dans plusieurs États membres de l'Union européenne[826]. En cas d'absence de telles dispositions, le responsable de traitement devra évaluer la durée de conservation des données qui est nécessaire à l'atteinte de la finalité fixée[827]. Le responsable de traitement pourra à ce titre se référer aux différents référentiels et préconisations délivrées par les autorités de contrôle[828]. Dans l'attente de tels référentiels, le responsable de traitement pourra également être orienté par les normes simplifiées adoptées par la CNIL qui n'ont pourtant plus de valeur juridique depuis l'entrée en vigueur du RGPD[829]. Par exemple, en matière de prospection commerciale, la norme NS-48 fournissait des informations précises sur les durées de conservation de données à caractère personnel concernant les prospects non clients :

> « Les données à caractère personnel relatives à un prospect non-client peuvent être conservées dans un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel ; en revanche, l'ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect)
>
> Au terme de ce délai de trois ans, le responsable de traitement pourra reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées conformément aux dispositions en vigueur ».

400. La durée de conservation des données va donc être évaluée principalement selon le principe de nécessité selon une analyse *in concreto* des besoins et des processus du responsable de traitement. Dans l'affaire *Spartoo*, la CNIL n'avait pas condamné la durée de conservation des données des prospects, fixée à cinq ans à partir de la dernière activité des prospects, par la société, sur la durée abstraite de celle-ci. Au contraire, la CNIL avait constaté que « la société n'adresse pas de prospection commerciale à ces personnes si elles ne manifestent pas d'intérêt pour ses produits ou services durant deux ans » : la conservation des données à caractère

---

[825] *Idem*, p. 14.
[826] Cette difficulté a poussé certains acteurs privés à créer des outils permettant de centraliser les durées de conservation des données à caractère personnel au sein des différents États membres. V. par exemple Alias.dev, « Durées de conservation », disponible sur https://www.durees-de-conservation.fr/ (consulté en décembre 2021).
[827] CNIL, juillet 2020, *op. cit.*, p. 14.
[828] *Ibidem.*
[829] CNIL, « Anciennes normes », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/les-cadres-de-reference/anciennes-normes

personnel des prospects ne se justifiait donc plus par la nécessité à partir de deux ans d'inactivité du prospect, et non pas cinq ans[830].

401. Une fois la base active déterminée et identifiée, le responsable de traitement devra décider si l'archivage intermédiaire des données est nécessaire légalement ou pour répondre à l'un de ses intérêts administratifs. La détermination des durées de conservation est plus aisée pour le responsable de traitement dans la mesure où elles vont s'aligner sur des délais légaux ou réglementaires (par exemple, « le temps des règles de prescription/forclusion applicables »[831]). L'archivage intermédiaire n'est pas systématique et doit être lu en concordance avec le principe de minimisation des données. Des difficultés sont ainsi nées dans les entreprises souhaitant se mettre en conformité avec le RGPD à propos de la détermination des données à conserver dans le cadre de l'archivage intermédiaire. Le cabinet *DPO consulting* dénonce par exemple la liste de documents pouvant faire l'objet d'un archivage intermédiaire en matière de ressources humaines fournie par la CNIL dans la norme simplifiée NS 46[832]. Le cabinet spécialisé en protection des données à caractère personnel s'interroge en effet sur l'adéquation de la destruction de certaines données avec le risque de contentieux prud'homal, la prévention de la fraude ou encore les exigences légales en matière de preuve[833].

402. Enfin, l'archivage définitif relève des dérogations prévues à l'article 89 du RGPD. Les finalités d'un tel archivage sont limitées à des finalités répondant à un intérêt public, permettant la recherche scientifique ou historique ou à la représentation statistique. Un tel archivage nécessite de la part des responsables de traitement une prudence particulière dans la mise en balance de ces traitements avec les droits fondamentaux de la personne concernée. Le responsable de traitement doit en effet mettre en place des garanties appropriées pour les droits et libertés des personnes concernées, parmi lesquelles la mise en place de mesures techniques et organisationnelles afin d'assurer le principe de minimisation des données ou encore de mettre en place une pseudonymisation des données voire une anonymisation[834]. La prudence est

---

[830] CNIL, Délibération de la formation restreinte SAN-2020-003 du 28 juillet 2020 concernant la société X, §51 ; CNIL, « Spartoo : sanction de 250 000 euros et injonction sous astreinte de se conformer au RGPD », 5 août 2020, disponible sur https://www.cnil.fr/fr/spartoo-sanction-de-250-000-euros-et-injonction-sous-astreinte-de-se-conformer-au-rgpd (consulté en décembre 2021).

[831] CNIL, « Comment concilier les durées de conservation et les archives », *CNIL.fr*, 18 septembre 2019, https://www.cnil.fr/fr/comment-concilier-les-durees-de-conservation-et-les-archives (consulté en décembre 2021).

[832] DPO Consulting, « Les difficultés d'application du RGPD dans les entreprises – La conservation des données, un casse-tête pour les entreprises ? », *Cahiers de droit de l'entreprise*, 2019, n°1, dossier 6.

[833] *Ibidem.*

[834] EDPB, *Avis 10/2017 sur les garanties et dérogations prévues à l'article 89 du RGPD dans le cadre d'une proposition de règlement concernant les statistiques intégrées sur les exploitations agricoles,* 20 novembre 2017, p. 14.

d'autant plus importante pour l'archivage à des fins de recherche scientifique qui peut découler d'un consentement dont les finalités n'ont pas été entièrement cernées au moment du consentement[835]. Ainsi, l'article 89 prévoit des dérogations aux droits d'accès, de rectification de limitation du traitement et d'opposition de la personne concernée « dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités »[836]. L'EDPB a eu l'occasion de préciser que de telles entraves ne pouvaient pas consister ni en la nécessité de ressources financières et humaines supplémentaires (« rapport coût-efficacité ») ni en des difficultés techniques si l'état de l'art montre qu'il existe des mesures techniques et organisationnelles permettant de les dépasser[837].

403. Si la pratique du principe de limitation des durées de conservation peut présenter des difficultés du point de vue du responsable de traitement, ce principe constitue cependant une garantie indispensable de la liberté du consentement. En effet, son couplage avec le principe de minimisation des données et de limitation des finalités permet à la personne concernée d'entrevoir les contours du traitement de données à caractère personnel : le traitement correspond ainsi aux attentes raisonnables de la personne concernée. Il peut cependant être regretté que ces durées de conservation ne fassent ni l'objet d'une standardisation ni d'une obligation d'information précise au titre du principe de transparence. Une telle pratique aurait le double bénéfice de simplifier la détermination des durées de conservation par le responsable de traitement et de préciser les contours des attentes raisonnables de la personne concernée. De plus, la délimitation dans le temps de l'objet du consentement (du moins, la délimitation de la durée de conservation en base active) peut raisonnablement entrer dans les critères de décision de la personne concernée quant aux traitements de ses données à caractère personnel[838]. Ainsi, la limitation des durées de conservation constitue une garantie de la liberté du consentement dont le potentiel protecteur est limité par la difficulté d'implémentation de la pratique et l'absence de standards permettant de déterminer des attentes raisonnables qui correspondent aux réelles attentes raisonnables de la personne concernée. Cependant, s'agissant du consentement, ces difficultés sont compensées par la possibilité de retirer son consentement à tout moment, ce qui permet à la personne concernée de faire correspondre activement ses

[835] RGPD, 27 avril 2016, considérant 33.
[836] RGPD, 27 avril 2016, Article 89(2), Article 89(3).
[837] EDPB, 20 novembre 2017, *op. cit.*, pp. 9-10
[838] *Ibidem.*

attentes en matière de traitement de données à caractère personnel avec la mise en œuvre du traitement par le responsable de traitement.

§2 – Le retrait du consentement

404. La consécration textuelle du retrait du consentement est une garantie supplémentaire au consentement de la personne concernée. En effet, le considérant 42 du préambule du RGPD va lier le retrait du consentement au caractère libre de ce dernier. Dès lors, le retrait du consentement se présente en premier lieu comme un moyen de protection des données à caractère personnel en faveur de la personne concernée (A).

405. Cependant, le consentement est un mécanisme juridique qui oblige et qui a notamment pour objet la garantie de la sécurité des actes juridiques[839] : en donnant son consentement, la personne rend le traitement de ses données à caractère personnel licite. Dès lors, les modalités de retrait du consentement doivent concilier le retrait du consentement avec les intérêts, importants et principalement économiques, du responsable de traitement (B).

A. La protection de la personne concernée

406. Le consentement au traitement des données à caractère personnel est « précaire »[840]. Le G29 considère par conséquent que « le consentement n'est pas susceptible de fournir un cadre adéquat à long terme pour les responsables du traitement »[841], notamment du pouvoir accorder à la personne concernée de pouvoir retirer son consentement. Le retrait du consentement comme manifestation d'un consentement temporellement limité à l'adéquation du consentement à la volonté de la personne concernée a pour objet principal la protection de la personne concernée. Ainsi, l'article 7(3) du RGPD consacre textuellement le retrait du consentement :

> « La personne concernée a le droit de retirer son consentement à tout moment […]. Il est aussi simple de retirer que de donner son consentement ».

407. Ainsi, le retrait du consentement, tel qu'établi par le RGPD, apporte une double garantie à la personne concernée. Premièrement, le consentement garantit positivement la liberté de la personne concernée puisqu'il est un engagement qui ne s'inscrit pas dans une durée figée

---

[839] BERGEL Jean-Louis, « La sécurité juridique », *Revue du Notariat*, volume 110, numéro 2, septembre 2008.
[840] PERRAY Romain, *op. cit.*, §110 ; BOURGEOIS Matthieu, *Droit de la donnée*, Paris, 2017, p. 72 ; MATTATIA Fabrice, « Pour en finir avec le mythe du consentement RGPD », *La Semaine Juridique Administrations et Collectivités territoriales*, n°16, 20 avril 2020.
[841] Groupe de travail « Article 29 », *Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995,* adopté le 25 novembre 2005, 2093-01/05/FR, WP 114, p. 25.

puisque la personne concernée peut se dégager de cet engagement à tout moment. Deuxièmement, le RGPD protège la personne concernée du responsable de traitement contre d'éventuelles manœuvres visant à l'empêcher de retirer son consentement en inscrivant en son sein une obligation de facilité de retrait de son consentement sans subir de préjudice.

408. En premier lieu, le consentement garantit la liberté positive de la personne concernée, qui peut se dégager d'un engagement à tout moment. Bien que l'on puisse voir dans l'interdiction des contrats perpétuels une manifestation du droit de changer d'avis, ce droit est limité en matière de droit des contrats. Le consentement en matière de protection des données à caractère personnel va se différencier de manière importante avec le consentement contractuel. En effet, si le consentement en matière de protection des données oblige la personne concernée, il ne l'oblige pas en vertu d'une prestation de service ou une fourniture de bien déterminée. Ainsi, le consentement en matière de protection des données à caractère personnel relève, comme relevé plus tôt, plus du sacrifice que de l'échange en vue d'un bénéfice.

409. Or, si la personne concernée consent à l'atteinte de son droit à la protection de ses données à caractère personnel, elle « entend rester libre »[842]. Le consentement à l'atteinte, au sacrifice, se module différemment sur le plan de la temporalité. En matière d'atteinte, le consentement « doit exister au moment de l'atteinte pour avoir une valeur significative », le consentement doit donc nécessairement être évalué au moment de l'atteinte[843]. *A contrario*, en matière de contrat, le contractant « projette dans l'avenir les effets d'une volonté présente »[844]. Ainsi, les enjeux liés au retrait du consentement vont être les mêmes qu'en matière pénale et en matière des droits de l'Homme. En effet, puisque le consentement a un effet transformateur de l'illégal au légal, la pratique rendue légale par le consentement ne l'est que durant la durée de ce dernier. L'arrêt précité *K.A. contre Belgique* rendu par la CEDH en est la parfaite illustration. En l'espèce, les pratiques sadomasochistes n'avaient été rendues légales au regard du Code pénal belge et de l'article 3 de la Convention européenne de sauvegarde des droits de l'Homme que par le consentement de la femme victime de ces pratiques. Ainsi, la condamnation des deux magistrats se restreignait aux faits de sadomasochismes infligés à leur victime à partir du moment où celle-ci avait retiré son consentement. La Cour résume ce principe :

---

[842] TOSI-DUPRIET Isabelle, « Le consentement aux atteintes aux droits de la personnalité, un fait juridique : la doctrine *Ancel* », *in* DEUMIER Pascale *et al.* (dir.), *Mélanges en l'honneur de Pascal Ancel*, 1re édition, Bruxelles, Larcier, 2021, p. 593.
[843] *Ibidem.*
[844] *Ibidem.*

> « Si une personne peut revendiquer le droit d'exercer des pratiques sexuelles le plus librement possible, une limite qui doit trouver application est celle du respect de la volonté de la « victime » de ces pratiques, dont le propre droit au libre choix quant aux modalités d'exercice de sa sexualité doit aussi être garanti »[845].

410. Ainsi, la limite temporelle du consentement au traitement des données à caractère personnel coïncidera avec la limite temporelle de la volonté. Rien de surprenant dans la mesure où la règle de droit doit tenir compte « du caractère temporaire des situations humaines ».[846] C'est ainsi que le retrait du consentement renforce l'adéquation de celui-ci avec la volonté de la personne concernée. Ce renforcement est d'autant plus indispensable si l'on considère, à l'instar de Florence Bellivier, que le consentement « peut n'être pas l'expression d'une volonté enthousiaste, mais une adhésion plus ou moins subie »[847]. En effet, si le consentement en tant qu'acte juridique oblige en droit des contrats, la liberté du consentement en tant que fait juridique réside dans le pouvoir du « non »[848] : le retrait du consentement est une manifestation de la liberté du consentement de la personne concernée[849]. Le lien entre liberté du consentement et retrait du consentement est d'ailleurs explicite dans le RGPD, dont le considérant 42 dispose que « le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée […] n'est pas en mesure de retirer son consentement sans subir de préjudice ».

411. Cette réflexion a trouvé un écho auprès des autorités de contrôle : en 2011, le G29 a relié la notion du retrait du consentement – notion qui n'était alors pas consacrée dans les textes de protection des données à caractère personnel – à la notion de contrôle de la personne concernée sur ses données[850]. La place accordée au sein du RGPD au retrait du consentement proviendrait ainsi d'une « codification » de la réflexion développée par le G29, dans la lignée de l'enjeu de liberté du consentement[851]. L'inscription du droit au retrait du consentement au sein du RGPD est ainsi une avancée dans le renforcement du consentement. Cependant, ce droit

---

[845] CEDH, n°42758/98 et 45558/99, *op. cit.*, §85.
[846] AYNÈS Augustin, « Les fonctions du temps », *in* Association Henri Capitant, *Le temps et le droit*, Journées nationales, Tome XVIII, Dijon, p. 78.
[847] BELLIVIER Florence, « Le droit de retrait en bioéthique sur la voie de l'émancipation », *Droits*, 2008/2, n°48, pp. 131-146.
[848] La nature juridique du consentement en matière de droit des contrats et de droits de la personnalité est analysée par TOSI-DUPRIET Isabelle, « Le consentement aux atteintes aux droits de la personnalité, un fait juridique : la doctrine *Ancel* », *in* DEUMIER Pascale *et al.* (dir.), *Mélanges en l'honneur de Pascal Ancel*, 1re édition, Bruxelles, Larcier, 2021, p. 593. La différence entre les deux natures de consentement réside dans la force obligatoire du consentement-acte juridique et à la libre révocabilité du consentement-fait juridique.
[849] FRISON-ROCHE Marie-Anne, « Remarques sur la distinction de la volonté et du consentement en droit des contrats », *RTD Civ*., 1995, p. 573.
[850] Groupe de travail « Article 29 », WP 187, *op. cit.*, p. 10.
[851] Groupe de travail « Article 29 », WP259 rév. 01, *op. cit.*, p. 25.

doit être garanti vis-à-vis du responsable de traitement : c'est pourquoi le RGPD prévoit, dans ses modalités, une protection du retrait du consentement opposable au responsable de traitement.

412. En second lieu, la personne concernée sera protégée contre d'éventuelles manœuvres visant à l'empêcher de retirer son consentement, le RGPD interdisant d'attacher au retrait du consentement un préjudice. Formellement, la protection du droit au retrait du consentement est garantie par un parallélisme des formes, dans la mesure où « il est aussi simple de retirer que de donner son consentement. Si le G29 remarque que le RGPD ne précise pas que le parallélisme des formes doive résulter en la même action permettant de donner et retirer son consentement, il considère tout de même que les personnes concernées doivent pouvoir donner et retirer leur consentement par « le même biais » afin d'éviter à la personne concernée de devoir déployer des « efforts inutiles »[852].

413. Dans ses lignes directrices sur le consentement, le G29 a eu l'occasion de préciser ces dispositions. Ainsi, la simplicité du retrait du consentement implique un parallélisme des formes, soit la possibilité de retirer le consentement via la même interface que celle permettant de le donner dans la mesure où « changer d'interface à la seule fin de retirer son consentement nécessiterait des efforts inutiles »[853]. L'autorité de contrôle polonaise a eu l'occasion de préciser ce qui pouvait constituer un effort inutile. Premièrement, le retrait du consentement ne doit pas comporter d'étapes non essentielles au retrait du consentement, comme l'obligation d'indiquer la raison du retrait du consentement. Deuxièmement, le retrait du consentement ne doit pas être rendu difficile par le responsable de traitement par des manœuvres induisant la personne concernée en erreur. Par exemple, en l'espèce, la société demandait à la personne de remplir un formulaire de retrait du consentement, puis envoie un message demandant d'envoyer à nouveau sa demande à une adresse mail déterminée, message comportant la phrase suivante : « votre consentement est retiré aujourd'hui ». En effet, l'autorité de contrôle considère :

> « Il ne fait aucun doute que la grande majorité des gens, après avoir lu le contenu de ce libellé, déclarent que la déclaration de retrait du consentement a été acceptée par la Société à la date indiquée dans l'annonce et ne prend donc aucune mesure supplémentaire à cet égard »[854].

Dans cette optique, le retrait du consentement relève non seulement de la liberté du consentement, mais également de l'obligation de transparence et de loyauté du traitement à

---

[852] Groupe de travail « Article 29 », WP259 rév. 01, *op. cit.*, p. 25.
[853] *Ibidem.*
[854] Urząd Ochrony Danych Osobowych (UODO), 16 octobre 2019, ZSPR.421.7.2019, disponible sur https://uodo.gov.pl/decyzje/ZSPR.421.7.2019 (consulté en avril 2021) [traduction libre].

l'égard des personnes concernées. En effet, en vertu de ces principes, la personne concernée doit être informée à tout moment de la possibilité de retirer son consentement et de l'existence de l'opération de traitement.

B. La licéité limitée des traitements antérieurs

414. L'article 7(3) du RGPD protège les intérêts du responsable de traitement à l'égard des traitements antérieurs au retrait du consentement qui restent licites et dont l'arrêt ou l'effacement relèvent de l'exercice de droits supplémentaires par la personne concernée. Cependant, une telle solution limitant la licéité du traitement à une date de retrait de consentement déterminée crée, à l'égard du responsable de traitement, une obligation de diligence particulière dans sa gestion des consentements.

415. La solution de préserver la légalité des traitements antérieurs au retrait du consentement n'est pas étonnante dans la mesure où cette solution permet de mettre en balance les droits de la personne concernée avec les intérêts du responsable de traitement. Une telle solution avait notamment été énoncée en matière de droit à l'image par la deuxième chambre civile de la Cour de cassation le 10 mars 2004. En l'espèce, un tradipraticien avait par lettre recommandée mis en demeure la société TF1 de ne pas diffuser les images et les propos enregistrés au cours d'un reportage le concernant et pour lequel il avait donné son accord à l'utilisation ou à la diffusion de son image. En effet, le tradipraticien considérait qu'il avait le droit au retrait de son consentement à tout moment, sans justifier de sa décision. La Cour de cassation avait rejeté ce moyen et avait jugé que le fait que le tradipraticien ait donné son accord à la réalisation du reportage et n'avait émis aucune protestation au cours du tournage résultait en ce que « le retrait de son consentement sans justification réelle d'un manquement à la finalité visée dans l'autorisation qu'il avait donnée, n'était pas légitime »[855]. Ainsi, dès 2004, la Cour de cassation parvient à une solution en matière de droit à l'image identique à celle retenue en matière de données à caractère personnel : le retrait du consentement ne rend pas illégaux les traitements des données à caractère personnel antérieurs, à moins qu'un motif légitime (comme par exemple, l'éventuel exercice du droit à l'oubli) s'applique au traitement.

Ainsi, l'article 7(3) du RGPD permet aux responsables de traitement de bénéficier d'une certaine sécurité juridique de leurs traitements de données à caractère personnel, puisqu'il

[855] Cass. Civ. 2, 10 mars 2004, n°02-16.354, Publié au bulletin.

dispose que « le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait ».

416. Cependant, il est important de rappeler que la licéité des traitements antérieurs doit être limitée dans le temps de manière étanche. Le retrait de consentement suppose donc une diligence particulière du responsable de traitement quant à la gestion des consentements et retraits de consentement. Le responsable de traitement doit définir un processus particulier lui permettant de gérer de manière efficace les consentements, et notamment d'arrêter immédiatement le traitement des données à caractère personnel d'une personne concernée. Ce processus pourra prendre une forme automatisée permettant de déclencher l'arrêt automatique du traitement dès la réception de la requête de la personne concernée[856].

417. Ainsi, les autorités de contrôle n'accepteront pas comme justification l'erreur évitable du responsable de traitement. Par exemple, l'autorité de protection des données espagnole (AEPD) a condamné la société Vodafone pour traitement de données sans base légale, dans la mesure où la personne concernée avait retiré son consentement. La société Vodafone a plaidé à cet effet une erreur dans la suppression des données de leurs systèmes, niant toute forme d'intention quant à la commission des faits reprochés[857]. L'autorité de contrôle balaye cet argument et rappelle le devoir de diligence du responsable de traitement :

> « Il convient de souligner que le respect du principe de licéité des traitements de données à caractère personnel exige qu'il soit prouvé que la personne concernée a consenti au traitement de ses données à caractère personnel et que la diligence raisonnable requise pour le prouver soit déployée. Sinon, le résultat viderait de contenu le principe de licéité du traitement »[858].

418. Le responsable de traitement devra également prêter une attention particulière à la question de la conservation des données à la suite du retrait du consentement de la personne concernée. À cet égard, le G29 précise que « les responsables de traitement ont l'obligation de supprimer les données ayant été traitées sur la base du consentement une fois le consentement retiré, à condition qu'aucune autre finalité ne justifie leur conservation »[859], tout en précisant

---

[856] Voir par exemple, BESIK Saliha, FREYTAG Johann-Christoph, « Managing consent in Workflows under GDPR », *in* MANNER Johannes *et al.* (dir.), 12th ZEUS Workshop, ZEUS 2020, Postdam, Germany, Février 2020.

[857] « Que tal y como dio contestación al requerimiento deinformación recibido de la Agencia, los hechos se debieron a un error en el proceso desupresión de datos de nuestros sistemas. Todos los datos fueron efectivamente suprimidos de todos los sistemas de la compañía a excepción de la cuenta de correo en el sistema de envío de avisos de facturación. Es decir, no existió intencionalidad alguna por parte de mi representada en cometer los hechos producidos ». AEPD, PS-00278-2019, publiée le 3 février 2020..

[858] « Hay que señalar que el respeto al principio de licitud de los datosexige que conste acreditado que el titular de los datos consintió en el tratamiento de los datos de carácter personal y desplegar una razonable diligencia imprescindible para acreditar ese extremo. De no actuar así el resultado sería vaciar de contenido el principio de licitud » [traduction libre]. *Ibidem.*

[859] Groupe de travail « Article 29 », WP 259 rev. 01, *op.cit* , p. 26.

en note de bas de page que cette autre finalité « doit disposer de sa propre base juridique »[860], neutralisant ainsi toute possibilité pour le responsable de traitement de substituer au consentement une autre base juridique au moment du retrait du consentement[861].

419. Cependant, cette solution s'articule mal avec la décision de l'autorité de protection des données grecque (HDPA) qui dans un arrêt de 2019 considère :

> « *Where the legal basis of consent is properly applied, in the sense that no other legal basis is applicable, refusal of consent or its withdrawal is equivalent to an absolute prohibition on the processing of personal data* »[862].

En effet, selon l'HDPA, conserver les données à caractère personnel de la personne concernée après le retrait de son consentement reviendrait à rendre son consentement « tartufe », puisque cela reviendrait à lui donner « la « fausse impression » de consentir à ce traitement quand celui-ci est en réalité fondé sur une autre base juridique »[863].

420. Si l'interprétation de l'HDPA respecte l'esprit du consentement indépendant de l'ensemble des autres bases juridiques, force est de constater que l'interprétation du G29 prend davantage en compte l'ensemble des dispositions du RGPD. Finalement, c'est à travers ses dispositions sur le droit à l'effacement que le législateur européen envisage la possibilité pour le responsable de traitement de contourner le retrait du consentement de la personne concernée en conservant les données en vertu d'un autre fondement juridique. En effet, l'article 17 du RGPD dispose :

> « La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant […] lorsque l'un des motifs suivants s'applique : […]
>
> b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ».

421. Dès lors, la liberté du consentement de la personne concernée semble garantie par l'exercice du droit au retrait de son consentement, même si une interrogation persiste sur l'effectivité de ce droit en vertu de la possibilité pour le responsable de traitement de le neutraliser à travers une autre base juridique.

---

[860] *Ibidem.*
[861] *Ibidem.*
[862] HDPA, *Summary of Hellenic DPA's Decision No 26/2019, op. cit.*
[863] *Ibidem.*

422. Conclusion de section. – La délimitation temporelle du consentement permet de garantir la liberté de consentement de la personne concernée dans la mesure où elle permet une délimitation active, par le retrait du consentement, ou passive, par le principe de limitation de la durée de conservation des données, de l'objet du consentement. La durée de traitement de données à caractère personnel devient ainsi soit un critère de décision quant à l'émission ou non d'un consentement, soit le résultat de la volonté de la personne concernée, dont le consentement est également limité dans le temps. La délimitation temporelle du consentement s'accompagne d'une délimitation spatiale du consentement, concrétisée par l'identification du consentement.

Section 2 – Un consentement identifié

423. Pour que le consentement soit libre et éclairé, il faut que le périmètre du consentement ainsi que l'acte de consentir soient correctement et facilement identifiés par la personne concernée. Le consentement, en ce qu'il oblige la personne qui a consenti[864], doit d'abord pouvoir être exactement être identifié par la personne concernée dont la liberté consistera en l'évaluation de ce que Anne-Marie Frison-Roche appelle « l'échange des otages »[865] :

> « Car le consentement est donc bien un otage donné : il doit y avoir un échange des otages […]. Je ne donne mon consentement que si je me saisis du consentement de l'autre. Le consentement n'est supportable que par l'échange. Il faut concevoir non pas tant l'échange des consentements que le consentement parce que l'échange »[866].

424. Dès lors, pour le consentement soit un reflet *a minima* de la volonté, le RGPD a protégé le consentement de la personne concernée en lui permettant d'une part d'évaluer le périmètre de son consentement en instituant un consentement spécifique (A) et d'autre part, d'identifier toutes les demandes de consentement en exigeant un consentement explicite (B).

§1 – Un consentement spécifique

425. Qualifier le consentement de spécifique n'est pas une nouveauté du RGPD puisque la directive 95/46/CE définissait le consentement comme « toute manifestation de volonté, libre, spécifique et informée par laquelle la personnelle concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement »[867]. En France, le consentement spécifique était également exigé en ce qui concernait la prospection par voie électronique. L'article L. 34-5 du Code des postes et des communications électroniques disposait en effet qu'on « entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe »[868]. En 2015, le Conseil d'État a eu l'occasion de rappeler ce principe lors d'un arrêt condamnant la société TUTO4PC. Le juge du Palais Royal avait alors rappelé :

> « alors même que, comme le soutient la société, l'information serait suffisante et les conditions générales d'utilisation claires et explicites, le consentement donné à ces dernières pour

[864] FRISON-ROCHE Marie-Anne, 1995, *op. cit.,* pp. 573-574.
[865] *Idem,* p. 575.
[866] *Ibidem.*
[867] Directive 95/46/CE, 24 octobre 1995, Article 2 (h).
[868] Article L34-5 du Code des postes et des communications électroniques, tel que modifié par l'article 115 de la loi n°2014-344 du 17 mars 2014 (version en vigueur au 19 mars 2014).

> l'ensemble des finalités d'un traitement, dont l'usage des données personnelles de l'utilisateur, ne saurait être regardé comme valant consentement spécifique »[869].

426. Déjà sous le régime de la directive 95/46/CE, la CNIL avait déjà jugé que le fait de fournir une information générale ne permettant pas à la personne concernée « d'associer un type de cookie et une finalité au service qu'il utilise » n'était pas considéré comme valide au sens de la directive dans la mesure où « cette information n'est pas suffisamment circonstanciée quant aux cookies liés au service que l'utilisateur va utiliser »[870]. La CNIL avait également, à l'occasion d'une autre affaire, précisé qu'un consentement obtenu pour l'objet principal de « fournir un contenu d'information » devait faire mention, au titre de l'obligation d'un consentement spécifique, de l'objet « à titre accessoire à assurer une opération de prospection ».[871]

427. La CJUE avait aussi rappelé la préexistence de l'exigence d'un consentement spécifique dans la directive 95/46/CE lors d'un arrêt du 1er octobre 2019, dans lequel elle a examiné la conformité des traitements de données à caractère personnel de la société Planet49 GmbH successivement par rapport à la directive et au règlement[872]. Elle avait ainsi affirmé :

> « La manifestation de volonté visée à l'article 2, sous h), de la directive 95/46 doit, notamment, être « spécifique », en ce sens qu'elle doit porter précisément sur le traitement de données concerné et ne saurait être déduite d'une manifestation de volonté ayant un objet distinct […]. L'interprétation qui précède s'impose, à plus forte raison, à la lumière du règlement 2016/679 »[873].

428. Comme le remarque la Cour, l'obligation du RGPD est en effet plus précise dans la mesure où elle explicite les obligations découlant du caractère spécifique du consentement. Le considérant 43 précise en effet que « le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel ». De plus, le Groupe de l'Article 29 a précisé :

> « sans préjudice des dispositions relatives à la compatibilité des finalités, le consentement doit être spécifique à la finalité. Les personnes concernées donneront leur consentement en sachant qu'elles en possèdent le contrôle et que leurs données ne seront traitées qu'à ces fins spécifiques »[874].

---

[869] CE, 10e et 9e sous-sections réunies, 11 mars 2015, n° 369624.
[870] CNIL, Délibération de la formation restreinte n°2013-420 du 3 janvier 2014 prononçant une sanction pécuniaire à l'encontre de la société X.
[871] CNIL, Délibération de la formation restreinte n°2015-155 du 1 juin 2015 prononçant une sanction pécuniaire à l'encontre de la société X.
[872] CJUE, C-673/17, *op. cit.*.
[873] *Idem*, §58 et 60.
[874] Groupe de travail « Article 29 », WP 259 rev. 01, p. 11.

Dans un arrêt Orange România du 11 novembre 2020, la CJUE a confirmé son arrêt Planet49 en ce qui concerne le consentement spécifique en reprenant exactement son point 58 définissant le consentement spécifique[875].

429. En 2019, la CNIL a rappelé que l'obligation de consentement spécifique doit s'apprécier au regard de la finalité du traitement. Lors de son contrôle des traitements de la société EDF et notamment de ses compteurs Linky, l'autorité de contrôle a regretté que la société recueille à l'aide d'une seule case à cocher le consentement des usagers de ses compteurs Linky alors même qu'elle traite leurs données pour trois finalités distinctes (« l'affichage dans l'espace client des consommations quotidiennes, l'affichage dans l'espace client des consommations à la demi-heure et des conseils personnalisés visant à mieux maîtriser leur consommation d'électricité »)[876]. Or, la CNIL va d'autant plus mettre en exergue la non-conformité d'un tel consentement aux exigences du RGPD que « ces opérations de traitement sont distinctes et indépendantes les unes des autres : ainsi, un usager peut souhaiter consulter l'historique de ses consommations à la journée, sans nécessairement vouloir bénéficier d'un affichage à la demi-heure ou souhaiter recevoir des conseils personnalisés de la part de son fournisseur ». D'ailleurs, la CNIL liera même l'absence de caractère spécifique du consentement à l'absence de consentement éclairé puisqu'en l'espèce, la case à cocher proposée par EDF pouvait induire l'usager en erreur en ce qui concerne la portée de son abonnement, dans la mesure où « les données quotidiennes et à la demi-heure sont présentées comme étant équivalentes, alors que les données à la demi-heure sont plus révélatrices des habitudes de vie des personnes que les données quotidiennes »[877].

430. Cette interprétation du RGPD permet également une interprétation plus stricte de la directive e-privacy. L'autorité de protection des données danoise a par exemple considéré qu'il n'est pas possible de consentir en un bloc à l'ensemble des cookies lorsque ces derniers poursuivent différentes finalités de traitement[878].

431. Le caractère spécifique du consentement « vise à garantir un certain de degré de contrôle utilisateur et de transparence pour la personne concernée »[879]. Le caractère spécifique du

---

[875] CJUE, C-61/19, *op. cit.*, §38.
[876] CNIL, Décision MED 2019-035 du 31 décembre 2019 mettant en demeure la société ÉLECTRICITÉ DE France (EDF).
[877] CNIL, Décision MED 2019-035 du 31 décembre 2019, *op. cit.*
[878] Datatilsynet, 11 février 2020, 2018-32-0357, résumé disponible sur GDPRHub, *Datatilsynet – 2018-32-0357*, disponible sur gdprhub.eu (résumé en anglais). L'original est disponible sur le site de l'autorité de protection des données danoise : https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/feb/dmis-behandling-af-personoplysninger-om-hjemmesidebesoegende/ (en danois).
[879] Groupe de travail « Article 29 », WP259 rév.01, *op. cit.*.

consentement a pour objectif d'interdire aux responsables de traitement de proposer des choix « à prendre ou à laisser », voire des choix de « tout ou rien » à la personne concernée en ce qui concerne la protection de ses données à caractère personnel. Ainsi, la personne concernée pourra vouloir autoriser le responsable de traitement à traiter ses données à caractère personnel pour que ce dernier puisse mesurer les performances de son site internet, tout en refusant que ces mêmes données puissent être utilisées pour des fins commerciales. L'augmentation du degré de contrôle sera renforcée par l'obligation qui en découle de fournir une information spécifique à la finalité de traitement considérée : la personne concernée sera ainsi « consciente de l'impact des différents choix qui lui sont offerts »[880].

432. Le caractère spécifique du consentement permet également à la personne concernée de savoir exactement à quoi elle s'engage. Dans l'affaire TCF, l'APD avait considéré que le *Consent Management Platform* (CMP) utilisé dans le cadre du *Transparency & Consent Framework* ne permettait pas aux personnes concernées « d'identifier de manière simple et claire les finalités de traitement associées à l'autorisation d'un fournisseur adtech particulier ou d'identifier les fournisseurs adtech qui traiteront leurs données pour une finalité spécifique »[881]. Le président de la Chambre contentieuse de l'APD a par la suite insisté sur l'importance de la jurisprudence TCF, qui met fin à une pratique dans laquelle « les utilisateurs sont invités à donner leur consentement alors que la plupart d'entre eux ne savent pas que leur profil est vendu à maintes reprises chaque jour afin de leur montrer des publicités ciblées »[882].

433. Le consentement spécifique est également étroitement lié à l'obligation de limitation des finalités de traitement prévu à l'article 5(1)(b) du RGPD. L'obligation de spécifier l'ensemble des finalités du traitement lors de la demande du consentement va ainsi permettre à la personne concernée de se protéger en contrôlant si ses données à caractère personnel ont fait l'objet d'un détournement des finalités du traitement. Ainsi, selon le Comité européen de la Protection des Données (EDPB),

> « The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in

[880] EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/579*, *op. cit.*, p. 15.
[881] APD, 2 février 2022, *Décision sur le fond 21/2022*, p. 105.
[882] APD, « L'APD remet de l'ordre dans l'industrie de la publicité en ligne : IAB Europe est tenue responsable d'un mécanisme qui viole le RGPD », 2 février 2022, disponible sur https://www.autoriteprotectiondonnees.be/professionnel/iab-europe-est-tenue-responsable-d-un-mecanisme-qui-viole-le-rgpd (consulté en août 2022).

unanticipated use of personal data by the controller or by third parties and in loss of data subject control »[883].

434. Ainsi, l'obligation d'obtenir un consentement spécifique joue un rôle important en matière de protection du choix de la personne concernée puisque cette obligation garantit à la fois l'obtention d'un consentement éclairé (la personne concernée sait à quoi elle s'engage), d'un consentement libre (la personne choisit à quoi elle s'engage) et permet également à la personne concernée de disposer d'un pouvoir de contrôle sur les finalités pour lesquelles ses données à caractère personnel sont collectées.

435. Une exception a été cependant insérée par le RGPD en matière de recherche scientifique. Le considérant 33 du RGPD cherche à concilier la nature de la recherche scientifique avec le respect des droits fondamentaux de la personne concernée et sa capacité à donner un consentement valide. De manière pragmatique, le législateur européen remarque que la recherche scientifique, du fait de son caractère expérimental, peut rencontrer des difficultés à définir de manière précise et définitive la finalité du traitement de données à caractère personnel envisagé. Dans cette situation « les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique ». Le RGPD ne donne cependant pas plus de précisions sur la nature et l'identification des normes éthiques. Cette absence de précision peut s'expliquer par la volonté du législateur de ne pas figer le temps les dispositions du RGPD afin de permettre l'évolution de la norme relative au consentement dans la recherche scientifique en même temps que l'évolution des normes éthiques en matière scientifique. De telles normes pourraient par exemple désigner pour les banques génétiques la Convention d'Ovedio, la Déclaration d'Helsinki ou encore la Déclaration de Taipei[884].

436. Le considérant 33 ne doit pas s'interpréter comme une dérogation accordée à chaque projet de recherche scientifique, mais comme une exception au consentement spécifique « dans les cas où les finalités du traitement de données dans le cadre d'un projet scientifique ne peuvent pas être précisées d'entrée de jeu »[885]. L'absence de spécificité du consentement doit être compensée par le responsable de traitement non seulement par le respect de normes éthiques en matière scientifique, mais également par une obligation d'information sur l'ensemble des

[883] EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/579, op. cit.,*, p. 14.
[884] STAUTON Ciara, SLOKENBERGA Santa, MASCALZONI Deborah, « The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks », *European Journal of Human Genetics*, 2019, pp. 1159-1167.
[885] EDPB, *Lignes directrices 5/2020, op. cit.,* pp. 35-36.

éléments pouvant éclairer au mieux la personne concernée, parmi lesquels l'expression de la finalité en des termes plus généraux, la fourniture des étapes du projet de recherches connues à l'avance, la communication régulière d'informations sur l'évolution de la finalité avec le temps, ou encore l'ouverture à consultation du plan de recherche exhaustif défini à l'avance[886].

437. Par conséquent, le consentement spécifique permet de garantir à la personne concernée qu'elle consent à un traitement de données à caractère personnel déterminé, selon un choix granulaire en fonction des finalités du traitement. Par exemple, une personne concernée qui visite un site internet peut accepter le traitement de ses données à caractère personnel à des fins d'analyse des visites du site internet par le responsable de traitement, mais refuser le traitement de ses données à caractère personnel à des fins de publicité comportementale. Le consentement spécifique prévient ainsi les influences manipulatrices du consentement à travers la manœuvre du « tout ou rien » quant à l'acceptation des traitements de données à caractère personnel. La liberté du consentement est également protégée de manipulations techniques du consentement à travers l'obligation d'obtenir un consentement univoque.

§2 – Un consentement univoque

438. En plus du fait de savoir à quoi la personne concernée consent, le législateur européen a également souhaité garantir que la personne concernée soit consciente, au moment où elle donne son consentement, qu'elle est en train de consentir à un traitement de données à caractère personnel. L'exigence d'obtenir un consentement univoque s'attache non plus au contenu et aux circonstances du consentement, mais à la forme de l'acte de consentir. Ainsi, l'exigence d'un consentement univoque qui se traduit par un acte positif clair est peut-être le renforcement du consentement le plus visible du RGPD.

439. En effet, la nécessité d'un acte positif exprimant le consentement a marqué la fin de toute une série de pratiques diverses telles que le consentement implicite ou encore l'usage de cases précochées. Cette obligation est créée par l'article 4 (11) du RGPD définissant le consentement : ce dernier est ainsi défini comme une manifestation de volonté « univoque par laquelle la personne concernée accepte, par une déclaration ou un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Le considérant 32 précise que cet acte positif clair peut résulter par exemple « d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale ». Ainsi, le Règlement est plus exigeant que la Directive qui se contentait d'exiger que la personne concernée ait

[886] *Idem*, p. 37.

« indubitablement » donné son consentement[887] : tout au plus, la Directive exigeait un consentement « explicite » pour le traitement de données sensibles[888]. Si le Groupe « Article 29 » avait précisé que le consentement ne devait « laisser *aucun doute* quant à l'intention de la personne concernée de donner son consentement »[889], le consentement pouvait encore résulter d'un « consentement explicite clair »[890].

440. Le Groupe « Article 29 » recense différentes situations désormais interdites par le RGPD : les cases cochées par défaut, le silence ou l'inactivité de la personne concernée ou encore le fait que la personne concernée continue à utiliser un service ne peuvent plus constituer un consentement valide au sens du Règlement[891]. De même, ne constitue pas un consentement valide au sens du RGPD le fait qu'un responsable de traitement exige un acte positif de refus de traitement de données à caractère personnel (cases ou formulaires de refus par exemple)[892]. La nécessité d'un acte positif clair rejoint également l'exigence d'un consentement spécifique puisque le Groupe « Article 29 » précise qu'un « responsable de traitement doit également être conscient que le consentement ne peut être obtenu moyennant la même action que lorsqu'une personne concernée accepte un contrat ou les conditions d'un service »[893].

441. Les autorités de contrôle ont rapidement eu l'occasion de sanctionner l'inexistence d'un acte positif clair exprimant le consentement de la personne concernée. En 2019, l'autorité de contrôle néerlandaise, à la suite d'une enquête menée sur cent soixante-quinze sites internet, conclut que quatre-vingt-sept d'entre eux ne respectent pas avec les dispositions du RGPD lorsqu'ils placent des cookies sur le terminal de l'utilisateur[894]. L'autorité de contrôle en profite pour insister sur le fait que les cases précochées, le silence, l'inactivité de la personne concernée ou encore le fait qu'elle déroule une page internet ne peuvent pas constituer un consentement valide[895]. Face à l'obtention d'un consentement par inaction de la personne concernée,

---

[887] Directive 95/46/CE, 24 octobre 1995, Article 7 (a).
[888] Directive 95/46/CE, 24 octobre 1995, Article 8 (2) (a).
[889] Groupe de travail « Article 29 », WP 187, *op. cit.*, p. 23.
[890] *Ibidem.*
[891] Groupe de travail « Article 29 », WP259 rév.01, *op. cit.*, p. 18.
[892] *Idem*, p. 19.
[893] *Ibidem.*
[894] GDPRHub, *AP-Consent to place cookies*, disponible sur gdprhub.eu (résumé en anglais). L'original est disponible sur le site internet de l'autorité de contrôle néerlandaise : AP, « AP: veel websites vragen op onjuiste wijze toestemming voor plaatsen tracking cookies », 10 décembre 2019, disponible sur https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op-onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies (en néerlandais).
[895] *Ibidem.*

l'autorité de contrôle espagnole (AEPD)[896] et l'autorité de contrôle roumaine (ANSPDCP)[897] ont condamné l'utilisation de case à cocher pour exercer un *opt-out*. En France, c'est notamment la société Google LLC qui a fait l'objet d'une condamnation de la CNIL[898], confirmée par le Conseil d'État[899], en raison de l'utilisation de cases précochées pour influencer l'obtention du consentement en matière de ciblage publicitaire.

442. La Cour de Justice de l'Union européenne a eu aussi l'occasion de se prononcer à deux reprises sur la nécessité d'un acte positif clair. Dans son arrêt Planet49, la Cour lie la nécessité d'un acte positif clair au fait que la directive 95/46 exige que le consentement soit « indubitablement » donné par la personne concernée. Elle en déduit immédiatement l'interdiction des cases cochées par défaut :

> « À cet égard, il apparaît pratiquement impossible de déterminer de manière objective si l'utilisateur d'un site Internet a effectivement donné son consentement au traitement de ses données personnelles en ne décochant pas une case cochée par défaut ainsi que, en tout état de cause, si ce consentement a été donné de manière informée. En effet, il ne peut pas être exclu que ledit utilisateur n'ait pas lu l'infirmation accompagnant la case cochée par défaut, voire qu'il n'ait pas aperçu cette case, avant de poursuivre son activité sur le site Internet qu'il visite »[900].

443. Dans son arrêt Orange România, la CJUE confirme sa position à propos des cases cochées par défaut, en l'appliquant au cas de cases cochées par défaut au sein d'un contrat : « la circonstance selon laquelle lesdits clients ont signé les contrats contenant la case cochée ne permet pas, à elle seule, d'établir un tel consentement [une manifestation positive du consentement], en l'absence d'indications confirmant que cette clause a été également lue et assimilée »[901].

444. L'obligation d'obtenir un acte positif clair laisse cependant la liberté au responsable de traitement de choisir le mécanisme de recueil du consentement qu'il souhaite utiliser. Ainsi, le consentement peut revêtir par exemple la forme d'une déclaration écrite, d'une déclaration

---

[896] AEPD, PS-00187-2019, publiée le 25 février 2020, résumé disponible sur GDPRHub, *AEPD, PS/00187/2019*, disponible sur gdprhub.eu (résumé en anglais). L'original est disponible sur le site internet de l'autorité de contrôle espagnole : https://www.aepd.es/es/documento/ps-00187-2019.pdf (en espagnol).
« *Así las cosas, los hechos conocidos podrían ser constitutivos de una infracción,imputable al reclamado, por vulneración del artículo 7 del RGPD mencionado, alrealizar la recogida del consentimiento mediante una acción no afirmativa, unainacción que no asegura que el interesado otorga inequívocamente el consentimiento* ». AEPD, PS-00134-2020, publiée le 23 juillet 2020.
[897] ANSPDCP, « Another sanction for the violation of GDPR », *dataprotection.ro*, 22/08/2020, disponible sur https://www.dataprotection.ro/index.jsp?page=Alta_sanctiune_RGPD&lang=en
[898] CNIL, Délibération de la formation restreinte no SAN-2020-012 du 7 décembre 2020 concernant les sociétés Google LLC et Google Ireland Limited.
[899] CE, n°430810, *op. cit.* .
[900] CJUE, C-673/17, *op. cit.*, §55.
[901] CJUE, C-61/19, *op. cit.* §46.

orale, d'un comportement, etc. Ainsi, la validité du consentement en raison de son caractère univoque dépendra de deux critères : l'absence d'ambiguïté du consentement et la nature des données à caractère personnel concernées.

445. Le critère de l'absence d'ambiguïté avait déjà été étudié par le Groupe « Article 29 » sous le régime de la directive 95/46/CE. En effet, le G29 avait déduit du caractère indubitable du consentement que l'accord de la personne concernée ne devait « laisser aucune ambiguïté quant à son intention »[902], concluant de manière pédagogique que « s'il existe un doute raisonnable sur l'intention de la personne concernée, il y a ambiguïté »[903]. Ce critère de l'absence d'ambiguïté est repris par l'EDPB dans ses lignes directrices relatives au consentement[904]. Cependant, le Comité ajoute que, pour pouvoir considérer qu'il y a absence d'ambiguïté, le responsable de traitement doit « veiller à ce que l'acte par lequel le consentement est accordé puisse se distinguer de tout autre acte »[905]. Le critère d'absence d'ambiguïté est particulièrement intéressant à deux égards. Premièrement, il renforce l'obligation d'obtenir un consentement spécifique, puisqu'il insiste une fois de plus sur l'impossibilité d'obtenir un consentement au traitement des données à caractère personnel par la simple acceptation, par exemple, de conditions générales[906]. À cet égard, le comité précise que même si le considérant 32 du RGPD précise que la demande de consentement par voie électronique « ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé »[907], il peut néanmoins être nécessaire, afin de lever l'ambiguïté du consentement, que la « demande de consentement interrompe l'expérience d'utilisation jusqu'à un certain point afin que cette demande soit effective »[908]. Il reviendra dès lors au responsable de traitement de déterminer la méthode de demande de consentement la moins ambiguë, en prenant en compte de limiter au maximum les interruptions dans l'expérience de l'utilisateur. Deuxièmement, ce critère présente une importance particulière pour vérifier si un comportement est suffisamment univoque pour constituer un consentement valide. Pour expliquer ce critère, l'EDPB présente l'exemple d'un consentement qui peut résulter de manière valide du fait d'agiter la main devant une caméra intelligente à la condition que « des informations claires soient fournies et qu'il soit

[902] Groupe de travail « Article 29 », WP 187, *op. cit.*, p. 23.
[903] *Ibidem.*
[904] EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/*679, *op. cit.*, p. 22.
[905] *Ibidem.*
[906] Ce qui est rappelé par l'EDPB dans ses lignes directrices. Voir *Idem*, p. 21.
[907] RGPD, 27 avril 2016, considérant 32.
[908] EDPB, *Lignes directrices 5/2020*, *op. cit.*, p. 22.

clair que le mouvement en question signifie que la personne concernée accepte une demande spécifique »[909].

446. Dès lors, le consentement univoque permet à la personne concernée de savoir qu'elle est en train de consentir à un traitement de données à caractère personnel, puisque ce consentement relèvera d'une action de sa part. Le consentement RGPD protège aussi la personne concernée de méthodes manipulatrices en vue d'obtenir un consentement. Par exemple, contrairement à la directive 95/46/CE, les cases précochées constituent une pratique interdite, le consentement résultant de cette pratique relevant aujourd'hui de l'illégal quand il pouvait relever sous la directive d'un manque d'attention ou de prudence de la personne concernée.

447. Le législateur européen a également souhaité protéger la personne concernée de certains traitements sensibles en exigeant un consentement explicite. Plus stricte que le consentement univoque, l'exigence d'un consentement explicite nécessite une action de la part de la personne concernée qui s'inscrit sur un temps plus long que le consentement univoque. L'EDPB interprète la notion de consentement explicite comme impliquant « que la personne concernée doit formuler une déclaration de consentement exprès »[910], lequel peut résulter en une déclaration signée, le remplissage d'un formulaire, l'envoi d'un email ou encore le recours à une signature électronique. Dans le RGPD, le consentement explicite est requis en ce qui concerne le consentement aux traitements de certaines catégories particulières de données (les données dites « sensibles »)[911], le consentement aux traitements automatisés et notamment au « profilage »[912], et le consentement aux transferts de données à caractère personnel hors Union européenne[913]. L'exigence d'un consentement explicite sort de la logique de simple protection de la personne concernée contre des pratiques du responsable de traitement. En temporisant le consentement, le RGPD offre à la personne concernée un moment, aussi bref soit-il, entre l'information et l'acte de consentir.

448. Ainsi, en s'intéressant à la forme du consentement, le législateur européen a permis de protéger la liberté de consentement de la personne concernée qui, par l'exigence d'une action de consentir, sait qu'elle consent au traitement de ses données à caractère personnel. La forme du consentement se décline d'ailleurs en consentement univoque pour les traitements de

---

[909] *Ibidem.*
[910] *Ibidem.*
[911] RGPD, 27 avril 2016, considérant 51, Article 9(2)(a).
[912] RGPD, 27 avril 2016, considérant 71, Article 22(2)(c).
[913] RGPD, 27 avril 2016, considérant 111, Article 49(1)(a).

données à caractère personnel ordinaires et en consentement explicite pour les traitements de données à caractère personnel particulièrement sensibles. Cette déclinaison permet de temporiser le consentement à deux niveaux de protection différents. La temporisation du consentement dans le cadre du consentement univoque permet de mettre en valeur l'acte de consentir ; la temporisation du consentement explicite permet de créer un moment de réflexion entre la réception de l'action et l'acte de consentir.

449. Conclusion de section. – Le RGPD identifie l'objet et l'acte associé au consentement. La personne concernée, consciente de son acte de consentir, peut consentir au traitement de ses données à caractère personnel de manière granulaire, selon les finalités de traitement proposées par le responsable de traitement. La liberté de consentement de la personne concernée est ainsi garantie puisque le législateur européen s'est assuré que le consentement corresponde à une manifestation (par l'action) de la volonté (par le choix) de la personne concernée.

Conclusion du Chapitre 2

450. Le chapitre précédent s'était efforcé de démontrer que le consentement, pour être libre, devait être isolé de contraintes externes susceptibles d'influencer le consentement au-delà de ce qui était acceptable au regard de l'autonomie de la personne concernée. Le chapitre présent s'est quant à lui efforcé de démontrer que le consentement doit également être clairement délimité de manière spatio-temporelle pour que la manifestation de volonté de la personne concernée corresponde effectivement au consentement au traitement de ses données à caractère personnel. En effet, une manifestation de volonté n'est ni illimitée dans le temps, ni dans son objet.

451. La question des limites temporelles est doublement encadrée par le principe de limitation de conservation des données à caractère personnel et le droit accordé à la personne concernée de retirer son consentement. Il a ainsi été démontré que les limites temporelles passives, les durées de conservation des données à caractère personnel, souffrent d'un manque de transparence et de standardisation qui ont pour conséquence d'une part, la complexification de la mise en œuvre du principe pour le responsable de traitement, et d'autre part, l'absence d'une prise de conscience collective qui aurait pu aboutir à une définition plus harmonisée des attentes raisonnables de la personne concernée en matière de conservation de ses données à caractère personnel. L'octroi d'un droit au retrait de son consentement permet cependant à la personne concernée d'activement traduire ses attentes raisonnables sur un traitement de données à caractère personnel précis, sans qu'il s'agisse d'une solution compensant de manière satisfaisante les lacunes du principe de limitation de conservation des données. Néanmoins, le droit au retrait de son consentement satisfait complètement son objectif premier : faire correspondre la durée du consentement de la personne concernée avec la durée du traitement de données à caractère personnel.

452. La question des limites spatiales est également doublement encadrée dans le RGPD par l'exigence d'un consentement spécifique et d'un consentement univoque, la première exigence délimitant l'objet du consentement et la seconde l'acte de consentir. Ainsi, la personne concernée est maître de son consentement. Le consentement spécifique lui permet en effet d'opérer un choix granulaire au niveau de la finalité et non du responsable de traitement, prévenant les effets de verrouillages de « tout ou rien » si souvent dénoncés sous l'égide de la directive 95/46/CE. Le consentement univoque permet quant à lui de mettre en exergue l'acte

de consentir, afin d'éliminer les risques de consentement par accident, négligence ou manipulation du responsable de traitement.

453. Proposer un choix aux contours trop vagues ou trop généraux est ainsi susceptible de corrompre le consentement de la personne concernée, se sentant « obligée » d'accepter ou refuser un traitement pour des critères externes à la réalité de ce traitement. Délimiter l'objet et la forme du consentement permet de prendre en compte le fait que la manifestation de volonté porte sur un objet spécifique, dont la granularité peut varier selon la personne concernée.

Conclusion du Titre 2

454. La liberté du consentement se caractérise par l'absence de contrainte exercée sur la personne concernée, susceptible de corrompre son consentement. Ainsi, la liberté du consentement nécessite un effort du législateur visant à prévenir les contraintes externes à l'exercice du consentement, et à garantir une adéquation acceptable entre la manifestation de la volonté de la personne concernée et l'exercice de son consentement.

455. La prévention des contraintes externes est une question souvent adressée en droit concernant la liberté du consentement, à l'image du droit civil français invalidant le consentement donné sous l'emprise de la violence, du dol ou de l'erreur. En matière de protection des données à caractère personnel, le législateur européen a reconnu la position défavorable de la personne concernée par rapport au responsable de traitement, que cette position soit économique ou hiérarchique. Dès lors, le pouvoir de négociation de la personne concernée est conservé soit à travers l'isolation vis-à-vis de biens et services, soit à travers l'interdiction du recours au consentement en cas de déséquilibre manifeste. Dans l'ensemble de ces situations, le RGPD concilie l'*empowerment* de la personne concernée et la réalité de la relation entre la personne concernée et le responsable de traitement. Dès lors, si le déséquilibre est acceptable, la personne concernée est réputée avoir le contrôle de ses données à caractère personnel. Dans le cas inverse, les données à caractère personnel relèveront de la logique protectrice du règlement.

456. La délimitation du consentement dans son objet et sa forme relève d'une spécificité de la protection des données à caractère personnel. En effet, le droit des contrats consacrant le principe de l'égalité des cocontractants, le consentement ne pourra être invalidé qu'en cas de manœuvre frauduleuse de l'un des cocontractants. La protection des données à caractère personnel se rapproche ainsi plus de régimes protecteurs tels que le droit de la consommation ou le droit du travail. Si l'autonomie de la personne concernée est bel et bien consacrée, cette autonomie est accompagnée de garanties quant aux contours de leur consentement. Ainsi, la personne concernée consent de manière consciente et active, à un objet déterminé, et pour une durée limitée.

457. La liberté du consentement est ainsi particulièrement renforcée par le RGPD tant ses dispositions semblent répondre aux dérives observées sous le régime de la directive 95/46/CE.

Conclusion de la Partie 1

458. L'observation des pratiques usuelles sous le régime de la directive a fait naître une réflexion sur la nécessité d'adapter le régime de protection des données à caractère personnel aux pratiques et technologies modernes. Cette adaptation s'est traduite non seulement par l'élargissement du champ d'application du règlement aux nouvelles technologies, mais également par la prise en compte par le règlement des nouveaux rapports entre personnes concernées et responsables de traitement. La complexité héritée des évolutions technologiques a rendu les traitements de données à caractère personnel opaques et difficiles à comprendre. En réaction, le législateur européen a érigé le principe de transparence en principe central du RGPD. La mondialisation et l'apparition d'acteurs hégémoniques ont créé un espace numérique dans lequel la personne concernée possède peu de pouvoir de négociation. En réaction, le législateur européen a créé des critères de validité supplémentaires du consentement afin de protéger la liberté de la personne concernée. L'étude a ainsi démontré à mi-chemin que les efforts du législateur ont permis un renforcement du consentement par rapport à la directive 95/46/CE, dont les effets semblent prévenir les dérives identifiées sous l'égide de la directive.

459. Dans un premier temps, l'étude a montré que l'élévation de la transparence en principe central du cadre de la protection des données à caractère personnel a permis un renforcement substantiel du caractère éclairé du consentement. Le double prisme de l'accessibilité et de l'exhaustivité de l'information permet de prendre en compte l'opacité des traitements de données à caractère personnel pour les personnes concernées. Certaines nuances sont cependant à apporter puisque le RGPD ne prend pas en compte suffisamment les circonstances technico-économiques relatives à la délivrance de l'information, la situation des personnes vulnérables ou encore la capacité de la personne concernée de se saisir du volume d'information qui lui est délivrée.

460. Dans un second temps, l'étude s'est attachée à démontrer que le RGPD a aussi contribué au renforcement du caractère libre du consentement à travers les exigences de consentement explicite et univoque, le principe de limitation de la conservation des données et le droit au retrait du consentement. Ce constat n'est pas non plus dressé sans nuance puisque certaines notions telles que le « préjudice » ou le « déséquilibre manifeste » restent encore à éclaircir. En effet, l'interprétation de ces notions ne permet pas encore d'assurer la sécurité juridique des responsables de traitement dans la mise en œuvre de celles-ci et révèle le malaise voire la

mauvaise compréhension de certains enjeux attachés à la protection des données à caractère personnel.

461. La première étape a ainsi démontré que les efforts du législateur ont porté théoriquement porté leur fruit en matière de protection des données à caractère personnel, même s'il est regrettable que certains enjeux aient été volontairement ou non mis de côté ou adressés de manière incomplète. Les nuances attachées aux efforts du législateur européen en matière de consentement sont cependant plus larges que la simple interprétation des dispositions du règlement. Pour dresser un tableau fidèle de la place du consentement dans le RGPD, il semble dès lors nécessaire de prendre en compte l'ensemble des circonstances relatives aux traitements des données à caractère personnel, qu'il s'agisse de leur pratique, leur réception, leur cadre, etc.

PARTIE 2 – LES LIMITES DU CONSENTEMENT

462. Si le consentement a en effet été renforcé par le RGPD, l'adéquation de ce mécanisme avec la protection des données à caractère personnel ne fait pas l'unanimité auprès de la doctrine française, dont une partie appelle à « en finir avec le dogme du consentement »[914], dénonce « les dérives actuelles du consentement en matière de protection des données »[915], ou encore qualifie le consentement RGPD de « mythe »[916]. Le consentement souffre en effet du paradoxe d'être défendu au nom de la liberté et de l'autonomie et d'être accusé de fragiliser ces mêmes notions en ne prenant pas suffisamment en compte les asymétries dans les rapports de force[917]. Le consentement n'est ainsi pas envisagé sous le même prisme que le consentement contractuel puisque la personne concernée est réputée être en position de faiblesse par rapport au responsable de traitement. Les défauts du consentement sont donc analysés dans un champ d'études plus large que la protection juridique contre les vices du consentement. Reprenons par exemple les termes de Geneviève Fraisse, philosophe, pour qui « par-delà les vices du consentement, les défauts révèlent la négativité possible du consentement : acte de soumission, attitude de renoncement ; toute adhésion n'est pas enthousiasmante »[918]. À travers ces critiques se dessinent les limites de l'autonomie de la volonté dans le contexte numérique, à la fois dans sa dimension de capacité de la personne concernée que dans sa dimension d'individualité dans l'environnement digital.

463. L'omniprésence du consentement dans le paysage juridique contemporain est le résultat des réflexions visant à placer l'autonomie de la volonté au cœur du système juridique. Cette consécration de l'autonomie de la volonté provient notamment du Code civil de 1804, dont la maxime « qui dit contractuel dit juste »[919] irrigue encore aujourd'hui le droit des contrats. Le postulat découle d'une logique désormais bien huilée : les individus étant libres, égaux et

---

914 AULAS Adrien, « Faut-il en finir avec le dogme du consentement ? », 15 avril 2019, disponible sur https://aeonlaw.eu/faut-il-en-finir-avec-le-dogme-du-consentement/ (consulté en avril 2021).
915 DEBAETS Émilie, *op. cit.*, p. 346.
916 MATTATIA Fabrice, *op. cit.*, p. 2121 ; TCHIDER Charlotte A., « The Consent Myth: Improving Choice for Patients of the Future", 96 *Wash. U. L. Rev.*, 2018-2019, p. 1505.
917 COSTE Florent, COSTEY Paul, TANGY Lucie, « Consentir : domination, consentement et déni », *Tracés. Revue de Sciences humaines*, n°14, 2008, disponible sur https://journals.openedition.org/traces/365#quotation (consulté en avril 2021).
918 FRAISSE Geneviève, *Du consentement,* Paris, Éditions du Seuil, édition augmentée, 2007, p. 49.
919 MAUME Florian, *Essai critique sur la protection du consentement de la partie faible en matière contractuelle*, Thèse pour l'obtention du grade de docteur en droit sous la direction de HOUTCIEFF Dimitri, Université d'Evry Val d'Essonne, 2015, p. 6.

capables de défendre leurs propres intérêts, « les règles auxquelles ils consentent sont les mieux à même d'assurer le bien-être de tous, l'intérêt général n'étant que la sommation des intérêts particuliers »[920]. Le consentement permet d'exprimer la volonté d'un « sujet individuel pour lequel la possession de soi est la seule propriété naturelle »[921]. Les limites du consentement ne doivent donc pas, dans cette optique, s'interpréter comme une opposition à la place du consentement dans le système juridique ou même dans la protection des données à caractère personnel. Au contraire, l'étude a pour objectif l'étude des limites du consentement afin de déterminer comment en assurer la pertinence et la réalité, afin que la notion de consentement soit « capable de porter les ambitions qu'on lui prête »[922].

464. Le cadre légal entourant le consentement a pour objectif d'outrepasser les obstacles à la réalité du consentement et de réaliser enfin les ambitions portées par la notion. La réflexion du législateur porte sur la nature et la portée des interférences excluant la réalité du consentement afin de déterminer les conditions qui excluent ou attestent de la validité du consentement[923]. L'intervention législative est globalement acceptée lorsqu'elle a pour objectif de protéger la partie faible[924], que cette faiblesse relève des limites de l'objet du consentement ou des faiblesses propres au consentant. Elle se traduit par l'identification des vices du consentement – classiquement, l'erreur, la contrainte et le dol – mais également par la fixation de qualités attachées au consentement – classiquement, libre et éclairé.

465. Traduction de la pensée libérale dans la majorité de l'occident[925], le consentement a pour objectif de garantir l'autonomie individuelle à travers l'autonomie de la volonté des individus. Si le consentement est parfois considéré comme un acte de soumission ou de résignation, il s'agit également d'un acte permettant à l'individu de communiquer la permission et d'exercer ses droits[926]. La notion permet au législateur de mettre l'emphase sur la liberté, en rejetant l'intervention de l'État concernant les choix qui se rapportent à l'individu au profit de

---

[920] ROLLAND Louise, « Qui dit contractuel, dit juste. » (Fouillée) … en trois petits bonds, à reculons », *McGill Law Journal*, vol. 5, 2006, pp. 768-769.
[921] JAUNET Alexandre, MATONTI Frédérique, « L'enjeu du consentement », *Raisons politiques*, 2012, n°46, p. 5.
[922] HUM Pierre *et al.*, « Le refus de soin : forces et faiblesses du consentement », *Éthique et Santé,* Volume 12, Issue 1, mars 2015, p. 56.
[923] GILLET Jean-Louis, « À la recherche du consentement perdu », *Les Cahiers de la Justice*, 2021, p. 659.
[924] GIRER Marion, « À la recherche du juste consentement en matière de soins », *Les Cahiers de la Justice*, 2021, p. 635.
[925] GUILLOUD Olivier, « Le consentement dans tous ses états », *in* Association française de droit de la santé (dir.), *Consentement et santé*, Paris, Dalloz, p. 1.
[926] KLEINING John, « The Nature of Consent », *in* MILLER Franklin, WERHEIMER Alan (dir.), *The Ethics of Consent: Theory and Practice*, Oxford University Press, 2010, p. 19.

ce dernier[927]. Le consentement est dès lors lié à de nombreux concepts centraux de la société tels que la liberté, la dignité, l'intégrité, l'indépendance ou encore la responsabilité[928]. La recherche de sa validité constitue également une protection contre des phénomènes jugés non souhaitables dans la société telles que la tromperie, la manipulation ou la coercition[929].

466. L'autonomie individuelle peut être analysée du point de vue de l'agent ou de l'action. Du point de vue de l'agent, l'autonomie se comprend comme la capacité d'agir d'une personne compétente et indépendante[930] : il s'agit de l'aptitude de l'individu à prendre les décisions qui le concernent. Du point de vue de l'action, l'autonomie se comprend comme la capacité pour l'agent de prendre une décision déterminée dans un contexte donné : ce point de vue permet de constater que même autonomes, les personnes peuvent échouer à prendre des décisions de manière autonome du fait de circonstances particulières[931]. Appliquée au consentement en matière de protection des données, l'autonomie de l'agent entraîne comme conséquence que le consentement ne doit être demandé à la personne concernée que dans les situations dans lesquelles l'objet du consentement lui permet d'exercer un choix du fait de sa capacité et de son indépendance. L'autonomie de l'action nécessite quant à elle une réflexion plus circonstanciée dont l'objectif est d'identifier les situations dans lesquelles la personne concernée, normalement capable d'exercer son consentement en toute autonomie, perd sa capacité en raison de circonstances particulières. Le RGPD présente des limites pour chacune des acceptions de l'autonomie individuelle. D'une part, l'autonomie de l'agent peut être mieux protégée par une meilleure identification des situations d'adéquation et d'inadéquation du consentement à un traitement de données à caractère personnel (Titre 1). D'autre part, l'autonomie de l'action nécessite une contextualisation plus avancée de la situation de la personne concernée lorsqu'elle exerce son consentement à un traitement (Titre 2).

---

[927] MCLEAN Sheila A. M., *Autonomy, Consent and the Law*, Routledge, 2010, p. 1.
[928] O'NEIL Onora, « Some limits of Informed Consent », *Journal of Medical Ethics*, 2003, n°29, p. 5.
[929] BEAUCHAMP Tom L., « Autonomy and Consent », *in* MILLER Franklin, WERHEIMER Alan (dir.), *The Ethics of Consent: Theory and Practice*, Oxford University Press, 2010, p. 60.
[930] *Idem*, p. 61.
[931] *Ibidem.*

TITRE 1 – LA PERTINENCE DU CONSENTEMENT VIS-À-VIS DE CERTAINS TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

467. La validité du consentement dépend de plusieurs qualités que lui octroie le RGPD : le consentement doit être éclairé, libre, spécifique, univoque, temporaire. Dès lors, le consentement ne peut pas constituer la base unique de fondement des traitements de données à caractère personnel puisque de nombreux traitements ne permettront pas au responsable de traitement de garantir la manifestation de l'autonomie de la volonté en raison des caractéristiques du traitement des données à caractère personnel (par exemple, un traitement obligatoire selon la loi), ou de la nature du responsable de traitement (par exemple, un employeur).

468. Ne pas fonder le traitement de données à caractère personnel sur le consentement ne signifie pas pour autant sacrifier l'autonomie de la personne concernée ni même la protection de ses données à caractère personnel. Les données à caractère personnel peuvent être traitées à travers d'autres formes d'expression de l'autonomie individuelle comme le consentement contractuel ou encore la possibilité d'*opt-out* pour certains traitements fondés sur les intérêts légitimes du responsable de traitement. Dans d'autres situations, les données à caractère personnel sont collectées lors de situations relevant soit de la protection de la personne concernée (la sauvegarde des intérêts vitaux de la personne concernée), soit de l'intérêt général (à travers, le respect d'obligations légales ou l'exécution d'une mission d'intérêt public). Dans l'ensemble de ces situations, la personne concernée sera tout de même protégée par de nombreuses dispositions, parmi lesquelles les principes relatifs au traitement des données à caractère personnel[932]. Ces principes guidés par les principes de nécessité et de proportionnalité visent à concilier les intérêts des responsables de traitement avec la protection des droits fondamentaux de la personne concernée[933].

469. Dès lors, la base légale du consentement doit être réservée à des situations permettant à la personne concernée d'exercer son consentement de manière libre et éclairée. La personne concernée ne devrait pouvoir exercer son consentement que dans des situations où elle est capable de comprendre les frontières et les enjeux du traitement à caractère personnel auquel il

[932] RGPD, 27 avril 2016, Article 5.

[933] Cette philosophie est annoncée par le considérant 4 du RGPD qui dispose : « Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité ».

lui est proposé de consentir (Chapitre 1). De plus, le choix de la base légale sur laquelle est fondé le consentement doit faire l'objet d'une réflexion mûre sur la capacité de la personne à consentir et le respect du principe de proportionnalité plutôt que d'un choix d'opportunité (Chapitre 2).

CHAPITRE 1 – LA COMPLEXITÉ INADÉQUATE DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

470. Dès l'adoption du RGPD, la question du consentement a fait tellement de bruit que de nombreuses mises en garde ont été publiées, appelant les responsables de traitement à respecter le texte et ne pas faire du consentement une base légale par défaut[934]. La présentation du consentement publiée par la CNIL sur son site internet illustre bien ce mouvement, l'autorité de contrôle française alertant sur la nécessité de vérifier que le consentement des personnes peut être recueilli avant même d'étudier les critères de validité du consentement[935]. Ainsi, le RGPD requiert du responsable de traitement une précaution particulière en matière de consentement. Le responsable de traitement doit repérer les traitements pour lesquels le recours au consentement est non seulement autorisé, mais également approprié, c'est-à-dire les traitements permettant au responsable de traitement de respecter, tout au long l'ensemble des conditions permettant à la personne concernée d'émettre un consentement valide.

471. Dès lors, alors même que le responsable de traitement est *a priori* autorisé à fonder son traitement sur le consentement, il faudra vérifier si les conditions du traitement permettent à la personne concernée d'exercer un consentement éclairé au sens des articles 4(11) et 7 du RGPD. Le caractère éclairé du consentement, dont le prérequis est la capacité de la personne concernée de se saisir de l'information délivrée par le responsable de traitement, semble peu compatible avec les traitements de données à caractère personnel complexes. La première partie de l'étude a démontré que la capacité de compréhension de la personne concernée était fortement limitée par l'utilisation de jargon juridique ou technique. De manière similaire, la capacité de compréhension de la personne concernée du traitement est fortement limitée par la présence de difficultés juridiques ou techniques. En pratique, la difficulté juridique naît de traitements de données à caractère personnel qui, du fait de la localisation de ses destinataires, sont soumis à plusieurs systèmes de protection des données à caractère personnel différents (Section 1). La difficulté technique naît quant à elle de traitements dont la complexité technologique est

---

[934] Cette tendance est notamment visible dans les entreprises vendant comme service un accompagnement à la conformité RGPD. V. par exemple DEVERGRANNE Thiébaut, « RGPD : arrêtez de demander le consentement ! », *donneespersonnelles.fr*, disponible sur https://www.donneespersonnelles.fr/rgpd-arretez-le-consentement (consulté en octobre 2021) ; Sarbacane, « Le RGPD rend-il obligatoire le consentement ? », *Sarbacane.com*, disponible sur https://www.sarbacane.com/help/rgpd/general-rgpd/rgpd-consentement (consulté en octobre 2021).

[935] CNIL, « Conformité RGPD : comment recueillir le consentement des personnes », *CNIL.fr*, 3 août 2018, disponible sur https://www.cnil.fr/fr/les-bases-legales/consentement (consulté en octobre 2021).

difficile à comprendre par les personnes concernées non spécialistes, à l'image de l'intelligence artificielle (Section 2).

Section 1 – La complexité des transferts de données à caractère personnel

472. Nombreux sont les auteurs qui mettent en exergue la complexité du régime des transferts de données à caractère personnel[936]. Le caractère complexe des transferts de données à caractère personnel hors Union européenne a pour principale origine la multiplication des régimes juridiques auxquels les données à caractère personnel sont et seront soumises, ces régimes juridiques n'étant pas homogènes quant au niveau de protection des données à caractère personnel offert aux personnes concernées.

473. La complexité des transferts de données à caractère personnel hors Union européenne est le résultat de la volonté du législateur de protéger la personne concernée de régimes peu protecteurs vis-à-vis de leurs traitements de données à caractère personnel, dans des États aux législations permissives vis-à-vis du responsable de traitement. Face à ce risque, le législateur européen a créé le principe d'interdiction générale des transferts des données à caractère personnel, sauf dans le cas où le transfert répond à une des « autorisations » spécifiquement détaillées au chapitre V du RGPD. Ainsi, un transfert s'inscrira idéalement dans le cadre d'une décision d'adéquation adoptée par la Commission européenne, à défaut dans le cadre de garanties appropriées mises en place par le responsable de traitement et à défaut, sur une des exceptions inscrites à l'article 49 du RGPD, parmi lesquelles le consentement.

474. La complexité des transferts de données à caractère personnel hors Union européenne se situe donc non seulement dans la multiplication des régimes juridiques, mais également dans le régime instauré par le RGPD. Or, cette complexité perturbe la possibilité pour le responsable de traitement de collecter un consentement valide, qui soit à la fois valide et approprié. Il semble dès lors que la validité du consentement puisse, malgré une base légale textuelle inscrite à l'article 49, être incompatible avec les transferts de données à caractère personnel (§1). De plus, une clarification du régime des transferts de données à caractère personnel semble être nécessaire afin de s'assurer que la base légale du consentement soit appropriée (§2).

---

[936] V. par exemple DANIS-FATÔME Anne, « Arrêt Schrems II : sauvetage de façade des "clauses contractuelles types", mais invalidation du bouclier de protection des données », *Communication Commerce électronique*, n° 11, novembre 2020, comm. 83 ; METALLINOS Nathalie, « Transferts de données — Perspectives de sauvetage des "clauses contractuelles types", mais à quel prix ? », *Communication Commerce électronique*, n° 4, avril 2020, comm. 35 ; BU-PASHA Shakila, «Cross-border issues under EU data protection law with regards to personal data protection», *Information & Communications Technology Law*, volume 26, issue 3, pp. 213–228.

§1 – La difficile compatibilité entre le consentement et les transferts de données à caractère personnel

475. La complexité des transferts de données à caractère personnel est de double nature. Premièrement, la complexité du cadre juridique du transfert, de la capacité à s'informer sur le droit applicable dans un État hors Union européenne et des dispositifs techniques de sécurité des données à caractère personnel rend très difficile l'exercice d'un consentement éclairé par la personne concernée (A). Deuxièmement, la multiplication des systèmes juridiques régissant le traitement des données à caractère personnel peut faire obstacle au respect du régime établi par le RGPD relatif au consentement par le responsable de traitement (B).

A. Un système complexe du point de vue de la personne concernée

476. Dans le cas où le responsable de traitement ne peut ni fonder son transfert de données à caractère personnel sur l'existence d'une décision d'adéquation ou de garanties appropriées (dont les clauses contractuelles types et les règles d'entreprise contraignantes), le responsable peut se fonder sur les dérogations de l'article 49 du RGPD. En effet, l'article 49 permet au responsable de traitement de se fonder sur l'une des sept bases juridiques dérogatoires, parmi lesquelles le législateur a inclus le consentement explicite. Le RGPD autorise le transfert de données à caractère personnel vers un pays tiers ou une organisation interdiction dans le cas où « la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées »[937].

477. Ainsi, le consentement de la personne concernée au transfert de ses données à caractère personnel dans un pays tiers ne se confond pas avec le consentement au traitement des données à caractère personnel. Le législateur, conscient des risques que de tels transferts font peser sur les traitements des données à caractère personnel des individus, a voulu protéger la personne concernée en renforçant le consentement au traitement de ses données à caractère personnel (1). Cependant, ce renforcement ne semble pas résulter en une protection suffisante de la personne concernée face à un traitement des données à caractère personnel dans un pays tiers ou une organisation internationale qui n'est pas protégé par des garanties adéquates (2).

[937] RGPD, 27 avril 2016, Article 49 (1) (a).

1. La volonté du législateur de protéger le consentement de la personne concernée face aux transferts de données à caractère personnel

478. Dans le cadre de transferts de données à caractère personnel, le législateur européen a pris le soin de renforcer le consentement de la personne concernée afin de protéger la volonté de la personne concernée. Par conséquent, le consentement-dérogation est doublement protégé : son caractère libre est renforcé par l'exigence d'un consentement explicite et son caractère éclairé est renforcé par l'exigence spécifique d'information relative aux risques que le transfert crée pour la protection des données à caractère personnel. Ces garanties s'ajoutent à l'ensemble des protections régissant le consentement RGPD tel qu'étudiées en Partie 1.

479. L'exigence d'un consentement explicite a pour objectif de protéger la personne concernée face au niveau élevé de risque que représente le transfert de données à caractère personnel. Selon cette conception, le contrôle de la personne concernée doit être d'autant plus garanti que le traitement est risqué. Le caractère protecteur du consentement explicite est notamment hérité de la directive 95/46/CE. En effet, sous le régime de la directive, l'obligation d'obtenir un consentement explicite de la personne concernée était déjà envisagée comme un cas dans lequel « la condition d'obtention du consentement est plus stricte, dans la mesure où il doit aller plus loin que la condition générale d'octroi du consentement »[938]. Le G29 a ensuite confirmé le caractère plus strict, au sens de plus protecteur du consentement explicite dans le RGPD :

> « Le consentement explicite est requis dans certaines situations où un risque sérieux lié à la protection des données survient, et où un niveau élevé de contrôle sur les données à caractère personnel par la personne concernée est de ce fait jugé approprié »[939].

480. Cependant, si la philosophie protectrice du consentement explicite persiste entre la directive 95/46/CE et le RGPD, la définition du consentement explicite a quant à elle évolué. En 2011, sous le régime de la directive 95/46/CE, la définition du consentement explicite équivalait à celle du consentement exprès, regroupant l'ensemble des « situations où il est proposé à une personne d'accepter ou de rejeter une utilisation particulière ou la divulgation des informations la concernant et qu'elle répond activement à la question, que ce soit oralement ou par écrit »[940]. L'aspect protecteur d'une telle disposition résulte de la définition du consentement dans l'article 2(h) de la directive 96/46/CE qui définissait le consentement de la personne concernée comme « toute manifestation de volonté, libre, spécifique et informée par

[938] Groupe de travail « Article 29 », WP 187, *op. cit.*, p. 6.
[939] Groupe de travail « Article 29 », WP259 rév. 01, *op. cit.*, pp. 20-21.
[940] Groupe de travail « Article 29 », WP 187, *op. cit.*, p. 28.

laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Ainsi, le caractère équivoque du consentement par le biais d'une action positive était absent des exigences générales en matière de consentement. De l'avis même du G29, un consentement (même indubitable) pouvait être « déduit de certaines actions »[941]. Après l'adoption du RGPD, le G29 a décidé de faire évoluer la définition du consentement explicite « dès lors que les exigences pour un consentement « standard » dans le RGPD sont déjà portées à un niveau supérieur à celles de la directive 95/46/CE »[942]. Le consentement explicite est dès lors défini de la manière suivante :

> « Le terme *explicite* se rapporte à la façon dont le consentement est exprimé par la personne concernée. Il implique que la personne concernée doit formuler une déclaration de consentement exprès »[943].

481. La définition du consentement explicite sous le régime du RGPD est donc différente de celle proposée par le G29 en 2011. Le caractère auparavant explicite de l'action de cliquer sur un bouton ou sur des icônes[944] correspond désormais à la définition du consentement « standard » du RGPD qui demande une manifestation de volonté « univoque par laquelle la personne concernée accepte, par une déclaration ou un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »[945]. Désormais, un consentement explicite nécessite non seulement un acte positif clair de la personne concernée pour consentir à un traitement, mais également une formulation de ce consentement. Le G29 précise à cet effet qu'une telle formulation peut s'obtenir à travers une déclaration écrite et signée par la personne concernée, le remplissage d'un formulaire électronique, l'envoi d'un courrier électronique, l'utilisation d'une signature électronique ou encore le téléchargement d'un traitement scanné portant la signature de la personne concernée[946]. L'obtention d'un consentement oral à travers une déclaration orale ou une conversation téléphonique (accompagnée d'un acte positif clair de la personne) n'est pas exclue par le RGPD, mais le responsable de traitement doit garder à l'esprit qu'il doit prouver non seulement le recueil du consentement, mais également la loyauté et la clarté de l'information[947]. Le consentement explicite semble donc bien être une protection supplémentaire de la personne concernée dont le contrôle de ses données à caractère personnel est consolidé par une certaine temporisation du consentement à travers sa formulation. En effet, la nécessité pour la personne concernée de

---

[941] *Idem*, p. 25.
[942] Groupe de travail « Article 29 », WP259 rév. 01, *op. cit.*, p. 21.
[943] *Ibidem.*
[944] Groupe de travail « Article 29 », WP 187, *op. cit.*, p. 29.
[945] RGPD, 27 avril 2016, article 4 (11).
[946] Groupe de travail « Article 29 », WP259 rév. 01, *op. cit.*, p. 21.
[947] *Idem*, pp. 21-22.

devoir formuler son consentement met en exergue l'acte de consentir, qui ne peut plus, en théorie, résulter d'un simple réflexe de la personne concernée face à une case à cocher par exemple. Les transferts de données à caractère personnel vers des pays tiers étant plus risqués que les traitements de données à caractère personnel dans les pays de l'Union européenne et les pays appliquant le RGPD, une telle garantie semble appropriée aux risques inhérents à de tels traitements.

482. La deuxième condition, l'enrichissement de l'information de la personne concernée par une information spécifique relative aux risques du transfert de données à caractère personnel pour la personne concernée, présente plus de difficultés à cohabiter avec les exigences plus générales de l'obtention d'un consentement éclairé. Il faut en premier lieu rappeler que le consentement étant spécifique, la demande de consentement doit porter spécifiquement sur le transfert de données à caractère personnel. Ainsi, le consentement initial au traitement de données à caractère personnel ne peut sous aucune circonstance être interprété ultérieurement comme un consentement au transfert de ses données. Si un responsable de traitement souhaite, après la collecte de certaines données sur la base du consentement, fonder un transfert de données sur le consentement, il devra faire une nouvelle demande de consentement à la personne concernée, en respectant à la fois les conditions du consentement « standard » et celles spécifiques à l'article 49(1)(a).

483. Pour fonder un transfert de données à caractère personnel vers un pays tiers ou une organisation internationale sur la base du consentement au sens de l'article 49(1)(a), le responsable de traitement doit informer la personne concernée des risques auxquels elle s'exposer à travers l'acceptation du transfert de ses données en l'absence de décision d'adéquation et de garanties appropriées. Le contenu n'est pas plus précisé au sein du RGPD. Selon le Comité européen de protection des données,

> « des informations doivent être fournies concernant les éventuels risques pour la personne concernée découlant de l'absence de protection adéquate dans le pays tiers et de l'absence de garanties appropriées. Cet avertissement, qui pourrait être normalisé, devrait par exemple indiquer que le pays tiers est susceptible de ne pas disposer d'une autorité de contrôle ou de principes de traitement des données, ou encore de droits des personnes concernées »[948].

484. Une telle formulation implique une obligation d'information comparative, permettant d'éclairer la personne concernée sur l'absence de certaines garanties présentes dans le RGPD,

---

[948] Comité européen de protection des données, *Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679*, adoptées le 25 mai 2018, p. 9.

et donc d'évaluer le risque de consentir à un transfert de ses données vers un pays tiers. L'approche comparative prônée par le G29 semble avoir, de ce fait, le potentiel de constituer une protection efficace du consentement de la personne concernée.

485. L'exigence d'un consentement explicite et particulièrement informé sur les risques inhérents au transfert de données à caractère personnel renforce le consentement aux transferts de ces données, puisque le consentement naît de la formulation de la volonté de la personne concernée à la suite d'une information spécifique quant aux risques qu'elle encourt lors de ce transfert. Cependant, malgré ces garanties, la complexité des transferts de données à caractère personnel ne permet pas d'assurer de la concomitance entre le consentement au transfert et la volonté de la personne concernée.

2. L'insuffisance des garanties protégeant la réalité du consentement face aux transferts de données à caractère personnel

486. Si le consentement explicite et l'information spécifique aux risques du traitement constituent des garanties tout à fait légitimes et nécessaires à garantir l'adéquation du consentement avec la volonté de la personne concernée, ces garanties ne semblent pas pour autant être suffisantes. En effet, plusieurs points de vigilance sont à souligner quant à la compatibilité du consentement explicite tel qu'établi à l'article 49 avec les principes relatifs à la transparence et au consentement éclairés tels que sus-étudiés[949].

487. La principale difficulté concerne la capacité de la personne concernée à émettre un consentement éclairé pour les transferts de données à caractère personnel. Certes, l'article 49 du RGPD répond en partie à cette difficulté en obligeant le responsable de traitement à informer la personne concernée sur les risques spécifiques auxquels elle s'expose du fait du traitement. Cependant, ces risques peuvent s'avérer très complexes à expliquer auprès de la personne concernée. En adoptant une approche comparative entre deux systèmes juridiques, il sera difficile au responsable de traitement de délivrer une information ne nécessitant pas que la personne concernée ait une connaissance minimale du droit européen de la protection des données. Par exemple, si le responsable de traitement informe la personne concernée que « le pays tiers est susceptible de ne pas disposer d'une autorité de contrôle », la personne concernée entreverra-t-elle réellement le risque qui consiste à rendre difficile l'accès à ses droits ou l'accès à une voie de recours concernant le traitement de ses données ? De même, une personne concernée qui a le sentiment de voir ses données à caractère personnel traitées de manière

[949] V. *supra* n° 82-291.

importante et fréquente au sein de l'Union européenne est susceptible de ne pas évaluer correctement le risque associé à l'absence de principe de minimisation des données dans un pays tiers.

488. Par conséquent, le niveau de perception du risque par la personne concernée risque d'être compromis par des facteurs non rationnels, et notamment l'implication situationnelle : par exemple, l'utilisation d'un ton institutionnel « tendrait à réduire la perception du risque »[950]. La perception du risque peut également être réduite par le niveau d'engagement de la personne concernée avec le service envisagé[951], son biais d'optimisme[952], ou encore la confiance qu'elle peut porter au responsable de traitement[953]. Il est vrai qu'une future normalisation de cette information pourrait permettre à la personne concernée de comprendre l'information qui lui est délivrée, et notamment de comprendre les risques associés au transfert de ses données sur la base de l'article 49 du RGPD. Une telle normalisation permettrait, d'une part, de sensibiliser la personne concernée aux différents risques associés à l'absence de dispositions protectrices des données à caractère personnel. D'autre part, une normalisation de l'information délivrée lui permettrait également d'évaluer le risque associé au transfert de ses données à caractère personnel vers un pays tiers, dans la mesure où l'information relative au niveau de risque (de minime à très élevé) pourrait aussi être normalisée. Cependant, cette normalisation n'est aujourd'hui ni présente ni obligatoire. La complexité des transferts de données à caractère personnel vers un pays tiers sur la base de l'article 49 du RGPD est donc un frein au consentement éclairé dans son aspect de compréhensibilité de l'information et évaluation du risque.

489. Enfin, la temporisation du consentement par l'exigence d'un consentement explicite n'est pas toujours effective. Prenons l'exemple des formulaires constituant un consentement explicite. La multiplication des formulaires à remplir en ligne a motivé les fournisseurs de navigateurs internet à proposer des fonctions de remplissage automatique des formulaires avec des informations enregistrées. Ces fonctions semblent si ancrées dans nos pratiques qu'elles ne permettent pas d'assurer la temporalisation du consentement. *A contrario*, l'inscription d'une

---

950 BARCELOS Renato Hübner, GRIL Emmanuelle, « Réseaux sociaux : quel ton adopter ? », *Gestion*, Vol. 44, 2019/4, p. 87.

951 DHOLAKIA Utpal M., «A Motivational Process Model of Product Involvement and Consumer Risk Perception», *European Journal of Marketing*, Vol. 35 No. 11/12, pp. 1340–1362.

952 V. l'analyse très intéressante proposée par l'équipe de chercheurs de Taehwan Park sur l'impact du biais d'optimisme sur la perception du risque liée à la pandémie de Covid-19 : PARK Taehwan, «Optimistic Bias and Preventive Behavioral Engagement in the Context of COVID-19», *Research in Social and Administrative Pharmacy*, Vol. 17, Issue 1, janvier 2021, pp. 1859–1866.

953 SIEGRIST Michael *et al.*, «Perception of Risk: the Influence of General Trust, and General Confidence», *Journal of Risk Research*, 2005, Volume 8, Issue 2, pp. 145–156.

mention d'acceptation des risques dans un champ n'acceptant pas la fonction « copier/coller » est une pratique permettant une temporisation appropriée du consentement. Il est à cet égard regrettable que l'EDPB n'ait pas choisi d'adapter sa réflexion sur le consentement explicite en prenant en compte, en plus de l'évolution juridique, l'évolution des pratiques. Une telle réflexion aurait pourtant permis de formaliser le consentement de la personne concernée et de sortir le consentement au transfert de données à caractère personnel du champ du consentement normal au traitement de ces données.

490. La complexité des transferts de données à caractère personnel permet ainsi difficilement d'obtenir le consentement éclairé de la personne concernée. L'information spécifique aux risques et l'exigence de consentement explicite assurent une meilleure protection de la personne concernée, mais ne permettent pas d'atteindre un niveau de protection approprié et suffisant de la personne concernée face aux risques encourus par ces transferts. De plus, la complexité des transferts de données entame la liberté de consentement de la personne concernée, que le responsable de traitement risque de ne pas pouvoir garantir tout au long du traitement.

B. Le risque du consentement définitif

491. Les difficultés liées au consentement aux transferts de données à caractère personnel résultent de l'identification de la législation de l'État tiers comme moins protectrice que la législation européenne et de l'impossibilité de créer juridiquement des garanties appropriées. En effet, pour le responsable de traitement, recourir au consentement pour les transferts de données à caractère personnel revient à s'engager de pouvoir respecter, en plus des conditions relatives au consentement de l'article 49, les critères de validité du consentement standard.

492. La principale difficulté pour le responsable de traitement consiste à assurer le droit de retirer son consentement à la personne concernée dans un système juridique ne permettant pas un tel retrait. Comme il l'a déjà été sus étudié, la liberté du consentement implique que le consentement n'est pas définitif : le consentement lie certes la personne concernée, mais uniquement pendant la période où son consentement est réel. Pour assurer cette réalité du consentement, le RGPD a ainsi garanti à la personne concernée le droit de retirer son consentement à tout moment par son article 7(3) :

> « La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement ».

493. Utiliser le mécanisme du consentement pour transférer des données à caractère personnel vers un pays tiers crée dès lors un risque juridique important vis-à-vis du responsable de traitement. En effet, ce dernier, en utilisant la base du consentement et de l'article 49 du RGPD, doit pouvoir garantir à la personne concernée la possibilité de retirer son consentement à tout moment, alors même que ses données à caractère personnel sont régies par un système de protection des données plus faible que le RGPD. Cette situation a d'ailleurs été mise en exergue par l'EDPB, pour qui l'utilisation du consentement par le responsable de traitement n'est pas « une solution réalisable à long terme »[954]. L'avertissement de l'EDPB s'inscrit dans l'interprétation méfiante déjà proposée par le G29 en 2005 de l'utilisation du mécanisme du consentement lors d'un transfert de données à caractère personnel vers un pays tiers. Sous le régime de la directive 95/46/CE, le G29 avait déjà prévenu les responsables de traitement de la possibilité de se retrouver dans des situations insolubles si ne fût-ce qu'une personne concernée par le transfert décidait ultérieurement de retirer son consentement. […] Le recours au consentement peut donc se révéler être « une « fausse bonne solution », simple de prime abord, mais en réalité complexe et lourde à gérer »[955]. Cette interprétation a, par la suite, été reprise par l'ICO dans un article consacré aux transferts internationaux après la sortie du Royaume-Uni de l'Union européenne :

> « Étant donné le seuil élevé requis pour un consentement valide, et le fait que le consentement doit pouvoir être retiré, il est possible que l'utilisation du consentement ne soit pas une solution réalisable ».[956]

494. La responsabilité du responsable de traitement dans la mise en place de ses traitements hors Union européenne a été mise en exergue par la jurisprudence *Schrems II*[957]. À cette occasion, la Cour de justice de l'Union européenne a consacré l'obligation pour un responsable de traitement de garantir que les personnes concernées bénéficient de garanties appropriées et disposer de droits opposables et de voies de droit effectives lorsqu'ils mettent en place des transferts de données à caractère personnel fondés sur l'article 46 du RGPD[958]. Ainsi, si l'avocat général a pu considérer que l'utilisation des clauses contractuelles types adoptées par la

---

[954] EDPB, 25 mai 2018, *op. cit.*
[955] Groupe de travail « Article 29 », WP 114, *op. cit.*, p. 13.
[956] ICO, « International transfers after the UK exit from the EU Implementation Period », *ICO.org.uk*, disponible sur. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/ (consulté en septembre 2021).
[957] CJUE, C-311/18, *op. cit.*
[958] *Idem,* §90-105.

Commission peut représenter un mécanisme général applicable aux transferts[959], la Cour se montre plus stricte en concluant :

> « L'évaluation du niveau de protection assurée dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union et le destinataire du transfert établi dans le pays concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui-ci »[960].

495. Se faisant, la CJUE ne s'est pas directement prononcée sur les transferts de données à caractère personnel fondés sur le consentement[961], mais uniquement sur les garanties appropriées telles que définies à l'article 46 du RGPD. La solution s'étend pourtant à l'ensemble des transferts de données à caractère personnel. La Cour affirme en effet que l'existence d'un mécanisme de transfert de données n'exempte pas le responsable de traitement de ses obligations générales en matière de RGPD. Ainsi, transférer les données à caractère personnel sur le fondement du consentement signifie que le responsable de traitement est capable d'assurer la validité du consentement tout au long du traitement de données à caractère personnel.

496. Pour comprendre l'interprétation proposée par les autorités de contrôle européennes, il faut noter en premier lieu que la possibilité pour la personne concernée de retirer son consentement à tout moment est assurée par le fait que le consentement au sens du RGPD se distingue, comme nous l'avons vu en Partie 1, du consentement contractuel. Cette distinction permet au responsable de traitement de ne pas se retrouver dans des situations juridiquement impossibles à résoudre. Une telle situation peut résulter, par exemple, d'une personne retirant son consentement à un traitement de données, alors même que ce traitement est nécessaire à l'exécution d'un contrat. Or, l'approche non commerciale de la protection des données à caractère personnel proposée par le RGPD n'est pas une approche universelle.

---

[959] Conclusions de l'avocat général M. Henrik Saugmandsgaard Øe, *Data Protection Commissionner c. Facebook Ireland Limited, Maximilian Schrems*., présentées le 19 décembre 2019, C-311/18, §120.
[960] CJUE, 16 juillet 2020, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximilian Schrems*, C-311/18, §105.
[961] La recevabilité des questions préjudicielles avait d'ailleurs été contestée sur les éléments factuels, les gouvernements britannique et allemand considérant que la Haute-Cour irlandaise aurait dû, préalablement à sa question préjudicielle, établir factuellement que les transferts de données de Maximilian Schrems n'étaient pas établis sur la base du consentement de Maximilian Schrems à Facebook à ces transferts. Ces contestations ont rapidement été écartées par l'avocat général. Conclusions de l'avocat général M. Henrik Saugmandsgaard Øe, *op.cit.*, §96-99.

497. Pour illustrer l'avertissement de l'EDPB et les différences de système de protection des données dans le monde, étudions l'exemple du *California Consumer Privacy Act* (CCPA) tel qu'amendé par le *California Privacy Rights Act* (CPRA) en décembre 2020, qui a si souvent été présenté dans le paysage médiatique comme le « RGPD californien »[962]. Le responsable de traitement peut être amené à utiliser des sous-traitants californiens tant la *Silicon Valley* a acquis une image de pôle d'innovation, qui à la fois accueille des acteurs majeurs des technologies de l'information et des communications, et « crée un environnement encourageant l'évolution des entreprises existantes et […] la création de nouvelles entreprises »[963] depuis 1975. La réception du CCPA/CPRA qui n'a cessé de susciter la comparaison avec le RGPD pourrait en outre motiver le responsable de traitement à justifier un transfert de données à caractère personnel vers un territoire considéré comme protégeant les données à caractère personnel.

Or, le titre du CCPA est révélateur de la différence entre l'approche californienne et l'approche européenne : l'acte californien a vocation à s'appliquer aux consommateurs et non aux personnes concernées. Ainsi, « toute autre personne, employés, administrés, patients, etc., ne sont pas protégés par ce texte, même s'ils sont californiens »[964]. L'objectif et la philosophie des deux systèmes de protection des données vont également être substantiellement différents[965].

---

[962] V. par exemple La tribune, « Le "RGPD californien", une loi modèle, exportable au reste des États-Unis », *Latribune.fr*, 22 février 2020, disponible sur https://www.latribune.fr/economie/international/le-rgpd-californien-une-loi-modele-exportable-au-reste-des-etats-unis-840240.html (consulté en septembre 2021) ; Les Echos, « La Californie se dote d'un RGPD », *LesEchos.fr*, 2 juillet 2018, disponible sur https://www.lesechos.fr/tech-medias/hightech/la-californie-se-dote-dun-rgpd-133913 (consulté en septembre 2021).

[963] « create an environment encouraging the evolution of existing firms, and […] the creation of new firms » [traduction libre]. KENNEY Martin, *Understanding Silicon Valley: The Anatomy of an Entrepreneurial Region*, University of Chicago Press, 2000, p. 14.

[964] ZUBCEVIC Oriane, « Le "California Consumer Privacy Act" est-il le RGPD américain ? », *Éditions Législatives*, 28 janvier 2020, disponible sur https://www.editions-legislatives.fr/actualite/le-%C2%ABcalifornia-consumer-privacy-act%C2%BB-est-il-le-rgpd-americain (consulté en septembre 2021). Ajoutons également que le champ d'application territorial de la législation californienne est très restreint puisqu'il va protéger seulement les résidents californiens lorsqu'ils sont situés en Californie

[965] Afin de comprendre la philosophie qui gouverne le CCPA/CPRA, il nous faut revenir aux conditions de son adoption. En effet, « une grande partie de l'impulsion politique à l'origine de l'adoption de la loi est née de scandales majeurs en matière de protection de la vie privée qui ont été révélés [les derniers mois avant l'adoption du CCPA], y compris l'incident de Cambridge Analytica qui a affecté les données des utilisateurs de Facebook ». En 2018, les médias révèlent que Cambridge Analytica a eu accès aux données à caractère personnel de plus de 50 millions de votants américains qui avaient, contre rémunération, rempli un test de personnalité et accepté de voir ces données utilisées dans le cadre de la recherche académique. Cette application collectait de nombreuses données sur ses utilisateurs, dont la liste d'amis Facebook et les « likes », qui ont permis de dresser des profils utilisateurs afin de créer des publicités ciblées. Ces profils ont par la suite été utilisés lors de la campagne présidentielle de Donald Trump en 2016, Cambridge Analytica ayant offert à l'équipe de campagne des outils pour identifier la personnalité de votants américains afin d'influencer leur comportement. Ainsi, les données des utilisateurs de Facebook ont été monétisées en violation des politiques de confidentialités à la fois de Facebook et de l'application créée par le docteur Kogan, notamment pour influencer des campagnes politiques. Cambridge Analytica est une entreprise d'analyse de données à grande échelle, qui s'est donné « pour mission "de changer le comportement grâce aux données" […]} en mélangeant le traitement quantitatif de données, la psychométrie et la psychologie comportementale ». Le Monde, « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du

Notamment, le CCPA ne garantit pas un principe de licéité du traitement au sens de l'article 6 du RGPD dans le sens où le responsable de traitement ne va pas devoir fonder son traitement sur une liste de bases juridiques listées par l'instrument californien[966]. Ainsi, pour collecter des données à caractère personnel sur les personnes concernées sous le régime du CCPA/CPRA, l'entreprise ne sera soumise qu'à une simple obligation d'information (*notice*), et devra informer la personne concernée des finalités pour lesquelles les données sont collectées. Cette obligation d'information est renforcée par un droit d'accès aux données à caractère personnel collectées. Par ailleurs, le CCPA/CPRA va permettre aux consommateurs (les personnes concernées) de s'opposer à la vente ou au partage de ses données à caractère personnel[967]. Cette opposition s'exerce généralement à travers un lien « Do Not Sell or Share My Personal Information » sur le site internet de l'entreprise souhaitant vendre ces données[968]. De plus, le CCPA/CPRA offre la possibilité aux personnes concernées de limiter l'utilisation de ses données sensibles aux traitements nécessaires pour la livraison d'un service ou d'un bien et qui sont raisonnablement attendus par le consommateur[969] (sauf exception, par exemple les données sensibles publiquement accessibles[970]). Cette opposition s'exercera généralement grâce à un lien « Limit the Use of My Sensitive Personal Information »[971]. Enfin, concernant le profilage, de nouvelles règles sont à attendre puisque le CCPA/CPRA invite l'État californien à :

> « émettre des réglementations régissant les droits d'accès et l'*opt-out* en ce qui concerne l'utilisation par les entreprises de la technologie de prise de décision automatisée, y compris le profilage et exiger que la réponse des entreprises aux demandes d'accès comprenne des

scandale Facebook », *LeMonde.fr*, Pixels, 22 mars 2018, disponible sur https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html (consulté en septembre 2021) ; GHOSH Dipayan, « What You Need to Know About California's New Data Privacy Law », *Harvard Business Review*, 11 juillet 2018, disponible sur https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law (consulté en septembre 2021) ; The Guardian, « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », *TheGuardian.com*, 17 mars 2018, disponible sur https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (consulté en septembre 2021) ; The New York Times, « Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens », *NYTimes.com*, 19 mars 2018, disponible sur https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (consulté en septembre 2021) ; California Privacy Rights Act (CPRA), Section 1798.100.

[966] Future of Privacy Forum, *Comparing Privacy Laws: GDPR v. CCPA*, novembre 2018, p. 23, disponible sur https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf (consulté en septembre 2021).

[967] CPRA, Section 1798.120.

[968] *Idem*, Section 1798.135.

[969] *Idem*, Section 1,798,121.

[970] *Idem*, Section 1,798,140.

[971] *Idem*, Section 1,798,135.

> informations significatives sur la logique impliquée dans ces processus de prise de décision, ainsi qu'une description du résultat probable du processus en ce qui concerne le consommateur »[972].

Ainsi, le consentement de la personne concernée n'est globalement pas considéré comme un mécanisme d'*opt-in* mais comme un mécanisme d'*opt-out*. Dès lors, même si le CCPA/CPRA avait un champ d'application territorial englobant les personnes concernées européennes dont les données à caractère personnel sont traitées en Californie, la personne concernée ayant donné son consentement au transfert de ses données à caractère personnel vers une entreprise californienne ne pourra pas retirer son consentement, mais uniquement s'opposer à la vente de ses données à caractère personnel, au partage de ses données sensibles ou au profilage. Le droit à la suppression des données à caractère personnel garanti par le CCPA/CPRA ne suffit pas à pallier l'absence de possibilité pour la personne concernée de retirer son consentement. En effet, il ne s'agit pas d'un droit absolu, et une entreprise peut refuser de supprimer des données qui seraient « raisonnablement nécessaires à l'entreprise », notamment lorsque ces données sont traitées en interne par l'entreprise dans la limite des « attentes raisonnables » de la personne concernée dans sa relation avec l'entreprise. Ainsi, même si le CCPA/CPRA élargissait son champ d'application à la protection des personnes concernées européennes dont les données sont transférées en Californie, le responsable de traitement se retrouverait dans une situation illicite au regard du RGPD : il ne serait pas à même de respecter les conditions relatives au retrait du consentement, alors même que le consentement est la base juridique sur laquelle il a fondé le transfert.

498. Le CCPA/CPRA n'est qu'un exemple parmi d'autre d'environnement juridique dans lequel le retrait du consentement ne sera, en pratique, pas possible. L'illustration permet également de mettre en exergue l'existence de problématiques liées aux transferts de données même en présence d'un texte qui semble, aux yeux du responsable de traitement et de la personne concernée, similaire à celui du RGPD. Dès lors, en raison des conditions attachées à la validité du consentement dans le RGPD, il sera difficile pour le responsable de traitement de transférer des données à caractère personnel sur le fondement du consentement au sens de l'article 49 du RGPD.

---

[972] «Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer' [traduction libre]. *Idem*, Section 1,798,185.

§2 – Une nécessaire clarification du régime applicable aux transferts de données à caractère personnel hors Union européenne

499. Les difficultés relatives au consentement en matière de transferts de données à caractère personnel proviennent d'une mauvaise compréhension de la place du mécanisme du consentement dans les transferts de données à caractère personnel (A), mais également d'une absence de clarté du règlement quant à la possibilité de protéger la personne concernée (B).

A. L'exceptionnalité de l'article 49 du RGPD

500. Il est important pour les responsables de traitement de garder à l'esprit que le consentement en matière de transferts de données à caractère personnel en dehors de l'Union européenne est un régime exceptionnel, qui n'a aucune vocation à être utilisé de manière systémique. Or, il semble que certains responsables de traitement préfèrent encore recourir au consentement par commodité, notamment lorsque ces derniers fondent la majorité de leurs traitements sur le consentement. Il est vrai que la tentation est forte puisqu'*a priori*, étendre la demande de consentement aux transferts de données à caractère personnel hors Union européenne semble peu coûteux[973]. Par exemple, en matière de recherche médicale dans le cadre d'un consortium, il est peu probable que les décisions d'adéquation couvrent l'ensemble des données nécessaires aux recherches impliquant des participants volontaires. Dès lors, le consentement peut dès lors apparaître comme un moyen efficace de « fournir une couverture uniforme » des données collectées dans le cadre de tels projets[974].

501. Cependant, à la lecture du chapitre V du RGPD relatif aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales, le consentement est une dérogation très encadrée. Elle relève en effet de l'article 49, dont le caractère subsidiaire est explicite : cet article ne peut s'appliquer qu'en « l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes »[975]. L'EDPB a d'ailleurs une lecture particulièrement stricte de cet article et discerne une obligation à la charge du responsable de traitement exportateur de données de « d'abord s'efforcer de procéder au transfert à l'aide d'un des mécanismes prévus

[973] PHILLIPS Mark, «International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), *Human Genetics*, 2018, vol. 137, pp. 575–582 (disponible sur Springer Link).
[974] *Ibidem.*
[975] RGPD, 27 avril 2016, Article 49 (1).

aux articles 45 et 46 du RGPD »[976], et ainsi ne s'appuyer sur la dérogation de l'article 49 qu'en dernier recours.

502. De plus, l'article 49 du RGPD est intitulé « dérogations pour des situations particulières ». Le caractère dérogatoire est régulièrement rappelé par les autorités de contrôle[977] ainsi que par l'EDPB qui affirme, dans ses lignes directrices relatives aux dérogations prévues à l'article 49 du RGPD, que :

> « Les dérogations visées à l'article 49 sont donc des exemptions du principe général selon lequel des données à caractère personnel ne peuvent être transférées vers des pays tiers que si un niveau de protection adéquat est offert dans le pays tiers ou si des garanties appropriées ont été apportées et si les personnes concernées bénéficient de droits opposables et effectifs afin de continuer à bénéficier de leurs droits fondamentaux et garanties. De ce fait et conformément aux principes de droit inhérents à l'ordre juridique européen, les dérogations doivent être interprétées de manière restrictive afin que l'exception ne devienne pas la règle »[978].

L'article 49 est si dérogatoire que le RGPD permet même aux États membres de prendre certaines libertés vis-à-vis de l'harmonisation de la protection des données à caractère personnel. En effet, États membres peuvent adopter des dispositions législatives afin rendre ces dérogations encore plus strictes en limitant les transferts de certaines catégories spécifiques de données à caractère personnel « pour des motifs importants d'intérêt public »[979].

503. Le caractère exceptionnel des dérogations aux transferts de données à caractère personnel vers un pays tiers s'inscrit dans la continuité de l'interprétation déjà proposée par le G29 sous le régime de la directive 95/46/CE. Le G29 avait alors consacré un principe européen commun au droit de l'Union européenne et au droit du Conseil de l'Europe (en l'occurrence, le Protocole additionnel à la Convention 108): « le principe de droit inhérent à l'ordre juridique européen qui consiste à interpréter les clauses d'exception de manière restrictive afin que l'exception ne devienne pas la règle » [980].

504. La limite du recours à l'article 49 du RGPD s'explique d'ailleurs par le fait qu'il permette aux responsables de traitement de transférer des données vers un pays tiers où le niveau de protection des données à caractère personnel est moins élevé que dans l'Union

---

[976] EDPB, 25 mai 2018, *op. cit.,* p. 4.
[977] V. par exemple CNIL, « La CNIL appelle à des évolutions dans l'utilisation des outils collaboratifs états-uniens pour l'enseignement supérieur et la recherche », *CNIL.fr,* 27 mai 2021, disponible sur https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche (consulté en septembre 2021).
[978] EDPB, 25 mai 2018, *op. cit.*, p. 4.
[979] RGPD, 27 avril 2016, Article 49 (5).
[980] Groupe de travail « Article 29 », WP 114, *op. cit.,* p. 9.

européenne. Or, comme le remarquent Brunessen Bertrand et Jean Sirinelli, le RGPD « doit être lu, pensé, interprété comme un tout qui instaure une protection constitutionnelle européenne homogène et cohérente en dépit de la pluralité des régimes qu'il prévoit, en l'occurrence ici, de la multiplicité des fondements juridiques des transferts internationaux de données »[981]. L'articulation entre le régime de principe des articles 45 et 46 du RGPD et le régime d'exception de l'article 49 permet de résoudre ce qui, dans le discours du G29, aurait pu être interprété comme une « impression paradoxale »[982], voire une « incohérence majeure »[983]. En effet, la protection des données à caractère personnel a la particularité de devoir s'inscrire dans un contexte économique en croissance, ce que le RGPD rappelle dans son considérant 5 :

> « L'intégration économique et sociale résultant du fonctionnement du marché intérieur a conduit à une augmentation substantielle des flux transfrontaliers de données à caractère personnel »[984].

Dès lors, le lecteur du RGPD peut y voir, à l'instar du G29, « la reconnaissance du fait que l'expansion du commerce international rend nécessaire, dans certains cas, la flexibilité des transferts internationaux de données, y compris des transferts d'informations à caractère personnel »[985]. Cependant, le recours exceptionnel aux dérogations de l'article 49 permet de dépasser cette incohérence dans la mesure où il ne s'agit pas d'une mesure offrant la possibilité de contourner la législation européenne en matière de protection des données, mais d'un article qui « a été conçu pour régler un nombre limité de cas dans lesquels une dérogation […] a été considérée appropriée »[986], qui sont intitulés « situations particulières ».

505. L'application de l'article 49 du RGPD peut donc se justifier dans les cas où la situation relative à la protection des données à caractère personnel est si incompatible avec les principes édictés par le RGPD qu'il n'est possible de se fonder ni sur une décision d'adéquation ni sur des garanties appropriées. C'est notamment le cas de certains transferts de données vers les États-Unis, après l'invalidation du *Privacy Shield*[987] par la Cour de Justice de l'Union européenne[988]. En effet, la CJUE a considéré que les ingérences résultant des programmes de surveillance américains ne permettaient pas de constater que les États-Unis ont un niveau

---

[981] BERTRAND Brunessen, SIRINELLI Jean, « Schrems II : on prend les mêmes et on recommence », *Dalloz IP/IT*, novembre 2020, n° 11, p. 640.
[982] Groupe de travail « Article 29 », WP 114, *op. cit.*, p. 7.
[983] *Idem*, p. 8.
[984] RGPD, 27 avril 2016, considérant 5.
[985] Groupe de travail « Article 29 », WP 114, *op. cit.*, p. 8.
[986] *Ibidem.*
[987] Est communément appelé *Privacy Shield* (ou bouclier de protection des données) la décision d'adéquation (UE) 2016/1250 de la Commission européenne du 12 juillet 2016.
[988] CJUE, C-211/18, *op. cit.*.

adéquat de protection des données à caractère personnel. La Cour justifie cette inadéquation sur plusieurs fondements. Premièrement, la CJUE estime que les programmes de surveillance étatsuniens « ne correspondent aux exigences minimales attachées, en droit de l'Union, au principe de proportionnalité, si bien qu'il n'est pas permis de considérer que les programmes de surveillances fondés sur ces dispositions sont limités au strict nécessaire »[989]. Deuxièmement, la Cour regrette que la législation américaine en matière de surveillance ne confère pas « aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux, si bien que ces personnes ne disposent pas de recours effectif »[990]. Enfin, la Cour a jugé que le mécanisme de la médiation prévu par le *Privacy Shield* ne permettait pas de conférer un recours effectif, en raison d'un manque de garanties d'indépendance du médiateur ainsi que de l'absence de dispositions octroyant un caractère contraignant à ses décisions[991]. L'annulation de la décision d'adéquation sur le fondement des programmes de surveillance américains a également eu des conséquences sur la possibilité pour les responsables de traitement de fonder leurs traitements sur les garanties appropriées, décrites à l'article 46 du RGPD. Si la Cour n'a pas interdit un tel fondement, elle a toutefois rappelé que :

> « les garanties appropriées, les droits opposables et les voies de droit effectives requis par ces dispositions doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union par ce règlement, lu à la lumière de la Charte. À cet effet, l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques dans ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique »[992].

506. Le fait de devoir prendre en compte l'éventuel accès des autorités publiques a notamment eu pour effet de rendre très difficile la capacité de transférer des données à caractère personnel vers les États-Unis sur le fondement de l'article 46 du RGPD aux entreprises de télécommunication, aux fournisseurs de services de communication électronique, de services informatiques à distance, de services de communication ayant accès à des communications câblées ou électroniques (que ces données soient transmises ou stockées) et aux responsables, employés ou agents de telles entités. C'est notamment ce que le Comité européen de protection

---

[989] *Idem*, §176-184.
[990] *Idem*, §186-192.
[991] *Idem*, §194-197.
[992] *Idem*, §105.

des données a, dans ses recommandations du 10 novembre 2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, expressément affirmé :

> « Si l'importateur de données ou tout autre destinataire auquel l'importateur pourrait divulguer les données relève de l'article 702 de la FISA [soit les catégories d'importateur susvisées], les CCT [clauses contractuelles type] ou tout autre instrument de transfert visé à l'article 46 du RGPD ne peuvent être utilisés pour ledit transfert que si des mesures techniques supplémentaires rendent impossible ou inopérant l'accès aux données transférées »[993].

507. Ainsi, une entreprise de télécommunication qui souhaiterait transférer des données à caractère personnel de l'Union européenne aux États-Unis, sans être capable techniquement de rendre impossible l'accès à ces données aux autorités publiques américaines, ne peut fonder ce transfert ni sur une décision d'adéquation (article 45 du RGPD), ni sur des garanties appropriées (article 46 du RGPD). Dès lors, l'entreprise remplit la première condition lui permettant d'avoir recours aux dérogations de l'article 49 du RGPD. D'ailleurs, lors de son arrêt surnommé « Schrems II » (parfois appelé « Schrems III »), la Cour de Justice avait souligné la possibilité de recourir à l'article 49 en l'absence de décision d'adéquation et de garanties appropriées :

> « S'agissant du point de savoir s'il convient de maintenir les effets [de la décision bouclier de protection des données ou *Privacy Shield* (décision BPD)] aux fins d'éviter la création d'un vide juridique […], il y a lieu de noter que, en tout état de cause, compte tenu de l'article 49 du RGPD, l'annulation d'une décision d'adéquation telle que la décision BPD n'est pas susceptible de créer un tel vide juridique »[994].

508. Cependant, une telle affirmation ne semble pas être en adéquation avec la philosophie générale de l'article 49 du RGPD, telle que développée dans la doctrine du G29 et de l'EDPB. En effet, si un responsable de traitement veut mettre en place un traitement qui ne peut se fonder ni sur un transfert ni sur une décision d'adéquation, il remplit certes la première condition lui permettant d'avoir recours aux dérogations de l'article 49 du RGPD, mais cela ne signifie pas que l'application de l'article 49 soit opportune[995]. La lecture croisée de la solution de la CJUE et de la doctrine développée par l'EDPB aboutit plutôt à la conclusion selon laquelle chaque transfert de données vers les États-Unis fondé sur les articles 45 et 46 du RGPD devra être réévalué en fonction des éléments mis en exergue par la Cour de Justice (notamment le droit au recours et l'ingérence des autorités publiques américaines), sans que l'article 49 puisse être

---

[993] EDPB, *Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE,* 10 novembre 2020, p. 17.
[994] CJUE, C-311/18, *op. cit.*, §202.
[995] V. notamment en ce sens, TRACOL Xavier, « "Schrems II" : The return of the Privacy Shield », *Computer Law & Security Review*, Vol. 39, novembre 2020, disponible sur https://www.sciencedirect.com/science/article/pii/S0267364920300893 (consulté en septembre 2021).

utilisé comme une solution à long terme pour des traitements réguliers, dépourvus de tout caractère exceptionnel. Ainsi, certains traitements réguliers ne pouvant pas faire l'objet de garanties appropriées ne bénéficieront pas de la dérogation offerte par l'article 49 du RGPD. Le responsable de traitement est alors contraint de repenser le traitement, l'arrêter ou encore le relocaliser au sein de l'Union européenne[996]. Si la décision *Schrems II* n'a pas créé de vide juridique *stricto sensu*, elle a tout de même créé une grande insécurité juridique pour les exportateurs de données vers les États-Unis[997]. Par exemple, l'une des conséquences de l'insécurité juridique en ce qui concerne ces transferts a été la relocalisation des données dans l'Union européenne effectuée par Microsoft pour l'ensemble de ses services cloud, initiative dénommée « *EU Data Boundary for the Microsoft Cloud* » (« Frontière des données de l'Union européenne pour le Cloud Microsoft »)[998].

509. Si l'arrêt *Schrems II* a des effets bénéfiques sur la protection des données à caractère personnel en exigeant une protection réelle et effective des données transférées, l'absence de jurisprudence concernant les dérogations de l'article 49 a permis l'installation d'un *status quo*, témoignant parfois, chez certains acteurs, d'une méconnaissance générale des mécanismes de transferts[999]. Une clarification du caractère exceptionnel de l'article 49 aurait donc des effets bénéfiques sur la sécurité juridique des transferts. Cette clarification devrait s'accompagner d'un meilleur traitement judiciaire des questions relatives aux transferts de données à caractère personnel hors Union européenne à travers la clarification des mécanismes de recours applicables à ces transferts.

B. La clarification bienvenue des mécanismes de recours applicables aux transferts de données à caractère personnel hors Union européenne

510. Le mécanisme du guichet unique a connu une évolution substantielle entre la proposition de la Commission de 2012 et l'adoption du RGPD en 2016. Au sein de la

---

[996] La solution de la relocalisation des traitements au sein de l'Union européenne est notamment prônée par Maximillian Schrems. V. également CHANDER Anupam, «Is Data Localization a Solution for *Schrems II*?», *Journal of International Economic Law*, 2020, n° 23, pp. 1–14.

[997] Commission européenne, COM (2012) 11 final, *op. cit.*, p. 86.

[998] Microsoft, « Answering Europe's Call: Storing and Processing EU Data in the EU », *Microsoft.com*, 6 mai 2021, disponible sur https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/ (consulté en septembre 2021).

[999] Par exemple, la politique de confidentialité de Calendly affirme : « By submitting your personal data to Calendly and using Calendly, you expressly consent to have your personal data transferred to, processed, and stored in the United States or another jurisdiction which may not offer the same level of privacy protection as those in the country where you reside or are a citizen ». Or, quelques lignes plus tard, la politique de confidentialité révèle que les transferts de données à caractère personnel qu'effectue Calendly sont fondés sur des clauses contractuelles types. Calendly, *Avis sur la politique de confidentialité*, disponible sur https://calendly.com/fr/privacy (consulté en juillet 2022).

proposition de la Commission, l'article 51(2) semblait proposer une compétence exclusive de l'autorité de contrôle « chef de file », définie comme l'autorité de contrôle de l'établissement principal du responsable de traitement ou du sous-traitant[1000]. La Commission avait ainsi adopté la même logique qu'elle applique au marché intérieur, fondée sur le principe de reconnaissance mutuelle[1001]. Le contrôleur européen de la protection des données a, par la suite, exprimé ses regrets, estimant « que le rôle d'une autorité chef de file ne doit pas être perçu comme une compétence exclusive, mais plutôt comme un mode structuré de coopération avec d'autres autorités de contrôle compétentes »[1002]. Deux ans plus tard, le Conseil de l'Union européenne s'est raliée à la position du contrôleur européen de la protection des données, considérant qu'une « autorité chef de file ne peut pas faire cavalier seul »[1003] et que le RGPD doit opter pour un mécanisme de coopération entre les autorités de contrôle. Par conséquent, le contrôleur européen de la protection des données et le Conseil de l'Union européenne ont tous deux refusé une application du RGPD fondée sur une logique de marché intérieur au profit d'une application axée sur l'objectif de protection effective des individus d'un État membre[1004].

511. L'avis de ces deux entités a été écouté. Désormais, le mécanisme du guichet unique est consacré dès le préambule du RGPD qui dispose que « toute personne concernée devrait avoir le droit d'introduire une réclamation auprès d'une seule autorité de contrôle, en particulier dans l'État membre où elle a sa résidence habituelle »[1005]. Cette disposition est également présente en matière juridictionnelle. Désormais, la personne concernée peut choisir d'intenter une action devant une juridiction soit d'un État membre dans lequel « le responsable du traitement ou le sous-traitant dispose d'un établissement », soit d'un État membre dans lequel la personne concernée a sa résidence habituelle[1006]. Ce mécanisme s'inscrit dans la volonté plus large du législateur de procéder à une harmonisation de la protection des données au sein de l'Union européenne[1007]. Afin d'atteindre cet objectif, l'article 51(2) du règlement prévoit une obligation de coopération entre les autorités de contrôle.

[1000] Commission européenne, COM (2012) 11 final, *op. cit.*
[1001] HIJMANS Hielke, « Article 56. Competence of the lead supervisory authority», *in* KURNER Christopher, BYGRAVE Lee A., DOCKSEY Laura (dir.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press, p. 917.
[1002] EDPS *Avis du contrôleur européen de la protection des données sur le parquet,* 2012, §237.
[1003] Conseil de l'Union européenne, *Débat d'orientation sur le mécanisme de guichet unique*, Bruxelles, 26 mai 2014, Dossier interinstitutionnel 2012/0011 (COD), 10 139/14, §11.
[1004] HIJMANS Hielke, *op. cit.*, p. 917.
[1005] RGPD, 27 avril 2016, considérant 141
[1006] RGPD, 27 avril 2016, considérant 145.
[1007] L'objectif d'harmonisation est notamment inscrit au considérant 10 du RGPD.

512. Le mécanisme du guichet unique est doté de deux faces : une première face permettant la simplification des démarches de la personne concernée qui souhaite faire cesser une violation du règlement, et une seconde face de simplification des démarches du responsable de traitement qui lui offre la possibilité de centraliser l'ensemble de celles-ci devant une seule autorité de contrôle au sein de l'Union européenne. Ce dispositif innovateur du RGPD assure une simplification des démarches pour les entreprises établies au sein de l'Union européenne. En effet, ces entreprises bénéficient d'un interlocuteur unique, ce qui leur permet « de bénéficier d'un avantage concurrentiel fort puisqu'elles bénéficient des mécanismes harmonisés européens, tandis que les entreprises établies en dehors de l'Union, mais qui visent le marché européen continuent de devoir s'adresser à chacune des autorités de contrôle où elles adressent leurs services »[1008].

513. Le régime spécifique aux transferts transfrontaliers de données semble également relever du pragmatisme. Comme le remarque Émilie Brunet, juriste à la CNIL, ces situations concernent majoritairement « en pratique, les traitements mis en œuvre par les entreprises établies dans un seul État membre, mais dont les activités sont susceptibles d'impacter des personnes situées dans plusieurs États membres »[1009]. Plus précisément, pour les transferts de données à caractère personnel, le RGPD prévoit un mécanisme de guichet unique spécifique à l'article 56, imposant la désignation d'une autorité chef de file :

> « L'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable de traitement ou ce sous-traitant »[1010].

L'autorité de contrôle chef de file est définie par le G29 comme « l'autorité qui assume la responsabilité principale de la gestion d'une activité de traitement transfrontalier, par exemple lorsqu'une personne concernée introduit une réclamation concernant le traitement de ses données à caractère personnel »[1011].

514. Cependant, la mise en œuvre pratique du mécanisme du guichet unique dans le domaine des transferts de données à caractère personnel fait l'objet de conflits face à un risque important de *forum shopping* en cas de mauvaise application du système de coopération entre les États

---

[1008] BRUNET Émilie, « Les mécanismes de coopération des autorités de contrôle au sein de l'Union européenne et le Comité européen de la protection des données », *Revue de droit international d'Assas*, n° 2, décembre 2019, p. 5.
[1009] *Ibidem.*
[1010] RGPD, 27 avril 2016, article 56 (1).
[1011] Groupe de travail « Article 29 », *Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant*, adoptées le 13 décembre 2016, vision révisée et adoptée le 5 avril 2017, 16/FR, WP 244 rev.01, p. 5.

membres. En effet, le mécanisme de guichet unique a été soulevé plusieurs fois par des responsables de traitement établis en Irlande pour contester la compétence à adopter des décisions quant à la conformité des leurs transferts de données hors Union d'une autorité de contrôle d'un autre État membre de l'Union.[1012]

515. Le risque de *forum shopping* est d'autant plus présent que l'autorité de contrôle irlandaise, la *Data Protection Commission* (DPC), fait l'objet de nombreuses critiques relatives à son inefficacité. L'Irish Council for Civil Liberties (ICCL) a par exemple publié un rapport sur la paralysie de la mise en œuvre du RGPD en Europe, mettant en exergue la faible capacité des autorités de contrôle de s'opposer aux « Big Tech »[1013]. Ce rapport met en cause de nombreux facteurs, dont l'absence de moyens techniques et financiers ou encore une répartition très hétérogène des recours de grande ampleur. L'autorité de contrôle irlandaise est particulièrement pointée du doigt : l'ICCL affirme que 98% des 164 cas d'importance européenne[1014] qui lui ont été confiés ne sont pas résolus[1015]. Le Parlement européen s'est également saisi de la question dans une résolution adoptée le 20 mai 2021 concernant l'arrêt *Schrems II* : il est demandé à la Commission européenne « d'engager une procédure en manquement pour absence de contrôle satisfaisant de l'application du RGPD »[1016]. À cette occasion, le Parlement européen s'est dit :

> « fortement préoccupé par le fait que le commissaire irlandais à la protection des données n'ait pas encore tranché sur plusieurs réclamations concernant des infractions au RGPD déposées le 25 mai 2018, date de l'entrée en vigueur du RGPD, pas plus que sur d'autres plaintes émanant de groupes de consommateurs et autres alors qu'il est l'autorité de contrôle compétente au premier chef pour ces affaires ».

Les parlementaires ont affirmé leurs préoccupations non seulement sur le délai excessif « contrairement à l'intention du législateur » des décisions de l'autorité de contrôle irlandaise, mais également sur d'autres aspects tels que « la tentative infructueuse de l'autorité de

---

[1012] CNIL, Délibération de la formation restreinte n° SAN-2020-013 du 7 décembre 2020, *op. cit.* ; CE, juge des référés, 4 mars 2021, n° 449212 (requête déposée par la société Google LLC et la société Google Ireland Limited) ; CJUE, 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, C-645/19.

[1013] Irish Council for Civil Liberties, «Europe's enforcement paralysis. ICCL's 2021 report on the enforcement capacity of data protection authorities » .2021, p. 2.

[1014] Il s'agit de cas de transferts de données hors Union européenne qui implique parfois des acteurs importants comme Google, Facebook, Apple ou Microsoft.

[1015] Irish Council for Civil Liberties, 2021, *op. cit.*, p. 4.

[1016] Parlement européen, 20 mai 2021, *Résolution sur l'arrêt rendu par la Cour de justice de l'Union européenne le 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems (« arrêt Schrems II »),* 2020/2789 (RSP), §4.

protection des données de faire supporter à une partie défenderesse les coûts de la procédure judiciaire, ce qui aurait eu un effet dissuasif généralisé »[1017].

516. L'ensemble de ces éléments font naître une inquiétude quant à la question des transferts de données hors Union européenne qui risque d'être paralysée par l'autorité de contrôle irlandaise. En effet, le régime fiscal attractif de l'Irlande encourage de nombreuses grandes entreprises à s'installer à Dublin : s'y trouvent notamment Google, Facebook, Yahoo, LinkedIn, eBay, Amazon, Apple, Microsoft ou encore TikTok[1018]. Ainsi, les faiblesses de la DPC mises en exergue par le Parlement européen peuvent *de facto* exercer une influence substantielle sur la possibilité pour les personnes concernées d'obtenir gain de cause lorsqu'elles dénoncent une violation des transferts de données à caractère hors Union européenne de la part des GAFAM et autres *Big Tech*. La société civile s'est également emparée de la question, à l'image des activistes de *None of Your Business* (NOYB), avec à sa tête Maximilian Schrems. L'association accuse ouvertement l'autorité de contrôle irlandaise de vouloir donner le feu vert à un contournement du RGPD de la part de Facebook[1019].

517. Cependant, si l'autorité de contrôle chef de file assume la responsabilité principale d'un traitement transfrontalier, cela ne signifie pas pour autant qu'elle prend ses décisions indépendamment des autres autorités de contrôle. La Cour de Justice de l'Union européenne a ainsi répondu à certaines de ces inquiétudes en clarifiant le mécanisme de guichet unique, la notion d'autorité chef de file et la portée de l'obligation de coopération entre les autorités de contrôle. Il s'agissait en l'espèce d'un conflit opposant Facebook et l'autorité de protection des données belge (APD)[1020]. La première question du renvoi préjudiciel avait pour objectif de déterminer si la compétence de l'autorité chef de file était exclusive de la compétence des autorités de contrôle des autres États membres. La Cour de Justice a alors délivré une interprétation textuelle sous l'angle de la loyauté du mécanisme du guichet unique.

518. La Cour a tout d'abord répondu aux inquiétudes soulevées quant à l'attitude de l'autorité de contrôle irlandaise, en affirmant explicitement que :

> « le mécanisme de « guichet unique » ne saurait en aucun cas aboutir à ce qu'une autorité de contrôle nationale, en particulier l'autorité de contrôle chef de file, n'assume pas la responsabilité qui lui incombe

[1017] *Ibidem.*
[1018] The Guardian, « Will Ireland's corporation tax rise see tech companies leave Dublin? », *TheGuardian.com*, 23 octobre 2021, disponible sur https://www.theguardian.com/world/2021/oct/23/will-irelands-corporation-tax-rise-see-tech-companies-leave-dublin (consulté en octobre 2021).
[1019] NOYB, « Irish DPC greenlights Facebook "GDPR bypass" », *noyb.eu*, 13 octobre 2021, disponible sur https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass (consulté en octobre 2021).
[1020] CJUE, C-645/19, *op. cit.*.

> en vertu du règlement 2016/679 de contribuer à une protection efficace des personnes physiques contre des atteintes à leurs droits fondamentaux rappelés au point précédent du présent arrêt, sous peine d'encourager les pratiques d'un *forum shopping* notamment de la part des responsables de traitement, visant à contourner ces droits fondamentaux et l'application effective des dispositions de ce règlement en les mettant en œuvre »[1021].

Ainsi, la CJUE rappelle que la compétence de l'autorité chef de file s'inscrit dans l'obligation de coopération entre les États membres, et non dans une perspective de répartition stricte des compétences entre autorités de contrôle. Ainsi, comme le remarque Hielke Hijmans, l'obligation de coopération prévue par l'article 60 dispose que les autorités de contrôle doivent s'efforcer « de parvenir à un consensus »[1022]. Dès lors,

> « le concept de « chef de file » devrait être principalement compris comme un rôle procédural. L'autorité chef de file est responsable de la procédure et de la rédaction des décisions. Cependant, à la fin de la journée, sa position sur le fonds n'est pas plus forte que celle des autres autorités de contrôle »[1023].

519. Ce n'est que si cette obligation de coopération n'est pas respectée par l'autorité chef de file que l'autorité de contrôle concernée peut soit adopter une mesure provisoire, soit demander l'assistance du contrôleur européen des données. La notion d'autorité de contrôle concernée est définie par l'article 4(22) du RGPD. Il s'agit d'une autorité de contrôle qui relève d'un État membre sur lequel est établi le responsable de traitement ou le sous-traitant, d'une autorité de contrôle qui relève d'un État membre dans lequel les résidents sont des personnes concernées « sensiblement affectées par le traitement […] ou susceptibles de l'être » ou encore d'une autorité de contrôle devant laquelle une réclamation a été introduite. Cette autorité, si elle estime que l'autorité de contrôle chef de file n'a pas satisfait sa demande d'assistance dans le délai établi par l'article 61(8) du RGPD (soit un mois à compter de la réception de la demande), peut tout de même adopter une mesure provisoire sur le territoire de l'État membre dont elle relève[1024]. De plus, l'article 64(2) prévoit que toute autorité de contrôle est en mesure de « demander que toute question d'application générale ou produisant des effets dans plusieurs États membres soit examinée par le comité en vue d'obtenir un avis, en particulier lorsqu'une autorité de contrôle compétente ne respecte pas les obligations relatives à l'assistance mutuelle »[1025]. Enfin, si elle estime que les circonstances exceptionnelles impliquent que des

[1021] *Idem,* § 68.
[1022] RGPD, 27 avril 2016, article 60 (1).
[1023] HIJMANS Hielke, *op. cit.*, p. 918.
[1024] RGPD, 27 avril 2016, article 61 (8).
[1025] RGPD, 27 avril 2016, article 64 (2).

mesures définitives doivent être adoptées en urgence, l'autorité de contrôle concernée peut demander à l'EDPB un avis d'urgence ou une décision contraignante d'urgence[1026].

520. Ainsi, la CJUE reprend l'ensemble de ces dispositions afin de rappeler qu'une autorité de contrôle « chef de file » ne détient pas de compétence exclusive en matière de transferts de données à caractère personnel. L'obligation de coopération prévoit en effet que l'autorité chef de file n'a pas de position dominante en matière de position sur le fonds, et doit « tenir le plus grand compte » des observations et avis des autres autorités de contrôle[1027]. Certes, une telle procédure peut entraîner le ralentissement du traitement des recours concernant les transferts de données à caractère personnel. Néanmoins, cette procédure est un moyen de garantir efficacement l'application effective et homogène du RGPD sur l'ensemble des États membres de l'Union européenne, permettant à la fois de faciliter la circulation des données au sein de l'Union européenne, et de protéger les personnes concernées[1028].

521. Ces garanties procédurales sont d'autant plus importantes pour les traitements à risque. En effet, il vient d'être étudié que les transferts de données à caractère transfrontaliers comportaient des risques pour la personne concernée, dont le consentement est susceptible d'être biaisé par la complexité juridique de tels traitements. Il est donc essentiel que les autorités de contrôle soient à même de contrôler le comportement des responsables de traitement en matière de transferts de données et, plus particulièrement, de vérifier la garantie effective des conditions de validité du consentement pour permettre de fonder le traitement sur cette base légale.

522. Conclusion de Section. – Les transferts de données à caractère personnel ne semblent pas compatibles avec la base légale du consentement dans la mesure où ils sont à la fois complexes à comprendre pour la personne concernée, et complexes à mettre en œuvre pour le responsable de traitement. Le régime du consentement semble également s'opposer à la pratique actuelle des transferts des données à caractère personnel puisqu'il n'offre ni une sécurité juridique satisfaisante aux responsables de traitement ni un mécanisme de recours permettant une évaluation fluide des questions relatives aux transferts. Dans ce cadre, le consentement ne devrait pas constituer une base juridique pour les traitements, du fait de la

---

[1026] RGPD, 27 avril 2016, article 66 (1), article 66 (2).
[1027] RGPD, 27 avril 2016, articles 60 à 66 ; CJUE, 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit,* C-645/19, §61 ; HIJMANS Hielke, *op. cit.*, p. 922.
[1028] BLUME Peter, « Article 61. Mutual Assistance», *in* KURNER Christopher, BYGRAVE Lee A., DOCKSEY Laura (dir.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press, p. 979.

complexité résultat à la fois du traitement et du cadre juridique s'y appliquant. À cette difficulté s'en ajoute une autre concernant tout particulièrement le fondement du consentement : le consentement aux traitements faisant appel à de l'intelligence artificielle.

Section 2 – La complexité des traitements relatifs à l'intelligence artificielle

523. Le phénomène *big data* fascine autant qu'il interroge. D'un côté, le *big data* est un objet d'innovation technologique permettant de générer différents types d'opportunités comme l'augmentation de la productivité, l'appréhension améliorée des défis posés à la société, l'amélioration de la recherche, la rapidité de l'innovation, la personnalisation des services, la réduction des coûts ou encore l'efficacité du service public[1029]. D'un autre côté, le *big data* questionne le chercheur tant son développement se situe à l'intersection entre les capacités technologiques, les capacités d'analyse et un aspect mythologique constitué par « la croyance largement répandue que les grands ensembles de données offrent une forme supérieure d'intelligence et de connaissances qui peuvent générer des idées qui étaient auparavant impossibles, avec une aura de vérité, d'objectivité et d'exactitude »[1030]. Ainsi, si le *big data* peut s'appréhender en tant qu'opportunité, il reste important de garder à l'esprit qu'il comporte également des limites.

524. À travers le phénomène de l'analyse de données en masse (*big data analysis*), les notions de personne concernée[1031] et de consentement de la personne concernée au traitement de ses données à caractère personnel semblent inadaptées lorsqu'il s'agit de protéger la personne. D'une simple interconnexion des personnes sur internet, les traitements commerciaux de données à caractère personnel vont aujourd'hui chercher à constituer des profils ou des schémas comportementaux non plus d'une personne concernée, mais d'un groupe de personnes concernées[1032]. Désormais, les données sont donc utilisées pour créer des groupes selon leurs

---

[1029] Commission européenne, « Big data », *Europa.eu*, disponible sur https://digital-strategy.ec.europa.eu/en/policies/big-data (consulté en juin 2021).

[1030] « *the widespread belief that large data sets offer a higher form ofintelligence and knowledge that can generate insights that were previouslyimpossible, with the aura of truth, objectivity, and accuracy* » [traduction libre]. BOYD Danah, CRAWFORD Kate, «Critical Questions for Big Data», *Information, Communication & Society*, 15(5), 2012, p. 663.

[1031] Le RGPD et la directive 95/46/CE ont tous deux repris la définition de la personne concernée proposée par les lignes directrices de l'OCDE de 1980 : la personne concernée est définie comme la personne physique identifiée ou identifiable par toute information. RGPD, 27 avril 2016, Art. 4 (1) ; Directive 95/46/CE, 24 octobre 1995, art. 2 : OCDE, *op. cit.*, §1.

[1032] ROSIER Karen, « Titre 12 – La notion de "donnée à caractère personnel" a-t-elle encore un sens dans la protection des données de communications électroniques ?», *in* DEGRAVE Élise *et al.* (dir.), *Law, Norms and Freedom in Cyberspace/Droit, normes et libertés dans le cybermonde*, Larcier, Liber Amicorum Yves Poulet, 2018, p. 699.

qualités, leurs intérêts ou encore leurs habitudes pour prédire le comportement d'un individu en raison de son appartenance à ce groupe[1033].

525. Une nouvelle approche, prenant en compte ces éléments, doit voir le jour afin de protéger la personne concernée plus efficacement qu'avec le mécanisme du consentement tel qu'envisagé par le RGPD. Avant de s'intéresser aux initiatives déjà présentes et en cours de discussion devant les instances européennes, il convient de définir deux notions primordiales que sont l'intelligence artificielle d'une part et le *big data* d'autre part. Selon la CNIL, le *big data* désigne les ensembles de données traitées répondant « à trois caractéristiques principales : volume, vélocité et variété »[1034]. Cette définition des « 3V » est parfois complétée par une quatrième caractéristique (« un quatrième V ») : la véracité, incluant ainsi une variable relative à la qualité des données collectées et de leur analyse[1035]. Une approche incluant également la capacité d'utilisation de ces grandes qualités de données a été proposée par le Conseil d'État en 2014, à travers un « cinquième V » : « la valeur attendue » de l'exploitation de ces grandes quantités de données[1036]. Cependant, le critère de la diversité ne semble pas retenu par la Commission européenne qui définit le *big data* comme la production très rapide de grandes quantités de données par un grand nombre de sources variées[1037]. Ainsi, le *big data* désigne globalement un système de collecte et de stockage des données dont l'ampleur, la rapidité et la diversité sont suffisamment importantes pour se distinguer des autres traitements. C'est pourquoi la traduction française la plus retenue a été « données massives »[1038].

526. Le terme d'intelligence artificielle désigne pour sa part la technique utilisée pour traiter les données et à son objectif. La proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle définit le système d'intelligence artificielle comme « un logiciel qui est développé au moyen d'une ou plusieurs techniques et approches énumérées à l'annexe I [approches d'apprentissage automatique, approches fondées sur la logique et les connaissances ou approches statistiques[1039]] et qui peut, pour un ensemble donné d'objectifs

---

[1033] MANTERELO Alessandro, «Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection», *Computer Law & Security Review*, Vol. 32, Issue 2, avril 2016, p. 239.
[1034] CNIL, « Big data », *Cnil.fr*, disponible sur https://www.cnil.fr/fr/definition/big-data (consulté en juin 2021).
[1035] WARD Jonathan Stuart, BARKER Adam, « Undefined By Data: A Survey of Big Data Definitions », 20 septembre 2013, arXiv:1309.5821 [cs.DB].
[1036] Conseil d'État, *Le numérique et les droits fondamentaux*, Les rapports du Conseil d'État, 2014, p. 48.
[1037] « *Big data refers to large amounts of data produced vert quickly by a high number of diverse sources* ». Commission européenne, « Big Data », europa.eu, disponible sur https://digital-strategy.ec.europa.eu/en/policies/big-data (consulté en juin 2021).
[1038] CNIL, « Big data », *op. cit.*
[1039] Commission européenne, 2021/0106 (COD), *op. cit.*, article 3 (1).

définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit »[1040]. La Commission a ainsi choisi d'adopter une définition large de l'intelligence artificielle, ce qu'elle avait annoncé dans son livre blanc : « la définition de l'IA devra être suffisamment souple pour tenir compte des progrès techniques tout en étant suffisamment précise pour garantir la sécurité juridique nécessaire »[1041]. Si la définition de l'intelligence artificielle ne prend pas en compte le caractère massif de la collecte et du stockage de données, force est de constater que, par son approche technique fondée sur la comparaison de données (qu'il s'agisse de l'apprentissage, de la logique ou de la statistique), l'intelligence artificielle va nécessairement avoir besoin d'une quantité importante de données pour pouvoir fonctionner de manière optimale. Il s'agit ici donc d'un point d'interaction entre les notions de *big data* et d'intelligence artificielle.

527. L'intelligence artificielle crée de nouveaux risques qui vont au-delà de la simple protection des données à caractère personnel. Le livre blanc de la Commission européenne sur l'intelligence artificielle souligne que le développement de systèmes d'intelligence artificielle peut avoir des conséquences sur « la sécurité et le bon fonctionnement du régime de responsabilité » lorsque ces systèmes sont intégrés dans des produits et services[1042]. Ces risques rendent nécessaire la réflexion sur les questions de cybersécurité ou encore de couverture internet et de perte de connectivité[1043]. Cependant, les nouveaux risques posés par le développement des systèmes d'intelligence artificielle ne se limitent pas aux questions de l'atteinte physique de la personne. En effet, si l'objectif de l'intelligence artificielle n'est pas toujours de prendre des décisions impliquant des individus, les applications de *machine learning* dont les décisions ont des conséquences sur les individus sont nombreuses. Solon Barocas, Moritz Hart et Arvind Narayanan se sont par exemple intéressés aux trente principaux concours de sciences des données (en les classant par prix)[1044]. Dans quatorze de ces concours, l'objectif assigné aux candidats était de prendre des décisions sur les individus[1045]. Dans cinq autres concours, si l'objectif assigné n'est pas de prendre des décisions concernant les individus, les décisions découlant des modèles développés ont néanmoins eu un effet direct sur les

[1040] Commission européenne, 2021/0106 (COD), *op. cit.*, annexe I.
[1041] Commission européenne, COM (2020) 65 final, *op. cit.* p. 19.
[1042] *Idem*, p. 15.
[1043] *Idem*, p. 18.
[1044] BAROCAS Solon, HARDT Moritz, NARAYANAN Arvind, *Fairness and Machine Learning. Limitations and Opportunities*, disponible sur https://fairmlbook.org/pdf/fairmlbook.pdf (consulté en juin 2021), p.17.
[1045] *Ibidem.*

individus[1046]. Dès lors, l'intelligence artificielle détient un potentiel d'influence inédit sur le fonctionnement de la société. L'étude préliminaire sur l'éthique de l'intelligence artificielle de l'UNESCO souligne ainsi que de sa nature de « technologie cognitive », les implications de l'intelligence artificielle sont « intimement lié[e]s aux domaines centraux » que sont l'éducation, la science et la communication[1047]. De plus, la popularisation et l'arrivée de plus en plus massive de produits utilisant l'intelligence artificielle sur le marché accentuent cette influence puisque l'IA va désormais influencer la vie quotidienne et la vie professionnelle à travers les secteurs de la santé, de l'éducation, de la recherche scientifique, des communications, des transports, de la sécurité ou encore de l'art[1048].

528. Parmi les risques créés par l'utilisation de l'intelligence artificielle, la question de la protection des données à caractère personnel est centrale. Le RGPD est ainsi mobilisé par l'existence de volumes de données à caractère personnel collectées et déduites, dont l'exploitation peut constituer une ingérence dans le droit à la vie privée, le droit à la protection des données à caractère personnel, le droit de ne pas faire l'objet de discriminations, etc. En plus du régime général de protection des données à caractère personnel établi par le règlement, le RGPD s'intéresse plus particulièrement à la prise de décision automatisée en créant un droit spécifique. Dans ses lignes directrices relatives à la prise de décision automatisée, le G29 rappelle en effet que « le profilage et la prise de décision automatisée peuvent poser des risques importants pour les droits et libertés des personnes »[1049]. Au-delà du RGPD, l'intelligence artificielle, et plus particulièrement la prise de décision automatisée, est également au cœur d'une réflexion impliquant les citoyens, les autorités de contrôle et le législateur[1050].

529. Dans un contexte de popularisation des technologies artificielles, il est donc important de réfléchir à la place de l'individu dans ces traitements de données à caractère personnel. D'une part, la question de fonder des traitements impliquant l'intelligence artificielle (comme la publicité comportementale) sur le consentement relève de l'autonomie de la personne, le

---

[1046] *Ibidem.*

[1047] Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), Commission mondiale d'éthique des connaissances scientifiques et des technologies (COMEST), *Étude préliminaire sur l'éthique de l'intelligence artificielle*, Paris, 26 février 2019, SHS/COMEST/EXTWG-ETHICS-AI/2019/1, p. 3.

[1048] *Ibidem.*

[1049] Groupe de travail « Article 29 », *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, adoptées le 3 octobre 2017, Version révisée et adoptée le 6 février 2018, WP251 rev.01, p. 6.

[1050] La proposition de règlement sur l'intelligence artificielle est le résultat d'un processus de consultation impliquant le législateur et les parties prenantes. V. Commission européenne, « Une Europe adaptée à l'ère du numérique : La Commission propose de nouvelles règles et actions en faveur de l'excellence et de la confiance dans l'intelligence artificielle », *Communiqué de presse*, Bruxelles, 21 avril 2021, disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_1682 (consulté en décembre 2021).

traitement étant si intrusif qu'il ne saurait être justifié par une autre variable que le choix de la personne concernée. D'autre part, le consentement est loin d'apparaître comme une solution idéale en matière d'intelligence artificielle, tant les conséquences d'un traitement de données à caractère personnel automatisé peuvent être importantes sur la personne concernée.

530. En effet, la création d'un droit de ne pas faire l'objet d'une décision automatisée ne semble pas suffisante à protéger la personne concernée de l'ensemble des risques inédits[1051] que comportent les traitements de données à caractère personnel utilisant une technologie d'intelligence artificielle. Ces risques sont à la fois individuels, mais également collectifs puisque l'utilisation d'un système d'intelligence artificielle a le potentiel de léser un groupe, voire la société dans son ensemble[1052]. Dans ce contexte, la place du consentement de l'individu se heurte à l'existence de préjudices collectifs, à la complexité technique des systèmes d'intelligence artificielle, ou encore à la capacité pour l'individu d'identifier les risques relatifs à l'utilisation de tels systèmes. La solution proposée par le RGPD de pouvoir consentir aux traitements de données à caractère personnel et de pouvoir renoncer au droit de ne pas faire l'objet d'une décision automatisée en consentant explicitement à un tel traitement n'est dès lors pas satisfaisante.

531. La démonstration de l'inadéquation de l'approche du RGPD en l'état sera illustrée par la protection de la personne concernée contre les biais algorithmiques, qui constituent un risque systémique de l'utilisation de l'intelligence artificielle (§1). L'existence de ces risques, à la fois difficiles à détecter et difficiles à prévenir, nécessite une réflexion du législateur sur la conciliation entre autonomie des personnes concernées et complexité des risques relatifs à l'intelligence artificielle (§2).

§1 – L'identification difficile des biais algorithmiques

532. L'identification des biais algorithmiques constitue une étape essentielle afin de protéger la personne concernée contre une exploitation de ses données à caractère personnel qui aurait des conséquences injustes envers elle ou limiterait l'exercice de ses droits, comme le droit de ne pas faire l'objet d'une discrimination. Le développement de l'intelligence artificielle constitue pourtant une opportunité pouvant « procurer de nombreux avantages économiques et

[1051] EDPB, EDPS, *Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down hamonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 juin 2021, 5/2021, p. 5; Commission européenne, COM/2021/206 final, *op. cit.*, considérant 4.
[1052] EDPB, EDPS, 5/2021, *op. cit.*, p. 6.

sociétaux »[1053]. Afin de concilier le développement d'une technologie qui pourrait avoir un effet bénéfique sur l'économie et la société et la protection des personnes, le législateur doit être conscient du fait que l'intelligence artificielle comporte des risques liés à la création, à l'entraînement ou encore à l'utilisation des algorithmes : la création de biais algorithmiques.

533. Un biais se définit comme une « inclinaison ou préjugé en faveur ou en défaveur d'une personne ou d'un groupe, en particulier lorsque cette inclinaison ou préjugé est considéré comme injuste »[1054]. La définition du biais est explicite quant aux dangers que ceux-ci représentent, soit les risques de discrimination, de manipulation et de décision injuste envers la situation d'une personne. Dans son livre blanc consacré à une intelligence artificielle de confiance, la Commission avait identifié les « failles dans la conception globale des systèmes d'IA » et « l'utilisation de données sans correction de biais éventuels » comme un risque du recours à l'intelligence artificielle pour les droits fondamentaux[1055]. La question des biais est d'autant plus importante que le recours à l'exploitation de données massives par les systèmes d'intelligence artificielle a pour conséquence que « la qualité, le volume et le contenu des données influencent le fonctionnement des systèmes et entraînent souvent la reproduction et l'amplification des biais, erreurs et lacunes présentes dans les données » selon le Comité *ad hoc* sur l'intelligence artificielle (CAHAI)[1056].

534. L'identification des biais algorithmiques semble dès lors essentielle, mais difficile à effectuer. La sophistication des modèles mathématiques et de l'analyse de quantités massives de données ne permet pas à toute personne de comprendre et identifier les modèles mathématiques afin de déterminer comment une décision mauvaise, voire préjudiciable, a pu être calculée. L'opacité de l'intelligence artificielle envers les personnes concernées par ses décisions a été décrite par Cathy O'Neil :

> « Bon nombre de ces modèles ont encodé les préjugés, les malentendus et les préjugés humains dans les systèmes logiciels qui géraient de plus en plus nos vies. Comme des dieux, ces modèles mathématiques étaient opaques, leurs fonctionnements invisibles à tous sauf aux plus hauts prêtres de leur domaine : les mathématiciens et les informaticiens. Leurs verdicts, même erronés

[1053] Commission européenne, COM/2021/206 final, *op. cit.*, p. 1.
[1054] Lexico, « Bias », *Lexico.com*, Oxford University, disponible sur https://www.lexico.com/definition/bias (consulté en juin 2021).
[1055] Commission européenne, COM (2020) 65 final, *op. cit.*, p. 13.
[1056] Comité *ad hoc* sur l'intelligence artificielle (CAHAI), *Vers une régulation des systèmes d'IA. Perspectives internationales sur l'élaboration d'un cadre juridique fondé sur les normes du Conseil de l'Europe dans le domaine des droits de l'homme, de la démocratie et de l'État de droit*, Étude du Conseil de l'Europe, décembre 2020, DGI (2020) 16, p. 23.

> ou préjudiciables, étaient sans contestation ni appel. Et ils avaient tendance à punir les pauvres et les opprimés au sein de notre société, tout en enrichissant les riches ».[1057]

Cette description insiste sur le double caractère individuel et collectif des préjudices liés aux biais algorithmiques. Qualifiés d'« armes de destruction mathématique » par l'autrice, les algorithmes présentent des biais qu'il convient de prévenir et identifier afin d'éviter la survenance d'une décision algorithmique injuste, ou en réparer les dommages.

535. La première difficulté obstruant l'identification des biais algorithmiques est donc l'opacité des modèles mathématiques. Cependant, il ne s'agit pas de la difficulté principale puisque les biais algorithmiques ne résultent que très rarement d'une erreur dans le code du système d'intelligence artificielle[1058]. Les « hauts prêtres » que désigne Cathy O'Neil peuvent ainsi se révéler créateurs de biais, sans être forcément capables de les identifier. L'absence d'intentionnalité complexifie l'identification des biais algorithmiques. En effet, leur nature ne résulte pas forcément de l'attitude malveillante d'un agent, mais d'une série d'interactions imprévisibles mêlant rationalité absolue, bases de données inexactes ou imparfaites et limites du raisonnement humain[1059]. L'identification du biais est d'autant plus difficile que, plus que l'enchevêtrement des sources, la psychologie humaine a tendance à privilégier l'interprétation téléologique des événements, phénomène appelé « biais d'intentionnalité »[1060]. Ce biais d'intentionnalité s'additionne à la croyance d'une rationalité objective de la décision algorithmique :

> « Le fait que la décision émerge d'un objet mathématique, comme la construction d'un modèle par un processus d'apprentissage indépendant d'une intervention humaine (dans la définition de sa représentation interne, tout du moins), participe à une impression de neutralité du processus de décision automatique »[1061].

[1057] O'NEIL Cathy, *Weapons of Math Destruction*: *How Big Data Increases Inequality and Threatens Democracy*, Crown, 2016, p. 3

[1058] Il faut tout de même garder à l'esprit que les discriminations créées par les systèmes d'intelligence artificielle peuvent relever de l'intentionnalité. L'exemple de l'algorithme de livraison d'Amazon n'offrant pas un service de livraison en 24 h dans les quartiers à prédominance noire de la ville de Boston illustre bien la possibilité pour les décideurs de créer des algorithmes discriminatoires de manière intentionnelle. MACLURE Jocelyn, SAINT-PIERRE Marie-Noëlle, « Le nouvel âge de l'intelligence artificielle : une synthèse des enjeux éthiques », *Les Cahiers de propriété intellectuelle*, Vol. 30, n° 3, p. 755.

[1059] NERA Kenzo, « Biais de raisonnement et dangers des algorithmes », *TheConversation.com*, 19 août 2019, disponible sur https://theconversation.com/biais-de-raisonnement-et-dangers-des-algorithmes-120543 (consulté en juillet 2022).

[1060] *Ibidem.*

[1061] DELTORN Jean-Marc, « La protection des données personnelles face aux algorithmes prédictifs », *RDLF*, 2017, chron. N° 12, disponible sur www.revuedlf.com/droit-ue/la-protection-des-donnees-personnelles-face-aux-algorithmes-predictifs/ (consulté en juillet 2022).

536. Or, la neutralité du processus de décision automatique a de nombreuses fois été démentie par l'influence des personnes à l'origine du modèle mathématique ou encore des jeux de données utilisés pour entraîner l'intelligence artificielle. En 2015, Amazon découvre que son intelligence artificielle discrimine les femmes à l'embauche parce que le jeu de données comportait une banque de curriculum vitae largement dominée par des postes occupés par des hommes. En 2016, ProPublica démontre que l'intelligence artificielle COMPAS discrimine les personnes noires en prédisant un plus haut taux de risque de récidive que les personnes blanches[1062]. L'identification des biais algorithmiques a été difficile, de l'absence d'élément intentionnel dans la construction des modèles mathématiques de l'intelligence artificielle. L'exemple de COMPAS est particulièrement parlant : l'objectif des concepteurs de l'algorithme était justement de prévenir les préjugés raciaux dans les décisions judiciaires, fruits des préjugés des juges et jurés :

> « Naturellement, les concepteurs de l'algorithme ont exclu la couleur de peau des informations utilisées pour calculer le risque de récidive criminelle »[1063].

En dehors des biais intentionnels, les biais algorithmiques proviennent soit de biais cognitifs insérés dans le code du fait des croyances de la personne à l'origine du code[1064], soit de biais statistique et de stéréotypes liés au caractère conservateur de l'intelligence artificielle[1065].

537. Dans le premier cas, le biais constituera la traduction des biais du développeur de l'algorithme puisque le développeur va y insérer, volontairement ou involontairement, ses propres biais, « caractérisés par ses croyances, goûts, idéologies, etc. » [1066]. En avril 2019, une publication du *AI Now Institute* constatait une « crise de la diversité » dans le secteur de l'intelligence artificielle. Par exemple, seulement 18% des auteurs sont des femmes et plus de 80% des professeurs sur l'intelligence artificielle sont des hommes[1067]. Dans le secteur privé, les femmes ne sont pas non plus très représentées puisqu'elles représentent seulement 15% de

---

[1062] ZUIDERVEEN BORGESIUS Frederik, *op. cit.*, pp. 23-24.
[1063] NERA Kenzo, *op. cit.*
[1064] Le biais peut en effet résulter de l'humain sans être intentionnel, la personne à l'origine du code utilisant ses propres intuitions de la morale lors de la conception de l'algorithme. REICH Rob, SAHAMI Mehran, WEINSTEIN Jeremy M., *System Error. Where Big Tech Went Wrong and How we Can Reboot*, Harper, 2021, p. 94.
[1065] HAAS Gérard, ASTIER Stéphane, « Les biais de l'intelligence artificielle : quels enjeux juridiques ? », *Répertoire IP/IT et Communication*, juillet 2019.
[1066] CHAPUS Lucie, D'YVOIRE Anne-Victoire, « Le développement d'une intelligence artificielle éthique est un enjeu primordial pour les entreprises », *LeMonde.fr*, 15 novembre 2019, Tribune, disponible sur https://www.lemonde.fr/idees/article/2019/11/15/le-developpement-d-une-intelligence-artificielle-ethique-est-un-enjeu-primordial-pour-les-entreprises_6019262_3232.html (consulté en juin 2021).
[1067] WEST Sarah Myers, WHITTAKER Meredith, CRAWFORD Kate, «Discriminating Systems: Gender, Race, and Power in AI», *AI Now Institute*, avril 2019, disponible sur https://ainowinstitute.org/discriminatingsystems.pdf (consulté en juin 2021), p. 3.

l'équipe de recherche en intelligence artificielle de Facebook et 10% de celle de Google[1068]. La situation est encore pire quant aux Afro-Américains puisqu'ils ne représentent que 2,5% de la force de travail de Google, et 4% de celles de Facebook et Microsoft[1069]. Cette absence de représentation peut être à l'origine de biais cognitifs qui vont venir contaminer et biaiser le système d'intelligence artificielle.

538. La « crise de la diversité » de l'intelligence artificielle a des conséquences sur l'apparition de biais cognitifs intégrés au code de l'intelligence artificielle. Selon Kate Crawford, « comme toute technologie, l'intelligence artificielle reflétera les valeurs de ses créateurs »[1070]. Les biais cognitifs ne doivent donc pas être sous-estimés dans la conception de systèmes d'intelligence artificielle tant « les biais cognitifs semblent fiables, systématiques et difficiles à éliminer »[1071]. Ces biais doivent d'autant plus être identifiés que l'expression de biais cognitifs est directement liée à l'agent humain. Il a par exemple été démontré que l'explicabilité des décisions prises par l'intelligence artificielle était reliée à l'intuition de l'auteur de l'explication[1072]. L'identification des biais cognitifs intégrés au code est ainsi complexe, puisque l'auteur du biais ne sera pas forcément conscient des biais cognitifs dont il est l'auteur. Par exemple, le biais d'information a pour effet qu'une information supplémentaire peut faire paraître l'apparition d'une règle plus plausible, alors même que l'information n'est pas pertinente. Un tel biais cognitif relève de l'intuition et peut être difficile à identifier du fait qu'elle se fonde sur des sources informatives[1073].

539. Dans le second cas, les biais de statistiques sont liés aux informations contenues dans les bases de données utilisées dans la création du système d'intelligence artificielle. En effet, souvent, l'intelligence artificielle va utiliser un processus d'induction dont l'objectif sera de définir des règles générales à partir d'exemples spécifiques fournis par la base de données[1074]. L'utilisation d'importantes bases de données en matière de volume et la création de règles à partir d'un modèle déterminé depuis cet important volume de données ont pour conséquence

---

[1068] *Idem,* p. 5.
[1069] *Ibidem.*
[1070] CRAWFORD Kate, « Artificial Intelligence's White Guy Problem », *The New York Times*, 25 juin 2016, disponible sur https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html (consulté en juin 2021).
[1071] KAHNEMAN Daniel, TVERSKY Amos, « Subjective Probability: A Judgement of Representativeness », *Cognitive Psychology*, Juillet 1972, Vol. 3, Issue 3, pp. 430-454.
[1072] MILLER Tim, «Explanation in Artificial Intelligence: Insights from the Social Sciences», *Artificial Intelligence,* Vol. 267, Février 2019, pp. 1–38.
[1073] KLIEGR Tomáš, BAHNÍK Štěpán, FÜRNKRANZ Johannes, , « A Review of Possible Effects of Cognitive Biases on Interpretation of Rule-Based Machine Learning Models », *Artificial Intelligence*, Juin 2021, Vol. 295.
[1074] BAROCAS Solon, HARDT Moritz, NARAYANAN Arvind, *op. cit.,* p.12.

que les systèmes d'intelligence artificielle peuvent être sujets à des erreurs lorsque cette base de données n'est pas exacte. Une base de données exacte peut également être à l'origine de biais discriminatoires. En effet, de nombreux indicateurs sociaux sont le reflet de la persistance de situations discriminatoires dans la société[1075]. La question est d'autant plus épineuse que l'immoralité de la discrimination a rendu celle-ci insidieuse au point que « ces comportements s'immisceraient dans les rencontres intergroupes à l'insu des interlocuteurs eux-mêmes »[1076]. De plus, la dissimulation de la discrimination crée une difficulté de perception de la discrimination par la victime de la discrimination, alors même que celle-ci sera apte à identifier la discrimination subie par son groupe[1077].

540. Si la discrimination est peu perceptible par son auteur et par sa victime, elle a des conséquences en terme social, créant des indicateurs sociaux biaisant l'intelligence artificielle[1078]. Par exemple, selon l'INSEE, en 2018, les femmes avaient un salaire en équivalent temps plein inférieur de 16,8% à celui des hommes[1079]. En 2013, Anthony Edo et Nicolas Jacquemet estimaient à une moyenne de 40% le taux de discrimination à l'embauche à l'encontre des candidats issus de l'immigration[1080]. Or, ces chiffres ne sont pas neutres et peuvent biaiser les systèmes d'intelligence artificielle, notamment lorsque ceux-ci reposent sur un système de *machine learning*. L'exemple du programme de recrutement d'Amazon précité est parlant. Il a en effet été découvert que ce programme avait appris à préférer embaucher les hommes et pénalisait le score de CVs comportant le mot « *women* »[1081]. L'intelligence artificielle avait été entraînée à trier les candidatures en observant des modèles dans les *curriculum vitae* (CVs) reçus par la société pendant une période de 10 ans : or, la majorité de ces CVs provenait d'hommes, qui sont surreprésentés dans le domaine des nouvelles

---

[1075] WILLIAMS Betsy Anne *et al.*, «How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions and Policy Implications», *Journal of Information Policy*, 2018, Vol. 8, p. 81.

[1076] AUDÉ Benoite, *De la perception sociale à la discrimination : une contribution à l'étude des déterminants précoces des comportements discriminatoires*, Thèse de Psychologie sous la direction de RIC François, Université de Bordeaux, 2015, p. 186.

[1077] BASTART Jennifer, *La détection de la discrimination par un observateur : Le rôle de la catégorisation sociale du discriminateur et de la légitimité du comportement du discriminateur*, Thèse pour l'obtention du grade de docteur en sciences cognitives, psychologie et neurocognition sous la direction de DELMAS Florian et MULLER Dominique, Université de Grenoble, 2006, p. 4.

[1078] WILLIAMS Betsy Anne *et al., op. cit.*, p. 81.

[1079] INSEE, « Écart de salaires en équivalent temps plein entre femmes et hommes », Insee.fr, *Tableau de bord de l'économie française*, 5 mai 2021, disponible sur https://www.insee.fr/fr/outil-interactif/5367857/details/40_SOC/44_EGF/44G_Figure7 (consulté en juin 2021).

[1080] EDO Anthony, JACQUEMET Nicolas, « Discrimination à l'embauche selon l'origine et le genre : défiance indifférenciée ou ciblée sur certains groupes ? », *Économie et Statistique*, n° 464-465-466, 2013, p. 155.

[1081] Reuters, « Amazon scraps secret AI recruiting tool that showed bias against women », *Reuters.com*, 11 octobre 2018, disponible sur https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G (consulté en juin 2021).

technologies[1082] . Autre exemple, une étude de 2019 publiée dans *Science* avait détecté un biais racial dans l'intelligence artificielle utilisée pour prendre des décisions de santé[1083]. En effet, l'intelligence artificielle utilisée pour détecter les patients à haut risque se fondait sur les données relatives aux dépenses de santé des patients, et privilégiait ainsi le soin des patients blancs dans la mesure où plusieurs facteurs[1084] ont pour conséquence que les patients noirs ont des dépenses de santé inférieures pour un même état de santé[1085].

541. Ainsi, l'intelligence artificielle amplifie les biais discriminatoires, qui sont présents de différentes manières dans la société. Les bases de données mesurant l'état du monde seront biaisées par les phénomènes qu'elles mesurent, le modèle émanant du processus d'apprentissage à partir des données relevées sera biaisé par ces dernières, et l'application du modèle aux individus révélera ainsi les biais discriminatoires présents dans la société[1086]. L'objectif d'objectivité visé par la méthode scientifique par « l'application d'un processus dépassionnée par lequel les hypothèses sont proposées et testées » n'est pas forcément atteint par l'ingestion de quantités massives de données par l'intelligence artificielle[1087]. En effet, le nettoyage des données et l'interprétation des données seront teintés de subjectivité, laquelle variera selon la discipline et les pratiques de l'institution de son auteur[1088].

542. L'identification des biais algorithmiques est également complexifiée par l'absence de transparence sur les jeux de données utilisés et le caractère propriétaire d'un algorithme, empêchent également de mener des recherches sur la raison pour laquelle ces biais algorithmiques apparaissent. Cet obstacle est amplifié par le caractère opaque de la technicité des technologies d'intelligence artificielle, et plus particulièrement du *machine learning* (apprentissage automatique) et du *deep learning* (apprentissage profond). En effet, « l'utilisation de réseaux de neurones profonds » a pour conséquence que le développeur lui-même ne sera plus capable de déterminer les critères de décisions utilisés, la logique suivie, et

---

[1082] *Ibidem.*
[1083] OBERMEYER Ziad *et al.* « Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations », *Science*, n° 366 (6464), 25 octobre 2019, pp. 447-453.
[1084] L'étude mentionne des barrières à l'accès à la santé, même en cas de couverture par une assurance maladie : la situation géographique et l'accès au transport, le manque de temps du fait des demandes concurrentes d'emploi et de garde d'enfant, ou encore la connaissance des raisons pour lesquelles il faut se faire soigner. L'étude mentionne également une seconde piste : la discrimination résiduelle dans la relation entre le médecin et le patient. L'article mentionne en effet une expérience réalisée qui consistait à assigner de manière aléatoire des patients noirs à des médecins blancs et des médecins noirs. Il a alors été observé que les prescriptions de soins préventifs recommandés étaient significativement supérieures lorsque le médecin était noir. *Idem*, p. 451.
[1085] *Idem*, pp. 447-453.
[1086] BAROCAS Solon, HARDT Moritz, NARAYANAN Arvind, *op. cit.* p.15.
[1087] BOYD Danah, CRAWFORD Kate, *op. cit.* p. 667.
[1088] *Ibidem.*

donc le résultat[1089]. Dès lors, l'identification des biais algorithmiques se heurte aux limites du principe de transparence. Cette opacité empêche notamment de mener des recherches sur la raison pour laquelle ces biais algorithmiques apparaissent, limitant certains droits de la personne concernée. Par exemple, le logiciel COMPAS suscité n'a pas révélé l'algorithme utilisé ni les bases de données sur lesquels l'algorithme a été entraîné, complexifiant la recherche de la raison pour laquelle le logiciel prenait des décisions discriminatoires[1090]. Au-delà de la simple recherche, l'absence de transparence du logiciel a constitué une ingérence dans les droits des personnes concernées, notamment en ce qui concerne le droit de ne pas faire l'objet de discriminations et les droits procéduraux tels que le droit à la défense[1091].

543. Face à l'ensemble de ces facteurs, la protection individuelle contre une décision injuste semble limitée, ce qui remet en cause la pertinence du consentement, même explicite, à un traitement de données à caractère personnel dans le but de prendre une décision individuelle automatisée. La complexité de l'identification des biais algorithmique s'accompagne de la difficulté pour la victime d'une décision injuste de s'en rendre compte et de prouver qu'elle en est victime. Par exemple, si un algorithme de recherche d'emploi désavantage les femmes en ce qui concerne les offres d'emploi dans des postes de cadre, il sera difficile, voire impossible, pour les femmes utilisant ce service de recherche d'emploi non seulement de se porter candidates pour cet emploi, mais également de se rendre compte qu'elles font l'objet de discrimination[1092]. De même, il semble très difficile pour une communauté stigmatisée de savoir qu'ils font l'objet d'une surveillance excessive par l'utilisation de systèmes d'intelligence artificielle[1093].

544. L'ensemble des difficultés accompagnant la prise de décision automatisée et la pertinence des résultats de systèmes d'intelligence artificielle invite à repenser le régime applicable à ces prises de décision. En effet, l'article 22 du RGPD exclut le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé lorsque cette décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable de traitement et lorsque cette décision est fondée sur le consentement explicite de la personne concernée. Qu'il s'agisse du consentement contractuel ou du consentement explicite, il ne semble pas que la personne concernée soit en mesure de donner un consentement

[1089] CHAPUS Lucie, D'YVOIRE Anne-Victoire, *op. cit.*
[1090] BERTINO Elisa et al., *op. cit.*, p. 19.
[1091] *Ibidem.*
[1092] CRAWFORD Kate, *op. cit.*
[1093] CRAWFORD Kate, *op. cit.*

libre et éclairé à une prise de décision automatisée en l'état actuel des connaissances techniques et de la protection juridique des personnes concernées. Il convient dès lors de s'intéresser aux solutions juridiques proposées pour faire face aux difficultés soulevées par l'utilisation de plus en plus grande des systèmes d'intelligence artificielle.

§2 – Des solutions juridiques limitées

545. Concilier la complexité technique de l'intelligence artificielle, les risques sociétaux importants soulevés par la généralisation de cette technologie, et la possibilité pour la personne concernée d'émettre un consentement libre et éclairé lui permettant d'exercer un contrôle satisfaisant sur ses données à caractère personnel est une tâche complexe, qui semble aujourd'hui relever plus du souhait que de la réalité. La réflexion juridique, encore incomplète, propose des solutions permettant de maîtriser certains risques à travers la complémentarité en droit et éthique (A), ainsi que certaines solutions méritant d'être explorées plus minutieusement par le législateur européen (B).

A. La complémentarité de l'éthique avec le droit

546. L'éthique se définit comme une science philosophique « qui traite des principes régulateurs de l'action et de la conduite morale »[1094]. Si *a priori*, le droit et la morale se distinguent dans leur source, le premier relevant du bien commun, le second des valeurs individuelles, force est de constater que « le droit n'est pas radicalement séparé de la morale »[1095]. Traditionnellement, les valeurs morales sont implémentées dans la société à travers le droit – qu'il s'agisse d'obligations, restrictions ou encouragements – et les choix personnels[1096]. L'éthique fait son entrée dans le droit à travers plusieurs voies : l'intégration dans des politiques publiques, dans des textes de loi, mais aussi à travers des normes d'origine privée comme les standards. Dans le domaine de l'intelligence artificielle,

> « Vis-à-vis du droit, l'éthique apparaît comme un renfort par la légitimation morale qu'elle lui confère et/ou comme un expédient en attente de réponses de sa part. Cette interdisciplinarité s'avère nécessaire à la régulation de l'intelligence artificielle en apportant une vision globale de ses enjeux ».[1097]

[1094] CNRTL, « Éthique », CNRTL.fr, Lexicographie, disponible sur https://www.cnrtl.fr/definition/%C3%89thique (consulté en juin 2021).
[1095] DE LA TOUANNE Sébastien, « Les magistrats ont-ils confondu le droit et la morale dans certaines affaires politico-financières », *Dalloz Actualité*, Administratif, Pénal, 14 avril 2021.
[1096] ETZIONI Amitai, ETZIONI Oren, «Incorporating Ethics into Artificial Intelligence», *The Journal of Ethics*, 2017, Vol. 21, n° 4, p. 415.
[1097] GODEFROY Lêmy, « Éthique et droit de l'intelligence artificielle », *D.*, 2020, p. 231.

Une telle nécessité naît du fait que le droit n'est pas déconnecté de la société puisqu'elle en est un moyen d'organisation. Dans ce contexte, la finalité du droit sera orientée par les valeurs morales et éthiques de la société. Ce pilotage moral et éthique est bel et bien présent dans le RGPD, le considérant 3 affirmant expressément que « le traitement des données à caractère personnel devrait être conçu pour servir l'humanité »[1098].

547. Ce pilotage éthique est d'autant plus important lors de l'apparition de technologies disruptives, qui vont demander l'acceptation de la société, qu'il s'agisse de la *blockchain*, de l'« ubérisation » ou encore, ce qui nous intéresse dans ce paragraphe, l'intelligence artificielle[1099]. L'acceptation morale de la technologie résulte soit d'une valeur perçue spontanément faisant appel à la « magique morale »[1100] du consentement, soit d'un débat sociétal établissant les limites morales de l'utilisation d'une technologie déterminée. La mobilisation de l'éthique est dès lors principalement motivée par la polarisation des opinions autour de l'intelligence artificielle. Tantôt source d'optimisme débordant, tantôt source d'inquiétude catastrophiste[1101], l'intelligence artificielle divise[1102]. Les optimistes s'opposent à l'adoption de lois générales pour vérifier la présence ou non de biais algorithmiques dans les systèmes d'intelligence artificielle proposés aux consommateurs. Par exemple, l'institut Montaigne, think tank français, s'oppose clairement à l'adoption de lois interdisant les biais algorithmiques communes à l'ensemble des systèmes d'intelligence artificielle, peu importe le domaine d'activité, tout comme il s'oppose à l'adoption d'un système de police administrative vérifiant préalablement, à l'échelle étatique, l'absence de biais algorithmiques dans les systèmes d'intelligence artificielle insérés dans des produits ou services[1103]. À l'inverse, les catastrophistes appellent à un moratoire sur l'intelligence artificielle, à l'image de Jacques Attali, Bill Gates ou encore Stephen Hawking[1104]. Ainsi, l'acceptation d'une technologie par la

---

[1098] RGPD, 27 avril 2016, considérant 3.
[1099] GODEFROY Lêmy, 2020, *op. cit.*, p. 231.
[1100] JONES Meg Leta, EDENBERG Elizabeth, *op. cit.*, p. 358.
[1101] Le catastrophisme est présent depuis les années 1950 et est actuellement véhiculé par des personnalités influentes telles qu'Elon Musk, Stephen Hawkings ou Sam Altman. La théorie catastrophiste consiste à alerter sur le risque de perte de contrôle de l'intelligence artificielle dont les capacités cognitives dépassent l'intelligence humaine. v. BENBOUZIB Bilel, MENECEUR Yannick, ALISA SMUHA Nathalie, « Quatre nuances de régulation de l'intelligence artificielle », *Réseaux*, 2022, n°232-233, p. 31.
[1102] DE COOMAN Jérôme, *« Éthique et intelligence artificielle : l'exemple européen », Revue de la Faculté de Droit de l'Université de Liège, 2020, n° 3*, p. 81 ; MACLURE Jocelyn, SAINT-PIERRE Marie-Noëlle, *op. cit.*, p. 746.
[1103] Institut Montaigne, *Algorithms : Please Mind the Bias!*, Institutmontaigne.org, mars 2020, p. 6, disponible sur https://www.institutmontaigne.org/ressources/pdfs/publications/algorithms-please-mind-bias.pdf (consulté en juin 2021).
[1104] Assemblée Nationale, Sénat, *Pour une intelligence artificielle maîtrisée, utile et démystifiée*, Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, n° 4594 et 464, 2017, p. 97.

société passe nécessairement par la culture ou la conquête de la confiance[1105], notion sur laquelle se focalise la Commission européenne[1106]. Cette confiance doit être générée à travers une réflexion éthique, déterminant les usages acceptables et inacceptables de la technologie[1107], et qui implique une approche transversale, mêlant instruments de régulation[1108] et participation des parties prenantes[1109].

548. L'influence de l'éthique dans le droit de l'intelligence artificielle se traduit par l'interdiction des systèmes d'intelligence artificielle présentant un « risque inacceptable » pour les citoyens européens[1110]. Ainsi, l'article 5 de la proposition de règlement interdit les systèmes d'IA qui altéreraient substantiellement le libre arbitre des personnes concernées[1111], exploiteraient les faiblesses d'une personne concernée dues à l'âge ou au handicap, établiraient ou participeraient à l'élaboration d'un système de notation sociale ou utiliseraient dans des espaces accessibles au public des systèmes d'identification biométrique à distance « en temps réel » à des fins répressives. Le Règlement actuellement en négociation, d'autres propositions d'intelligences artificielles à proscrire ont été suggérées : par exemple, peuvent être considérés

---

[1105] BESSE Philippe, BESSE-PATIN Aurèle, CASTETS-RENARD Céline, « Implications juridiques et éthiques des algorithmes d'intelligence artificielle dans le domaine de la santé », *Statistique et Société*, vol. 8, n° 3, p. 23.

[1106] V. notamment Commission européenne, COM (2020) 65 final, *op. cit.*

[1107] Concernant l'Union européenne, la Commission propose l'interdiction des systèmes d'intelligence artificielle faisant peser un « risque inacceptable » sur les personnes. Commission européenne, « Excellence et confiance en matière d'intelligence artificielle », *ec.europa.eu*, disponible sur https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_fr (consulté en décembre 2021).

[1108] Tel que la proposition de règlement de la Commission européenne. Commission européenne, COM/2021/206 final, *op. cit.*

[1109] Par exemple, à travers la formation des acteurs de l'intelligence artificielle. À ce titre, l'UNESCO juge insuffisante la formation scientifique et technologique de l'ingénieur face aux « conséquences sociétales et éthiques potentielles de la technologie en développement, et des risques d'utilisation abusive », considère dès lors nécessaire une formation des ingénieurs à « l'analyse des valeurs humaines expressément vouées à améliorer le bien-être humain et la qualité de l'environnement ». Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), Commission mondiale d'éthique des connaissances scientifiques et des technologies (COMEST), *op. cit.*, pp. 11-12.

[1110] L'exclusion des risques inacceptables constitue un prérequis de l'acceptation d'une technologie par une société déterminée, plutôt que par une société universelle. Par exemple, la notation sociale constitue un des risques inacceptables identifiés par la Commission européenne. Ainsi, la notation sociale constitue « une menace évidente pour les citoyens de l'UE » tandis qu'elle semble acceptable en Chine et façonne le quotidien des citoyens chinois. Commission européenne, « Excellence et confiance en matière d'intelligence artificielle », *ec.europa.eu*, disponible sur https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_fr (consulté en décembre 2021) ; Le Monde, « En Chine, le « crédit social » des citoyens fait passer les devoirs avant les droits », *LeMonde.fr*, 16 janvier 2020, disponible sur https://www.lemonde.fr/idees/article/2020/01/16/le-credit-social-les-devoirs-avant-les-droits_6026047_3232.html (consulté en juillet 2022).

[1111] Plus précisément, l'article 5 interdit « la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui a recours à des techniques subliminales au-dessous du seuil de conscience d'une personne pour altérer substantiellement son comportement d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou un tiers ». Commission européenne, COM/2021/206 final, *op. cit.*, article 5 (1) (a).

comme inacceptables « les technologies qui contribuent à nuire à l'environnement »[1112], l'utilisation des systèmes d'IA pour les décisions de justice[1113], les technologies d'intelligence artificielle faisant appel à la reconnaissance des émotions[1114], les systèmes d'IA altérant la nature de mutualisation des risques des polices d'assurance[1115] ou encore tout système d'IA produisant des pratiques discriminatoires[1116]. L'interdiction de ces systèmes d'intelligence artificielle traduit les usages inacceptables définis par la Commission européenne, limitant la capacité de développer et de commercialiser des systèmes d'intelligence artificielle à ce que la société européenne considère comme acceptable au moment de l'élaboration du règlement. Il est cependant étonnant que la Commission européenne n'ait pas adopté une liste évolutive de systèmes d'IA considérés comme inacceptables, au même titre que la classification des systèmes d'IA comme systèmes à haut risque. Pourtant, le groupe d'experts indépendants avait bien mis en exergue l'importance de décider au sein de la communauté des usages inacceptables de l'IA, à travers un processus ouvert, transparent et responsable[1117], ce qui sous-entendait une approche évolutive.

549. L'identification des risques qualifiés d'inacceptables par le législateur est indispensable à la prise en compte des risques de nature collective qui ne pourraient pas être adressés à travers la simple émission du consentement. La mobilisation de l'éthique ne se limite cependant pas à la définition de l'inacceptable, dans la mesure où les risques collectifs peuvent exister sans relever pour autant de l'inacceptable. Par exemple, la proposition de Règlement de la Commission européenne présente les systèmes d'intelligence artificielle ayant une « incidence préjudiciable significative sur la santé, la sécurité et les droits fondamentaux des citoyens dans l'Union » comme systèmes d'intelligence artificielle à haut risque, mais non interdits à condition que ces systèmes « ne présentent pas de risques inacceptables pour d'importants intérêts publics de l'Union tels qu'ils sont reconnus et protégés par le droit de l'Union »[1118]. Dans ce cadre, l'approche législative s'inspire des organismes de standardisation, à l'image du

---

[1112] Parlement européen, *Rapport sur l'intelligence artificielle à l'ère du numérique*, 5 avril 2022, 2020/2266 (INI) § 215.
[1113] CNCDH, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*, 7 avril 2022, pp. 13-14.
[1114] *Idem*, p. 15.
[1115] POWERS Thomas M., GANASCIA Jean-Gabriel, «The Ethics of the Ethics of AI», *in* DUBBER Markus D., PASQUALE Frak, DAS Sunit, *The Oxford Handbook of Ethics of AI*, Oxford University Press, 2020, p. 38.
[1116] Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, Commission européenne, 8 avril 2019, p. 35.
[1117] Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle, *Policy and Investment Recommendations for Trustworthy AI*, Commission européenne, 26 juin 2019, p. 38.
[1118] Commission européenne, COM/2021/206 final, *op. cit.*, considérant 27.

Sénat et de l'Assemblée nationale citant comme exemple l'initiative IEEE afin de « favoriser des algorithmes et des robots sûrs, transparents et justes »[1119].

550. En effet, au-delà de l'action purement législative, les organismes de standardisation s'intéressent de plus en plus à la question de l'éthique dans le développement de systèmes d'intelligence artificielle. L'IEEE appelle à s'intéresser au caractère bénéfique de l'action de l'IA sur les humains et à l'environnement des systèmes d'intelligence artificielle, au-delà d'une simple approche technique et fonctionnelle[1120]. L'*International Electrotechnical Commission* (IEC) a créé le groupe de réflexion SEG 10 *Ethics in Autonomous and Artificial Intelligence Applications*[1121]. L'ISO travaille actuellement, en partenariat avec l'IEC, sur un projet de standard dénommé « *Overview of ethical and societal concerns* », actuellement en phase préparatoire[1122]. Au niveau européen, l'ETSI consacre tout un paragraphe à l'éthique au sein de son rapport sur la sécurisation de l'intelligence artificielle[1123] . Les principes éthiques développés par ces organismes de standardisation se résument en quatre principes : explicabilité, contrôle des données, responsabilité et transparence.

551. Les deux premiers principes garantissent à la société un contrôle des technologies utilisées, puisqu'ils assurent que les créateurs et développeurs du système sont capables de maîtriser les décisions prises à l'aide de l'IA. En effet, un consentement à une prise de décision automatisée dont les résultats ne pourraient être expliqués ne relèverait pas du consentement éclairé tant il reviendrait à dire que la personne concernée a accepté « de manière aveugle »[1124] le résultat de la décision. En revanche, face à une prise de décision explicable, la personne concernée peut choisir si elle souhaite être l'objet d'une décision précise, dont elle connaît les critères de décision[1125]. Dans ce cadre, l'explicabilité doit relever deux défis : celui de

---

[1119] Assemblée Nationale, Sénat, *Pour une intelligence artificielle maîtrisée, utile et démystifiée,* Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, n° 4594 et 464, 2017, p. 206.

[1120] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Proritizing Human Well-being with Autonomous and Intelligent Systems*, IEEE, 1e edition, 2019, disponible sur https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html (consulté en juin 2021).

[1121] International Electrotechnical Commission (IEC), «SEG 10. Ethics in Autonomous and Artificial Intelligence Applications », *IEC.ch*, disponible sur https://www.iec.ch/dyn/www/f?p=103:187:616184075401079::::FSP_ORG_ID,FSP_LANG_ID:22827,34 (consulté en juin 2021).

[1122] Il s'agit du standard ISO/IEC AWI TR 24 368 « Information technology – Artificial Intelligence – Overview of ethical and societal concerns ». v. ISO, « Standards by ISO/IEC JTC 1/SC 42. Artificial Intelligence. », *ISO.org*, disponible sur https://www.iso.org/committee/6794475/x/catalogue/ (consulté en juin 2021).

[1123] ETSI, *Securing Artificial Intelligence (SAI); Problem Statement*, ETSI, Group Report, ETSI GR SAI 004, décembre 2020, version 1.1.1, ETSI GR SAI 004, pp. 16–19.

[1124] DORAN Derek, SCHULZ Sarah, BESOLD Tarek R., «What Does Explainable AI Really Mean? A New Conceptualization of Perspectives », 2 octobre 2017, arXiv : 1810.00794v1.

[1125] SHIN Donghee, «The Effects of Explainability and Causability on Perception, Trust and Acceptance: Implications for Explainable AI», *International Journal of Human-Computer Studies*, 2021, vol. 146, 102,551.

déterminer les critères de décision et celui de rendre compréhensible l'explication à la personne concernée[1126]. De la même manière, le principe de contrôle des données à caractère personnel (*Data Agency*) tel que développé par l'IEEE[1127] permet de protéger ces données au-delà de la simple protection contre les utilisations non autorisées. Ce principe permet en effet une protection plus avancée des droits humains des personnes concernées en considérant que ces droits « reposent sur la capacité des individus à faire des choix, en dehors de l'influence potentielle d'algorithmes biaisés »[1128] et de l'utilisation de systèmes d'IA par des acteurs malveillants[1129].

552. Ces principes permettent de protéger la personne concernée de manière plus avancée que la simple question de savoir s'il y a des humains dans la boucle[1130]. En effet, la supervision humaine constitue la protection privilégiée actuelle du droit européen à travers le droit de ne pas faire l'objet d'une prise de décision automatisée. Or, cette approche présente des limites. Par exemple, le rapport du *AI Now Institute* estime que cette démarche est insuffisante et qu'il est indispensable de se demander également « quels humains sont dans la boucle »[1131]. De plus, comme il a été démontré précédemment, l'identification de biais peut présenter des difficultés pour l'humain supervisant la prise de décision automatisée, tant ces biais sont enracinés, parfois de manière invisible, dans la société[1132]. L'approche éthique permet de dépasser le simple contrôle de ses données à caractère personnel tel qu'établi par le RGPD pour prendre en compte le contexte dans lequel se trouve la personne concernée : la liberté de la personne concernée n'est plus présumée et est protégée contre les formes d'influences jugées inacceptables et contre la manipulation.

553. Les principes de responsabilité et de transparence permettent de s'assurer que malgré le caractère disruptif de la technologie, le régime de responsabilité régissant actuellement la société s'applique aux systèmes d'intelligence artificielle. Le caractère autonome et opaque des systèmes au « comportement intelligent »[1133] ne saurait en effet évincer le système juridique de

---

[1126] HIND Michael, «Explaining Explainable AI», *XRDS: Crossroads*, 2019, Vol. 25, n° 3, p. 17.
[1127] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Proritizing Human Well-being with Autonomous and Intelligent Systems*, IEEE, 1e edition, 2019, p. 23, disponible sur https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html (consulté en juin 2021).
[1128] *Ibidem.*
[1129] *Ibidem.*
[1130] *Ibidem.*
[1131] WEST Sarah Myers, WHITTAKER Meredith, CRAWFORD Kate, *op. cit.*, p. 8.
[1132] COLLET Clementine, DILLON Sarah, *op. cit.*, p. 4.
[1133] Conseil de l'Europe, *Responsabilité et IA*, Strasbourg, Conseil de l'Europe, septembre 2019, rapporté par Karen Yeung, p. 16.

responsabilité qui garantit que les individus et organisations répondent effectivement des effets négatifs de leurs actions et actes sur autrui[1134]. Le rôle central du régime de responsabilité civile au sein de l'Union européenne a été mis en exergue par le Parlement européen, qui lui attribue une double fonction :

> « d'une part, [la notion de responsabilité] garantit qu'une personne ayant subi un préjudice ou un dommage est en droit de demander et de recevoir une indemnisation de la partie dont la responsabilité pour ce préjudice ou ce dommage est avérée et […] d'autre part, elle incite économiquement les personnes physiques et morales à éviter de causer un préjudice ou un dommage en premier lieu ou à évaluer le risque de devoir payer une indemnisation »[1135].

Le respect du principe de responsabilité est essentiel, afin de garantir que la faute intentionnelle ou non du concepteur du système d'intelligence artificielle causant un préjudice puisse donner lieu à une indemnisation de la personne concernée par le dommage. En effet, si l'intelligence était reconnue juridiquement comme autonome, par exemple par l'octroi d'une personnalité juridique, la voie de recours par laquelle la personne concernée pourrait contester une action contraire à son consentement ou la validité de son consentement serait complexifiée par l'existence d'un système reconnu comme autonome et par conséquent de la possible exemption de responsabilité de son concepteur.

554. Ainsi, envisager l'intelligence artificielle au prisme de l'éthique permet de penser le consentement au-delà du consentement RGPD, en prenant en compte les risques inhérents à la prise de décision automatisée. Or, si l'éthique contient des principes avantageux en matière de protection, ceux-ci ne suffisent ni à créer une protection suffisante ni à créer une confiance satisfaisante au sein de la société. En effet, « la confiance des usagers sera nettement plus franche et massive si elle repose sur une protection juridique, plutôt que sur des bonnes intentions éthiques (*ethical washing*), aussi louables soient-elles »[1136].

B. Des solutions juridiques à explorer

555. La complexité de l'intelligence artificielle empêche *a priori* la personne concernée de consentir de manière éclairée à un traitement de données à caractère personnel impliquant un système d'intelligence artificielle. Cependant, un consentement libre et éclairé ne signifie pas

---

[1134] *Idem,* p. 18.
[1135] Parlement européen, *Résolution du Parlement européen contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle,* Bruxelles, 20 octobre 2020.
[1136] BESSE Philippe, BESSE-PATIN Aurèle, CASTETS-RENARD Céline, « Implications juridiques et éthiques des algorithmes d'intelligence artificielle dans le domaine de la santé », *Statistiques et Société,* vol. 8, n° 3, décembre 2020, p. 24.

une compréhension du système même traitant les données de la personne concernée, ni même la cause des risques de son utilisation.

556. Ainsi, la maîtrise des risques des systèmes d'intelligence artificielle à travers une obligation de *due diligence* permettrait d'une part une réflexion collective sur les risques acceptables pour la personne concernée et leur maîtrise par le responsable de l'algorithme (1). D'autre part, une obligation renforcée de transparence permettrait, à travers la conciliation des intérêts du responsable de traitement, du responsable de l'algorithme et de la personne concernée, l'émission par la personne concernée d'un consentement plus éclairé (2).

1. Une obligation de due diligence propre aux systèmes d'intelligence artificielle

557. Pour garantir la protection de la personne concernée, une première proposition est de recourir aux notions de vigilance et de loyauté du responsable de l'algorithme. La 40e conférence internationale des commissaires à la protection des données et de la vie privée avait adopté en 2018 une déclaration en ce sens, invitant les responsables des algorithmes à s'assurer que « l'utilisation des systèmes d'intelligence artificielle reste fidèle aux objectifs d'origine », à tenir compte « non seulement de l'impact de l'utilisation artificielle sur l'individu, mais aussi de son impact collectif sur les groupes et la société dans son ensemble » et enfin à s'assurer de développer de tels systèmes « de façon à faciliter l'épanouissement de l'individu, sans l'entraver ni le mettre en danger »[1137]. Ainsi, l'obligation de *due diligence* permettrait de prendre en compte les risques collectifs posés par la généralisation des systèmes d'intelligence artificielle. Dans ce cadre, la validité du consentement pourrait être envisagée, l'obligation de *due diligence* protégeant la personne concernée des risques collectifs, le consentement la protégeant des risques individuels.

558. La proposition de règlement de la Commission adopte cette approche, mais seulement en partie. En effet, la proposition de règlement sur l'intelligence artificielle crée un principe de bonne gouvernance des données qui s'appliquera uniquement aux « systèmes d'IA à haut risque »[1138]. Pour déterminer les systèmes d'IA à haut risque, la Commission européenne ne propose pas de définition, mais une liste de systèmes considérés à haut risque annexée à la proposition de règlement[1139]. Sont ainsi considérés comme systèmes d'IA à haut risque les

[1137] Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), *Déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle*, 40e conférence internationale des commissaires à la protection des données et de la vie privée, Bruxelles, 23 octobre 2018.
[1138] Commission européenne, COM/2021/206 final, *op. cit.*, article 10.
[1139] Commission européenne, COM/2021/206 final, *op. cit.*, Annexe III.

systèmes d'IA d'identification biométrique à distance, les systèmes d'IA relatifs à la gestion et l'exploitation d'infrastructures critiques, les systèmes d'IA relatifs à l'éducation et à la formation professionnels, les systèmes d'IA relatifs à l'emploi, les systèmes d'IA relatifs à l'accès et au droit aux services privés essentiels, aux services publics et aux prestations sociales, les systèmes d'IA utilisés par les autorités répressives, les systèmes d'IA utilisés dans le cadre de la gestion de la migration, de l'asile et des contrôles aux frontières et enfin les systèmes d'IA relatifs à l'administration de la justice et aux processus démocratiques[1140]. Cette approche a été critiquée par le Comité européen de protection des données et le Commissaire européen à la protection des données comme un choix pouvant paraître manichéen et peu adapté à l'approche fondée sur les risques puisque des situations à haut risque pourront échapper aux dispositions relatives aux systèmes d'IA à haut risque, comme les systèmes d'IA relatifs aux primes d'assurance, ou encore à l'accès aux traitements médicaux[1141].

559. Pourtant, l'utilisation d'une liste annexée pour déterminer quels systèmes d'intelligence artificielle sont à haut risque peut s'avérer pertinente puisqu'elle permet, comme discuté ci-dessus, de déterminer les usages admis et non admis par la société. Il est en effet tout à fait audible de la part de la Commission européenne de moduler les obligations du fournisseur du système d'intelligence artificielle en fonction du risque que ce système crée vis-à-vis de la société européenne afin de concilier protection et compétitivité des produits européens. Cependant, la proposition de règlement de la Commission ne propose pas d'obligation de prudence générale, qui permettrait de prendre en compte de façon globale les risques que la généralisation de l'intelligence artificielle crée au sein de la société. Par exemple, l'article 10 de la proposition de règlement qui dispose que le fournisseur du système d'intelligence artificielle doit procéder à un examen des jeux de données d'entraînement, de validation et de test afin de repérer d'éventuels biais ne s'applique qu'aux systèmes d'intelligence artificielle à haut risque. Or, cette approche devrait s'appliquer à tout système d'intelligence artificielle puisque, comme il a été démontré, les biais sont difficiles à identifier pour la personne concernée. Par exemple, la Défenseure des droits propose à la Commission d'assigner « des « obligations d'égalité » contraignantes et opposables à tous les concepteurs et utilisateurs d'IA »[1142].

[1140] *Idem,* Annexe III.
[1141] EDPB, EPDS, *op. cit.,* §19.
[1142] Défenseur des droits, « Intelligence artificielle : la Défenseure des droits appelle à replacer le principe de non-discrimination au cœur du projet de règlement de la Commission européenne », *Communiqué de presse*, Paris, 21 juin 2022.

560. Si le cadre proposé par la Commission européenne rejoint la logique d'*accountability* qui parcourt le RGPD, la proposition de règlement sur l'IA présente des lacunes en matière de gestion des risques collectifs induits par la généralisation de la technologie d'intelligence artificielle. Ces lacunes se reflètent sur la capacité d'émettre un consentement valide de la personne concernée par des décisions prises par ou à l'aide d'une technologie d'intelligence artificielle. En effet, il est déraisonnable de faire peser sur le consentement de la personne concernée la gestion des risques collectifs et sociétaux, notamment le risque de généralisation des discriminations. Ainsi, le législateur européen gagnerait à généraliser les obligations permettant d'atténuer les risques collectifs et sociétaux à travers une obligation de *due diligence* générale qui comporterait une obligation de vérifier que les jeux de données ne comportent pas de biais et une obligation de former aux questions des biais algorithmiques les personnes chargées de la supervision humaine[1143] telle qu'établie par le RGPD.

561. Au-delà d'une obligation de *due diligence* généralisée permettant à la personne concernée de ne pas prendre la responsabilité des risques collectifs et sociétaux causés par l'intelligence artificielle, la validité du consentement à une prise de décision automatisée nécessite une obligation de transparence accrue vis-à-vis des systèmes d'intelligence artificielle utilisés.

2. Une obligation de transparence renforcée

562. Une seconde piste propose une obligation de transparence accrue. À la suite de l'évolution des algorithmes et l'utilisation de plus en plus généralisée des algorithmes de profilage, le RGPD a inclus dans son article 13 l'obligation d'informer la personne concernée de « l'existence d'une prise de décision automatisée, y compris un profilage »[1144] au titre de l'obligation de transparence. La seule obligation d'information sur l'existence d'une prise de décision automatisée – si elle est nécessaire à l'exercice de ses droits par la personne concernée – n'est pourtant pas suffisante pour que la personne concernée s'informe correctement sur le traitement de données à caractère personnel concerné et les risques qui y sont attachés.

[1143] L'obligation de former les personnes chargées de la supervision humaine a été mise en exergue par la CNCDH, qui affirme qu'assurer « une intervention humaine effective suppose d'informer l'intervenant sur les caractéristiques de l'algorithme utilisé ». Cette formation permet de la part de l'intervenant « une prise de distance » nécessaire à la réduction du biais cognitif d'automatisation, c'est-à-dire le biais d'accorder une confiance excessive dans les décisions de l'algorithme. En effet, la supervision humaine consiste à réexaminer la décision prise par l'algorithme et ne saurait, dès lors, pour être effective, souffrir du biais d'automatisation. CNCDH, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*, 7 avril 2022, p 25.
[1144] RGPD, 27 avril 2016, Article 13 (2) (f).

563. L'article 13 du RGPD est ainsi complété par le considérant 71 qui octroie à la personne concernée le droit de se voir fournir « une information spécifique » ainsi que « le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise […] et de contester la décision ». Le RGPD semble donc créer un droit à l'explication de la décision prise grâce à un système automatisé, droit qui a pu être évalué par certains acteurs comme limité lorsqu'il s'agit de systèmes de *deep learning*[1145]. Lors de l'utilisation de systèmes d'intelligence complexes, les relations, le poids accordé aux paramètres et les seuils de décision seront inconnus par le créateur du système, qui n'aura accès qu'à la connaissance de corrélations[1146]. La raison de cette opacité réside dans le cœur du *machine learning* : le système apprend de sa propre expérience, et non de celle de l'humain. Ces lacunes de connaissance, aussi appelées « boîtes noires », sont problématiques non seulement au niveau de la protection des données à caractère personnel et plus largement des droits fondamentaux, mais également au niveau du marché, réduisant la confiance accordée à l'intelligence artificielle dans son ensemble[1147]. Cette confiance est essentielle puisque les attentes humaines vont parfois se confronter à une différence de nature entre le raisonnement humain et les résultats offerts par la machine uniquement tournés vers l'optimisation de la performance[1148]. Ainsi, les destinataires de l'information ne seraient pas constitués uniquement des personnes concernées, mais également des développeurs de systèmes incluant la technologie d'intelligence artificielle, des décideurs utilisant ces systèmes comme aide à la prise de décision et les régulateurs voulant s'assurer que ces systèmes n'exercent pas une influence néfaste sur la société[1149]. Ce double enjeu a conduit au développement d'une recherche scientifique en matière d'intelligence artificielle explicable (*Explainable AI*), la communauté scientifique développant des méthodologies ayant comme objectif d'encourager la création de systèmes d'intelligence artificielle explicables sans pour autant en sacrifier les performances[1150]. En effet, plus que d'obtenir une explication scientifique exacte quant au

---

[1145] O'HARA Kieron, «Explainable AI and the Philosophy and Practice of an Explanation», *Computer Law & Security Review*, 2020, n° 39, p. 4.
[1146] *Ibidem.*
[1147] HOLZINGER Andreas *et al.*, «Current Advances, Trends and Challenges of Machine Learning and Knowledge Extraction: From Machine Learning to Explainable AI», *in* HOLZINGER Andreas *and al.* (dir.), *Machine Learning and Knowledge Extraction*. *Lecture Notes in Computer Science*, Springer, 2018, pp. 1–8.
[1148] MICHAEL Nathan, « Trustworthy AI: Why Does It Matter? », *National Defense*, octobre 2019, vol. 104, n° 791, p. 26.
[1149] HAMON Ronan *et al.*, «Impossible Explanations? Beyond Explainable AI in the GDPR from a COVID-19 use case scenario», *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT'21)*, Nex York, Association for Computing Machinery, p. 550
[1149] HIND Michael, *op. cit.*, p. 18.
[1150] HAMON Ronan *et al.*, *op. cit.*, p. 550.

fonctionnement du système d'intelligence artificielle fondé sur une technologie de *deep learning*, l'explicabilité de l'intelligence artificielle peut se limiter, à l'image des audits de société, à vérifier que le système a suivi un protocole adéquat[1151].

564. Les discussions en matière juridique sont cependant en retard sur les progrès en matière d'explication scientifique. Ainsi, les mathématiciens documentent les systèmes d'intelligence artificielle à travers des éléments mathématiques permettant au reste de la communauté de vérifier le système et la validité de l'explication[1152]. Dans la communauté juridique, le débat s'est beaucoup focalisé sur la question de savoir si le RGPD offrait ou non un droit à l'explication des décisions prises de manière automatisée aux personnes concernées[1153]. Cependant, il n'existe pas à ce jour de cadre juridique encadrant une obligation de transparence propre à l'intelligence artificielle. Pourtant, une telle obligation serait nécessaire non seulement dans le domaine du droit à la protection des données à caractère personnel, mais également dans les domaines du droit des contrats ou de la responsabilité civile[1154].

565. Le besoin de transparence est pourtant bien présent sur le marché, et constitue un sujet sur lequel les acteurs majeurs souhaitent se positionner, à travers différents standards : les principes de confiance et de transparence d'IBM, les principes de Google concernant l'intelligence artificielle ou encore les standards développés par l'IEEE[1155]. L'obligation de transparence comporterait principalement les éléments permettant à la personne concernée de faire valoir ses droits à un consentement éclairé, à la compréhension d'une décision prise à son encontre et à la possibilité de s'opposer à une décision qui résulterait, à ses yeux, d'une erreur. Ainsi, l'obligation de transparence envers les personnes concernées pourrait contenir par exemple une information sur les critères utilisés et leur poids dans la prise de décision[1156]. La proposition de règlement de la Commission européenne sur l'intelligence artificielle propose une obligation de transparence relative à certains systèmes d'intelligence artificielle. D'abord, la personne concernée doit être informée du fait qu'elle interagit avec un système d'intelligence

---

[1151] BRYSON Joanna J., «The Artificial Intelligence of the Ethics of AI' *in* DUBBER Markus D., PASQUALE Frak, DAS Sunit, *The Oxford Handbook of Ethics of AI*, Oxford University Press, 2020, p. 8.
[1152] HIND Michael, *op. cit.*, p. 16.
[1153] HACKER Philipp *et al.*, «Explainable AI under contract and tort law: legal incentives and technical challenges», *Artificial Intelligence and Law*, 2020, p. 415.
[1154] *Ibidem.*
[1155] Pour une liste plus exhaustive de ces standards, v. ROSSI Franscesca, « Building Trust in Artificial Intelligence », *Journal of International Affairs*, vol. 72, n° 1, pp. 127-134.
[1156] DOSHI-VELEZ *et al.*, « Accountability of AI Under the Law – The Role of Explanation», *Berkman Klein Center Working Group on Explanation and the Law*, 2017, disponible sur http://nrs.harvard.edu/urn-3:HUL.InstRepos:34372584 (consulté en décembre 2021).

artificielle[1157]. Cette information est renforcée en matière de systèmes de reconnaissance des émotions et de systèmes de catégorisation biométriques, systèmes évalués comme particulièrement risqués et qui impliquent pour le responsable de traitement d'informer la personne concernée « du fonctionnement du système »[1158]. L'information de la personne concernée est également renforcée pour les systèmes d'intelligence artificielle impliquant une génération ou manipulation d'images, contenus audio et vidéo « pouvant être perçus à tort comme authentiques ou véridiques » : le responsable de traitement devra, afin d'éviter la propagation de *deep fakes*, préciser « que les contenus ont été générés ou manipulés artificiellement »[1159]. Ensuite, le règlement crée à la charge du concepteur du système d'intelligence artificielle une obligation de transparence envers l'utilisateur, défini comme « toute personne physique ou morale, autorité publique, agence ou autre organisme utilisant sous sa propre autorité un système d'IA, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnelle »[1160].

566. La proposition de règlement ne clarifie donc pas l'interrogation suscitée par le règlement sur l'existence ou non d'un droit à l'explication des décisions adoptées par ou grâce à un système de décision automatisée. L'obligation de transparence envers les utilisateurs, si elle est essentielle au contrôle de ces systèmes, n'est pas suffisante pour générer la confiance des personnes concernées. Une obligation de transparence délivrant à la personne concernée les attributs utilisés par le système et la façon dont ils sont utilisés permet en effet à la personne concernée de « suivre la logique [utilisée par le système] et d'obtenir une information significative à propos de son sens et des conséquences envisagées de l'utilisation d'un tel système »[1161]. Cependant, une telle obligation de transparence se heurte à un certain nombre de difficultés techniques, économiques et juridiques.

567. Premièrement, comme sus-évoqués, les systèmes d'intelligence artificielle utilisant le *machine learning* se construisent au travers d'un apprentissage autonome à partir de jeux de données. La détermination des attributs et du poids accordé à ces attributs ne relève donc pas dans certains cas de la décision humaine, mais du processus logique du système. Cette caractéristique est d'autant plus prégnante lors de l'utilisation de systèmes de *deep learning*. En effet, « l'utilisation de réseaux de neurones profonds » ont pour conséquence que le

---

[1157] Commission européenne, COM/2021/206 final, *op. cit.* Article 52 (1).
[1158] *Ibidem.*
[1159] *Idem*, Article 52(3).
[1160] *Idem*, Article 3(4), Article 13.
[1161] THELISSON Eva, «Towards Trust, Transparency, and Liability in AI/AS Systems», *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17)*, p. 5215

développeur lui-même ne sera plus capable de déterminer les critères de décisions utilisés, la logique suivie, et donc le résultat[1162]. Les chercheurs ont tout de même développé plusieurs méthodologies permettant aux développeurs d'expliquer les résultats du système d'intelligence artificielle[1163]. Ainsi, l'obligation de transparence nécessite le déploiement de moyens additionnels au développement du système, dont le coût en termes de compétences, temps et moyens économiques peuvent freiner voire dissuader l'apparition de systèmes innovants.

568. Deuxièmement, l'obligation de transparence se heurte à la valeur attribuée par les développeurs de systèmes d'intelligence artificielle à l'information à délivrer. Les développeurs de systèmes d'intelligence artificielle peuvent craindre la divulgation des attributs utilisés dans la prise de décision et de leur poids dans la mesure où cette divulgation peut d'une part, créer des vulnérabilités dans leur système, et d'autre part, révéler une information essentielle au maintien d'un avantage compétitif sur le marché.

La crainte de voir l'obligation de transparence permettre l'exploitation de vulnérabilités du système provient de l'expérience sur le marché de l'innovation. Par exemple, la compréhension des critères de décision du moteur de recherche Google a été à l'origine de la recherche d'une optimisation acharnée de la notation des sites internet sur le moteur de recherche (connue sous le nom de *Search Engine Optimization* ou SEO)[1164]. La divulgation trop vaste d'informations concernant le fonctionnement des systèmes d'intelligence artificielle sur le marché pourrait « provoquer plus de mal que de bien » dans la mesure où elle pourrait entraîner une « gamification » de ces systèmes par des opérateurs externes aux objectifs « plus questionnables et certainement plus opaques » que les développeurs du système[1165]. Par exemple, la divulgation d'éléments de fonctionnement d'un algorithme ayant comme objectif la détection de fraudes fiscales pourrait engendrer des comportements d'ajustement des fraudeurs à l'algorithme leur permettant d'échapper à la détection[1166].

L'obligation de transparence peut également se confronter à d'autres principes s'appliquant sur le marché intérieur, principalement le secret des affaires. La directive 2016/943

[1162] CHAPUS Lucie, D'YVOIRE Anne-Victoire, *op. cit.*
[1163] DEEKS Ashley, «The Judicial Demand for Explainable Artificial Intelligence», *Columbia Law Review*, novembre 2019, vol. 119, n° 7, p. 1835.
[1164] SPINA ALÌ Gabriele, YU Ronald, «Artificial Intelligence between Transparency and Secrecy: From the EC Whitepaper to the AIA and Beyond», *European Journal of Law and Technology*, 2021, vol. 12, n° 3, p. 7.
[1165] NAUGHTON John, « Good Luck in Making Google Reveal its Algorithm », *The Guardian*, 13 novembre 2016, disponible sur https://www.theguardian.com/commentisfree/2016/nov/13/good-luck-in-making-google-reveal-its-algorithm (consulté en décembre 2021).
[1166] KROLL Joshua A. *et al.* «Accountable Algorithms», *University of Pennsylvania Law Review*, 2018, Vol. 165, p. 658.

relative à la protection des secrets d'affaires protège les entreprises contre l'obtention, l'utilisation et la divulgation illicites de ceux-ci[1167]. Les secrets d'affaires sont définis comme des informations secrètes (au sens d'informations qui ne sont « pas généralement connues des personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles »), qui font l'objet de dispositions destinées à les garder secrètes et qui « ont une valeur commerciale parce qu'elles sont secrètes »[1168]. La proposition de Règlement sur l'intelligence artificielle de la Commission porte une attention particulière à l'articulation de ce dernier avec la directive sur la protection des secrets d'affaires[1169]. En effet, les algorithmes constituent souvent « la clé de voûte des modèles économiques des entreprises concernées »[1170], comme la qualité des résultats du moteur de recherche Google ou la personnalisation du contenu proposé par Facebook.

569. Enfin, la complexité technique des algorithmes pourrait être un frein à la validité du consentement, en particulier à l'obtention d'un consentement éclairé de la personne concernée. Dans ses lignes directrices, le G29 a mis en garde les responsables de traitement sur l'inadéquation probable du consentement à la prise de décision automatisée et au profilage :

> « Le profilage peut être opaque. Il s'appuie souvent sur des données dérivées ou déduites d'autres données, plutôt que sur des données fournies directement par la personne concernée.
>
> Les responsables du traitement qui cherchent à se fonder sur le consentement pour procéder à un profilage devront démontrer que les personnes concernées comprennent exactement ce à quoi elles consentent, et se rappeler que le consentement n'est pas toujours une base appropriée pour le traitement. Dans tous les cas, les personnes concernées devraient disposer de suffisamment d'informations pertinentes sur l'utilisation envisagée et les conséquences du traitement pour garantir que leur consentement représente un choix éclairé »[1171].

570. L'anticipation du risque est en effet rendue difficile par la complexité du fonctionnement des systèmes d'intelligence artificielle, mais également par la détermination des contours de l'atteinte à la protection des données à caractère personnel des personnes concernées. En effet, le développement de l'intelligence artificielle a généralisé la création de « données bâtardes » (*bastard data*) ou de données déduites, générées par la mise en relation et le croisement des

---

[1167] Directive (UE) 2016/943 du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, 8 juin 2016.
[1168] *Idem,* article 2 (1).
[1169] Commission européenne, COM/2021/206 final, *op. cit.*, §3,5.
[1170] MARTY Frédéric, «La protection des algorithmes par le secret des affaires. Entre risques de faux négatifs et risques de faux positifs », *Revue internationale de droit économique*, 2019, n° 2, p. 211.
[1171] Groupe de travail « Article 29 », WP251rev.01, *op. cit.*, p. 19.

données initialement collectées[1172]. Ainsi, fonder le consentement au traitement automatisé de données à caractère personnel par un système d'intelligence artificielle pourrait entraîner l'effet pervers d'une « illusion de la transparence » (*transparency fallacy*), les personnes concernées ayant l'impression de consentir au traitement alors même qu'elles ne sont pas armées, en termes de compréhension et de temps de réflexion, à l'exercice d'un consentement valide[1173]. L'adéquation du consentement aux traitements de données à caractère personnel par l'intelligence artificielle a d'ailleurs été discutée au sein du Conseil de l'Europe qui dénonce « la faiblesse, en termes d'autodétermination, du consentement de la personne concernée »[1174].

571. Conclusion de Section. – De nombreuses pistes sont étudiées pour diminuer le risque d'apparition de biais algorithmiques, à travers un contrôle interne effectué par le responsable de traitement qui pourra par la suite être évalué par le juge (obligation de vigilance) ou un contrôle externe par la divulgation accrue d'informations, et notamment des critères de décision utilisés par l'algorithme dans sa prise de décision. La première piste a le mérite de proposer une approche facile à mettre en place, à travers un devoir particulier de vigilance, mais se heurte à la définition difficile du risque. L'apparition de systèmes d'intelligence artificielle particulièrement risqués qui ne seraient pas soumis aux dispositions du Règlement proposé en matière de systèmes d'intelligence artificielle à haut risque peut être raisonnablement crainte, d'autant plus que le temps du droit est substantiellement plus long que le temps de l'innovation. La seconde piste, qui s'intéresse quant à elle à la qualité du consentement en matière d'intelligence artificielle, présente des limites importantes en matière de conciliation avec les intérêts commerciaux et sécuritaires ainsi qu'en matière de capacité pour l'individu de comprendre le contenu et les conséquences des informations délivrées. Dès lors, le consentement paraît être une solution juridique difficile à concilier avec la généralisation des systèmes d'intelligence artificielle puisque d'une part le législateur doit permettre à la personne concernée de consentir dans un environnement où les risques sociétaux posés par la technologie, parmi lesquels les biais algorithmiques, font l'objet d'une protection suffisante, et d'autre part, le consentement de la personne concernée doit être éclairé à travers une obligation de transparence satisfaisante vis-à-vis du niveau de compréhension de la personne concernée.

[1172] EDWARDS Lilia, VEALE Michael, «Slave to the Algorithm? Why a "Right to an Explanation" is Probably Not the Remedy You Are Looking For», *Duke Law and Technology Review*, 2017, Vol. 16, n° 1, p. 33.
[1173] *Idem*, p. 67.
[1174] Conseil de l'Europe, « Intelligence Artificielle et Protection des données », *Lignes directrices sur l'intelligence artificielle et la protection des données*, adoptées par le Comité de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108), 25 janvier 2019, p. 24.

Conclusion du Chapitre 1

572. Le législateur européen a identifié que certains traitements de données à caractère personnel présentaient des enjeux particuliers en matière de consentement de la personne concernée. Ainsi, le consentement aux transferts hors Union européenne et le consentement à la prise de décision automatisée doivent tous deux être explicites. Cependant, plus qu'une formalisation et une temporisation du consentement à travers le consentement explicite, il a été démontré que la pertinence même du consentement vis-à-vis de ces traitements de données à caractère personnel mérite d'être discutée en raison de leur complexité.

573. Le consentement aux transferts de données à caractère personnel présente à la fois des lacunes en matière de compréhension des risques vis-à-vis de la personne concernée, créant le doute sur la capacité de celle-ci d'émettre un consentement éclairé, et des difficultés vis-à-vis du responsable de traitement de garantir que le consentement est libre, notamment le fait que la personne concernée puisse retirer son consentement à tout moment. Cette complexité ne permet pas de garantir que la personne concernée ait émis un consentement valide au sens même des critères établis par l'article 4(11) du RGPD.

574. Le consentement à la prise de décision automatisée est complexe vis-à-vis des risques collectifs et sociétaux que la technologie d'intelligence artificielle crée à travers de sa généralisation. La difficulté d'identification des biais, le caractère presque invisible des risques et la difficile conciliation de l'obligation de transparence avec des enjeux externes tels que la cybersécurité et le secret des affaires sont d'autant de difficultés obstruant la capacité de la personne concernée à fournir un consentement libre et éclairé.

575. L'étude des difficultés liées au consentement vis-à-vis des transferts hors Union européenne relève plus de l'incompatibilité que de la nécessité de compenser ces difficultés par une action législative. *A contrario*, le consentement à la prise de décision automatisée semble pouvoir faire l'objet d'une réflexion juridique certes complexe, mais qui pourrait aboutir à la possibilité pour la personne concernée de consentir de manière satisfaisante à ces traitements. Ces difficultés s'ajoutent à la complexité pour le responsable de traitement de choisir une base légale adaptée au traitement.

CHAPITRE 2 – LE CHOIX DIFFICILE D'UNE BASE LÉGALE ADAPTÉE AU TRAITEMENT

577. Au-delà des difficultés relatives à la validité du consentement face à des traitements de données à caractère personnel complexes, les responsables de traitement se trouvent confrontés à la question de la pertinence des différentes bases légales de traitement quant au traitement qu'ils souhaitent mettre en place.

578. La question de la pertinence de la base légale du traitement de données à caractère personnel peut tout d'abord se poser lorsque la source du traitement se trouve dans la volonté de la personne concernée. En effet, la distinction du consentement RGPD et du consentement contractuel, si elle a des vertus protectrices, pose également des difficultés quant au choix de la base légale du traitement (Section 1).

579. La question de la pertinence de la base légale du traitement trouve aussi sa source dans la confrontation des intérêts du responsable de traitement et de la personne concernée. Dans ce cas, la difficulté consiste à savoir qui de la personne concernée ou du responsable de traitement est légitime à contrôler la mise en place et le contour du traitement de données à caractère personnel (Section 2).

Section 1 – Le consentement et le contrat

580. Les bases légales du consentement et du contrat ont comme point commun de reposer sur la manifestation de volonté de la personne concernée. Cependant, l'objet du consentement exprimé par la personne n'est pas le même : le consentement RGPD porte uniquement sur le traitement de données à caractère personnel, le consentement au contrat porte sur un contrat, qui peut comporter certains traitements de données à caractère personnel. Dans le second cas, la base légale du contrat ne peut concerner que les traitements de données à caractère personnel indissociables du contrat, afin d'éviter que le responsable de traitement court-circuite la liberté du consentement RGPD en proposant à la personne concernée une offre de « tout ou rien ».

581. L'élément consensuel étant commun aux bases légales du consentement et de l'exécution du contrat, il a fallu que le législateur européen trace de manière certaine la frontière entre le consentement et le contrat. Comme il l'a déjà été étudié en première partie, cette frontière est principalement déterminée par la notion de traitement « indispensable » au contrat : le traitement indispensable relève du régime de l'article 6(1)(b) du RGPD quand le traitement non indispensable relèvera d'un autre régime, dont celui du consentement RGPD.

582. Déterminer si un traitement est indispensable à l'exécution du contrat implique un effort d'interprétation, qui a été étudié à la fois par le G29 et l'EDPB. Néanmoins, des zones d'ombre persistent quant à la question de savoir si certains traitements peuvent être interprétés comme étant nécessaires à l'exécution d'un contrat. Ces zones grises sont nées soit de la réticence de certaines autorités de contrôle à appliquer l'interprétation proposée par le G29 et l'EDPB, soit de la réluctance du législateur à légiférer sur certains sujets pourtant très présents sur internet. En effet, la distinction entre consentement et contrat a récemment été remise en cause par l'autorité de contrôle irlandaise (§1), relançant le débat sur la question épineuse du régime juridique applicable à la publicité ciblée (§2).

§1 – La remise en cause de la distinction entre consentement RGPD et exécution du contrat

583. Le responsable de traitement, lorsqu'il doit déterminer s'il peut fonder son traitement sur le consentement, doit vérifier si l'issue du choix de la personne concernée a des conséquences sur l'exécution d'un contrat. Par exemple, le responsable de traitement proposant un service de *quantified self*[1175] en matière de performance sportive ne peut pas fonder le

[1175] La CNIL propose la définition suivante : « Le quantified self désigne la pratique de la "mesure de soi" et fait référence à un mouvement né en Californie qui consiste à mieux se connaître en mesurant des données relatives à son corps et à ses activités ». CNIL, « Quantified self », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/definition/quantified-self (consulté en octobre 2021).

traitement des données à caractère personnel relatif aux performances sportives de la personne concernée sur le consentement, puisque ces données sont indispensables à la délivrance du service. *A contrario*, ce même responsable de traitement ne pourra pas fonder le traitement de données à caractère personnel relatif à la mesure des performances de son application, dans la mesure où un tel traitement n'est pas nécessaire à l'exécution du contrat.

584. La réflexion du responsable de traitement sur la base légale à choisir doit donc prendre en compte différents éléments. En ce qui concerne la frontière entre contrat et consentement, le responsable de traitement devra particulièrement s'intéresser au caractère indissociable du contrat et du traitement, ainsi que sur la nature du contrat entre lui et la personne concernée. Le responsable de traitement devra donc s'attarder sur le critère de nécessité (A), qui sera évaluée sur la base de l'élément fondamental du contrat. Or, l'interprétation de cette dernière notion a récemment été remise en cause par l'autorité de contrôle irlandaise (B).

A. Le critère de nécessité

585. L'article 6(1)(b) du RGPD dispose que l'une des bases légales sur laquelle le responsable de traitement peut fonder un traitement de données à caractère personnel est l'exécution d'un contrat, c'est-à-dire la situation dans laquelle « 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 ». Le fait qu'un traitement de données à caractère personnel soit nécessaire à l'exécution d'un contrat exclut de fait la possibilité de fonder le traitement sur la base du consentement, ce qui est rappelé par l'article 7(4) du RGPD :

> « Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat ».

Dès lors, il apparaît que le critère de nécessité est un élément distinctif majeur de la base légale du consentement et de celle du contrat. Le critère de nécessité permet de différencier une ingérence dans la protection des données à caractère personnel, fondée sur le choix de la personne concernée d'une ingérence plus importante fondée sur la passation d'un contrat.

586. Le critère de nécessité est une notion régulièrement mobilisée en matière de protection des données à caractère personnel, puisque l'article 8 de la Charte des droits fondamentaux de l'Union européenne conditionne les dérogations et les limitations du droit à la protection des données à caractère personnel à la satisfaction du critère de nécessité. Dans la mesure où le

critère de nécessité conditionne la possibilité de s'ingérer dans la protection des données à caractère personnel, ce critère est d'interprétation stricte. La Cour de Justice a en effet affirmé à plusieurs reprises que « la protection du droit fondamental à la vie privée exige que les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire »[1176]. L'exigence de stricte nécessité est d'ailleurs à la fois liée au droit à la vie privée et aux conséquences de l'ingérence dans le droit à la protection des données à caractère personnel sur d'autres droits fondamentaux. Par exemple, l'EDPS considère que « l'exigence de la « stricte nécessité » découle du rôle important que le traitement des données à caractère personnel suppose pour une série de droits fondamentaux »[1177]. Le critère de nécessité est également d'interprétation stricte pour fonder un traitement sur la base légale de l'exécution d'un contrat. Le caractère strict du critère de nécessité découle de l'interprétation classique du critère de nécessité dans le droit de l'Union européenne[1178].

587. Il n'est ainsi pas étonnant qu'à la fois le G29 et l'EDPB se soient saisis de la question afin de proposer une interprétation harmonisée du critère de nécessité. Dans un avis de 2014, le G29 affirme que le critère de nécessité doit être interprété de façon restrictive afin d'éviter qu'un traitement soit « imposé unilatéralement à la personne concernée par le responsable de traitement »[1179]. Le Groupe de l'article 29 propose notamment l'exemple du profilage d'un individu, qui ne remplirait pas la condition de nécessité, quand bien même ce traitement serait mentionné au sein du contrat[1180]. D'après l'EDPB, le critère de nécessité est lié au principe de loyauté et implique une double évaluation. Premièrement, le traitement doit être objectivement nécessaire à l'exécution d'un contrat, dont les finalités doivent être communiquées de manière précise à la personne concernée[1181]. Deuxièmement, le traitement doit satisfaire le test de subsidiarité du traitement par rapport au droit à la vie privée et à la protection des données à caractère personnel[1182]. De plus, il est important de rappeler que l'EDPB, comme le G29, n'évalue pas le critère de nécessité au regard des clauses contractuelles, mais au regard de « la

---

[1176] CJUE, C-73/07, *op. cit.*, §56 ; CJUE, 9 novembre 2010, *Volker und Markys Schecke et Eifert*, C-92/09 et C-92/03, §77 et §86 ; CJUE, 7 novembre 2013, *IPI c. Geoffrey Englebert e. a.*, C-473/12.
[1177] EDPS, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017, p. 7.
[1178] EDPB, *Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées*, version 2.0, 8 octobre 2019, p. 7.
[1179] Groupe de travail « Article 29 », WP 217, *op. cit.* p. 18.
[1180] *Ibidem.*
[1181] EDPB, *Lignes directrices 2/2019*, 8 octobre 2019, *op. cit.*, p. 9.
[1182] *Ibidem.*

finalité contractuelle fondamentale et mutuellement comprise »[1183]. Cela signifie que le responsable de traitement doit à la fois identifier clairement les activités constituant le cœur du contrat et informer la personne concernée de celle-ci[1184]. Le critère de nécessité est aussi lié au principe de minimisation des données. Ainsi, le responsable de traitement ne peut pas artificiellement ajouter des traitements de données à caractère personnel inutiles à l'exécution du contrat sous prétexte que les clauses du contrat mentionnent de tels traitements. Le critère de nécessité s'évalue donc au regard de l'objet du contrat[1185].

588. Par conséquent, le critère de nécessité est une notion qui doit faire l'objet d'une interprétation par le responsable de traitement et *a fortiori,* par l'autorité de contrôle et le juge. Ce critère permet de concilier d'une part, les intérêts économiques du responsable de traitement et d'autre part, les droits des individus. Il en résulte que le fondement de l'article 6(1)(b) n'est valable que lorsque le traitement est nécessaire à l'exécution du contrat dans sa finalité contractuelle fondamentale, comprise par la personne concernée raisonnable. La Cour de Justice a par exemple considéré que la conservation d'une copie de titre d'identité à des fins d'identification des clients n'était pas nécessaire à l'exécution d'un contrat quand la société conclut par ailleurs le même contrat avec des personnes ayant refusé ce traitement[1186]. L'évaluation du critère de nécessité ne s'évalue d'ailleurs qu'en prenant en compte le contrat actuellement conclu, dans sa finalité fondamentale, ce que l'EDPB a expressément rappelé à propos du stockage des données relatives aux cartes de crédit :

> « Si, en premier lieu, le traitement des données relatives à la carte de crédit utilisée par le client pour payer est nécessaire à l'exécution du contrat, déclenchant ainsi l'application de l'article 6, paragraphe 1, point b), du RGPD, le stockage de ces données n'est utile que pour faciliter l'éventuelle prochaine transaction et faciliter les ventes. Une telle finalité ne saurait être considérée comme strictement nécessaire à l'exécution du contrat pour la fourniture du produit ou du service que la personne a déjà payé »[1187].

589. Il est ainsi généralement admis que le consentement contractuel au traitement de ses données à caractère personnel ne peut être valable que si ce traitement est nécessaire aux éléments fondamentaux du contrat. Pourtant, il semble que l'interprétation de la notion

---

[1183] *Idem,* p. 11.
[1184] *Ibidem.*
[1185] L'autorité de contrôle slovène a lié le principe de minimisation des données et le critère de nécessité dans un arrêt de 2019. Elle a décidé que la création d'un compte en banque ne nécessitait pas de traiter les données relatives au statut marital ou à l'emploi du client ouvrant son compte en banque. IP, 5 novembre 2019, 0712-1/2019/2504 ; résumé disponible sur GDPR Hub, « IP — 0712-1/2019/2504 », *GDPRhub.eu,* disponible sur https://gdprhub.eu/index.php?title=IP_-_0712-1/2019/2504 (consulté en novembre 2021).
[1186] CJUE, 11 novembre 2020, C-61/19, *op. cit.,* §45-46.
[1187] EDPB, *Recommandations 02/2021 sur la base juridique pour le stockage des données relatives aux cartes de crédit dans le seul but de faciliter la poursuite des transactions en ligne*, adoptées le 19 mai 2021, p. 3.

d'élément fondamental du contrat soit remise en cause par l'interprétation de l'autorité de contrôle irlandaise.

B. La remise en cause de l'interprétation de l'élément fondamental du contrat

590. Il semblerait que l'interprétation proposée par l'EDPB, qui est non contraignante, ne soit pas partagée par l'ensemble des autorités de contrôle. En effet, l'autorité de contrôle irlandaise a récemment admis, dans une proposition de décision, une interprétation de la base légale contractuelle plus large dans l'affaire *LB c. Facebook Limited*[1188]. En l'espèce, le requérant conteste la possibilité pour Facebook de fonder un certain nombre de traitements sur la base légale de l'exécution du contrat, dont notamment le traitement ayant pour finalité la publicité comportementale.

591. Dans le contrat entre Facebook et son utilisateur, la première section est réservée à l'objectif de fournir une expérience personnalisée[1189]. À l'intérieur de cette section, le réseau social précise rapidement que cette personnalisation s'effectue à l'aide des données collectées à partir des *posts*, *stories*, événements, publicités et autres contenus regardés par l'utilisateur sur la plateforme[1190]. De plus, la quatrième section du contrat est consacrée à l'objectif de faire découvrir à l'utilisateur des contenus, produits et services qui peuvent l'intéresser, à travers des publicités, offres et contenus sponsorisés[1191]. Selon Facebook, la publicité comportementale constitue le cœur du service proposé étant donné qu'il s'agit d'une de ces « caractéristiques distinctives ».[1192]

592. Dans sa proposition de décision, l'autorité de contrôle irlandaise estime que Facebook peut légalement fonder son traitement relatif à la publicité comportementale sur le fondement de l'article 6(1)(b) du RGPD. La DPC considère que la publicité comportementale est incluse dans « le cœur du service proposé », dans la mesure où Facebook est présenté comme un service personnalisé incluant la publicité et que l'entreprise Facebook est financée par la publicité

[1188] DPC, 6 octobre 2021, Draft Decision, *LB (through NOYB) v. Facebook Ireland Limited*, Draft Decision for the purposes of article 60 GDPR of the Data Protection Commission made pursuant to Section 113 (2)(a) of the Data Protection Act 2018.
[1189] *Idem,* § 4.36.
[1190] *Idem,* §4,37.
[1191] *Idem,* §4,38.
[1192] L'EDPB, dans ses lignes directrices 2/2019, affirme que la première question à se poser pour savoir si l'article 6 (1) (b) est applicable à un traitement est la suivante : « quelle est la nature du service fourni à la personne concernée ? Quelles sont ses caractéristiques distinctives ? ». Facebook répond ainsi à cette question en considérant que la nature du service fourni à la personne concernée est un réseau social personnalisé, dont la publicité comportementale est une caractéristique distinctive. v. EDPB, *Lignes directrices 2/2019*, 8 octobre 2019, *op. cit.,* p. 11 ; DPC, 6 octobre 2021, Draft Decision, *op. cit.,* §4,39.

comportementale[1193]. D'après l'autorité de contrôle ; la publicité comportementale constituant « le cœur de la transaction commerciale » entre l'utilisateur et Facebook et il n'y a pas de doute que l'utilisateur raisonnable comprend que la publicité comportementale est un élément fondamental du contrat[1194]. De plus, la DPC refuse l'interprétation du critère de nécessité comme un élément rendant impossible la délivrance d'un service ou d'un contrat et préfère interpréter le critère de nécessité comme un élément nécessaire par rapport « au cœur du fonctionnement d'un contrat spécifique »[1195].

593. Ce faisant, l'autorité de contrôle vide de substance la condition de nécessité en l'appliquant non pas au regard de « l'exécution du contrat », mais des intérêts pécuniaires du responsable de traitement. Le glissement terminologique du texte proposé par l'autorité de contrôle est d'ailleurs révélateur de la démarche. En effet, la CPD reprend volontairement les termes « élément fondamental du contrat » (*core function*) pour asseoir son interprétation sur les lignes directrices de l'EDPB[1196] puis glisse, au fil de son raisonnement, vers des termes plus économiques tels que « cœur du modèle économique » (*core of business model*), « cœur du marché conclu » (*core of the bargain being struck*), « élément fondamental de la transaction commerciale » (*core element of the commercial transaction*). Or, un traitement nécessaire au modèle économique d'une entreprise n'est pas un traitement nécessaire à la finalité du contrat, ce que la CNIL avait déjà affirmé en 2017 :

> « S'agissant de l'exécution d'un contrat, la formation restreinte relève que l'objet principal du service est la fourniture d'un réseau social : les utilisateurs qui créent un compte sur le site […] souhaitent d'abord accéder aux fonctionnalités de ce réseau, c'est-à-dire interagir avec leurs relations, créer des groupes d'intérêt commun, organiser des événements ou partager des contenus tels que des photos ou des articles de presse. Ils ne s'inscrivent pas au réseau social pour recevoir de la publicité ciblée »[1197].

L'EDPB s'oppose aussi à une telle interprétation dans la mesure où la publicité ciblée ne relève pas de l'exécution du contrat, mais du financement indirect de la fourniture d'un service. En effet, le comité constate que « bien qu'un tel traitement puisse contribuer à la prestation d'un service, cela ne suffit pas en soi à établir qu'il est nécessaire à l'exécution du contrat en question »[1198]. L'EDPB justifie son interprétation au regard de la nature de droit fondamental de la protection des données à caractère personnel, et au regard de la finalité du RGPD « de

[1193] DPC, 6 octobre 2021, Draft Decision, *op. cit.*, §4.42-4.43.
[1194] *Idem*, § 4.43.
[1195] *Idem*, § 4.47.
[1196] *Idem*, § 4.31.
[1197] CNIL, SAN-2017-006, 27 avril 2017, *op. cit.*
[1198] EDPB, *Lignes directrices 2/2019*, 8 octobre 2019, *op. cit.* p. 16.

permettre aux personnes concernées de contrôler les informations les concernant », impliquant pour le comité que « les données à caractère personnel ne sauraient être considérées comme une marchandise négociable »[1199].

594. Le recours à la « spécificité » du contrat entre Facebook et l'utilisateur n'est pas plus convaincant étant donné que l'inscription d'un traitement au sein d'un contrat ne le rend pas pour autant nécessaire. Si Facebook peut revendiquer la personnalisation de ses services comme l'une de ses « caractéristiques distinctives » d'autres réseaux sociaux, il ne semble pas que la personnalisation d'un réseau social puisse inclure la personnalisation des publicités présentes sur ce réseau. Dès lors, Facebook peut justifier la personnalisation du réseau social (la suggestion de *posts, stories*, ou contact à l'utilisateur) sur l'exécution du contrat, mais pas la personnalisation des publicités, puisqu'il s'agit d'une activité annexe à celle du service de réseau social. Si l'on se place du côté de la personne concernée, le choix d'un réseau social sur un marché peut être influencé par la personnalisation du contenu. En revanche, il n'est pas établi que de la personnalisation de la publicité proposée par le service soit un critère décisif du choix d'un réseau social. Cette solution a notamment été adoptée par le Tribunal de Grande Instance de Paris le 7 août 2018. Le TGI avait jugé les clauses contractuelles de Twitter comme illicites au regard de la Loi informatique et Liberté et abusives au regard du Code de la Consommation, parce que ces clauses « se contentent de présenter la collecte des données personnelles, fournies par l'utilisateur, comme étant la nécessaire contrepartie de l'accès aux « Services » procuré par Twitter » et par conséquent, « de présupposer chez l'utilisateur un consentement implicite à l'intégralité des conditions générales d'utilisation, sans solliciter son consentement exprès à la collecte et au traitement de ses données personnelles ».[1200]

595. Enfin, il semble que l'intention même du législateur ait été d'autoriser la publicité ciblée sur la base du consentement, ce qui a une fois de plus été explicitement rappelé récemment par la proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques[1201]. De plus, la directive *e-privacy* énonce expressément que « les utilisateurs devraient avoir la possibilité de refuser qu'un témoin de connexion ou un dispositif similaire soit placé sur leur équipement terminal »[1202]. Selon la CNIL, la nécessité du

[1199] *Ibidem.*
[1200] TGI Paris, 7 août 2017, *UFC Que Choisir c. Twitter Inc et Twitter International Company*, n° RG 14/07300.
[1201] La proposition rappelle « la nécessité d'obtenir le consentement de la personne concernée avant de traiter des données à caractère personnel à des fins de publicité ciblée ». Commission européenne, COM (2020) 825 final, *op. cit.*, considérant 52.
[1202] Directive 2002/58/CE, 12 juillet 2002, considérant 25. L'article 5 (3) de la même directive énonce également que l'utilisateur doit avoir le droit de refuser un tel traitement.

consentement pour « certaines utilisations des données ayant une finalité publicitaire » est une règle d'ordre public, « c'est-à-dire qu'il ne peut pas y être dérogé par contrat »[1203].

596. Si la décision de l'autorité de contrôle irlandaise paraît critiquable à de nombreux égards, celle-ci reste juridiquement intéressante tant la question de la publicité ciblée est complexe et irrésolue par le législateur.

§2 – La question épineuse de la publicité ciblée

597. La question de la publicité ciblée est une question épineuse pour le législateur européen. Devenue essentielle à la survie de nombreux acteurs du numérique, cette pratique implique néanmoins la création de traitements de données à caractère personnel très intrusifs et très risqués au regard de la personne concernée[1204].

598. Dès lors, fonder les traitements de données à caractère personnel relatifs à la publicité ciblée sur le consentement de la personne concernée représente un risque pour le responsable de traitement de voir ses revenus diminuer drastiquement. Par exemple, le créateur de bannières de cookies Axeptio évalue que le taux d'*opt-in* d'une bannière de cookies permettant d'accepter, de refuser, ou de granuler son consentement aux cookies se situe entre 50 et 70%[1205]. La perte financière peut être d'autant plus importante que certains services de publicité exigent également le consentement aux cookies d'une personne concernée pour la délivrance de publicités non personnalisées. C'est par exemple le cas de Google Ad Manager qui requiert le consentement aux cookies pour les publicités non personnalisées, car celles-ci « utilisent aussi les cookies ou des identifiants mobiles pour lutter contre la fraude et les abus, pour la limitation du nombre d'expositions et pour la création de rapports sur les annonces agrégées »[1206]. Un autre exemple, qui montre l'ampleur de la perte des revenus publicitaires du fait d'une plus

---

[1203] CNIL, « Cookies walls et monétisation des données personnelles : les enjeux juridiques et éthiques », *CNIL.fr*, 31 mai 2021, disponible sur https://www.cnil.fr/en/node/121204 (consulté en novembre 2021).

[1204] V. notamment CNIL, « Publicité ciblée en ligne : quels enjeux pour la protection des données personnelles ? », *CNIL.fr*, 14 janvier 2020, disponible sur https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles (consulté en novembre 2021) ; Parlement européen, *Online advertising : the impact of targeted advertising on advertisers, market access and consumer choice*, Policy Department for Economic, Scientific and Quality of Life Policies, juin 2021, 154 p.

[1205] Axeptio, « Tout savoir sur les taux d'opt in cookies chez Axeptio », *Axeptio.eu*, disponible sur https://www.axeptio.eu/post/tout-savoir-sur-les-taux-dopt-in-cookies-chez-axeptio (consulté en novembre 2021).

[1206] « For non-personalized ads, consent for cookies or mobile identifiers is still required because non-personalized ads still use cookies or mobile identifiers to combat fraud and abuse, for frequency capping, and for aggregated ad reporting » (traduction libre). Google Ad Manager, « Ad Manager and Ad Exchange program policies. Publisher integration with the IAB TCF v. 2.0 », Google Ad Manager Help, disponible sur https://support.google.com/admanager/answer/9805023?hl=en&ref_topic=28145 (consulté en novembre 2021). La politique de Google Ad Manager peut sembler étonnante dans la mesure où l'ensemble des finalités de traitement énumérées pourraient, dans une certaine mesure, relever de l'intérêt légitime.

grande protection des données à caractère personnel, est le procès en cours intenté par un investisseur de Snapchat devant la Cour fédérale de district californienne[1207]. En l'espèce, l'investisseur accuse les responsables de Snapchat d'avoir délibérément sous-estimé les conséquences du changement de politique de protection des données d'Apple, restreignant l'accès aux données à caractère personnel sur sa plateforme iOS[1208]. Le changement de politique d'Apple avait en effet entraîné des conséquences financières sur l'entreprise Snapchat, dont l'annonce des pertes de revenus publicitaires avait fait perdre 26% à la valeur de ses actions[1209].

599. Du côté de la personne concernée, la publicité ciblée est une intrusion importante dans son droit à la protection de ses données à caractère personnel. Comme le souligne la CNIL,

> « aujourd'hui, de nombreux acteurs sont en mesure d'accumuler suffisamment d'informations pour créer des profils individuels très détaillés. Ces profils peuvent produire, au fil du temps, une image complète et plus ou moins exacte de votre personnalité, voire révéler des informations que vous n'aurez pas choisi d'exposer (par exemple, des données relatives à vos opinions politiques inférées à partir de l'analyse de vos lectures sur des sites d'information ou encore qui indiqueraient votre orientation sexuelle, par l'identification du genre des personnes dont vous consultez les profils sur des sites de rencontre »[1210].

Alors, comment faire pour concilier d'une part, les intérêts économiques des responsables de traitement et d'autre part, la protection des données à caractère personnel des personnes concernées ? L'absence de cadre juridique spécifique et précis régissant la publicité ciblée est-elle révélatrice de l'impossibilité de conciliation de ces enjeux ?

600. Tout d'abord, s'il n'y a pas de cadre juridique spécifique s'appliquant à la publicité comportementale, celle-ci n'en est pas moins régie par le droit de la protection des données à caractère personnel. Le RGPD « impose, en principe, le consentement pour l'utilisation des traceurs sur l'appareil de l'utilisateur »[1211]. Dans le paragraphe précédent, il a été étudié que la base légale du consentement se déduit d'une part de l'interprétation restrictive de la notion de traitement nécessaire à l'exécution du contrat, et d'autre part, du texte de la directive *e-privacy*, qui invite les responsables de traitement à permettre aux utilisateurs de refuser le placement de traceurs sur leur terminal. La nécessité de garantir à la personne concernée le choix de faire

---

[1207] United States District Court, Central District of California, *Kellie Black v. Snap Inc. et al.*, Class Action Complaint for Violation of the Federal Securities Laws, Case 2:21-cv-08892.
[1208] *Idem*, §22.
[1209] *Idem*, §31-32.
[1210] CNIL, « Publicité ciblée en ligne : quels enjeux pour la protection des données personnelles », *CNIL.fr*, 14 janvier 2020, disponible sur https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles (consulté en novembre 2021).
[1211] *Ibidem.*

l'objet d'un traitement en vue de la diffusion de publicité ciblée avait par ailleurs figuré parmi les résultats de la consultation nationale publique sur le droit à l'oubli numérique de 2009, ayant abouti à la Charte sur la publicité ciblée et la protection des internautes[1212].

601. Ce constat désormais dressé, deux zones grises sus-étudiées ont déjà retenu notre attention : les *cookie paywalls* et l'interprétation irlandaise du RGPD permettant de considérer la publicité ciblée comme étant « nécessaire à l'exécution d'un contrat ». Ces zones grises, toutes deux nées de la volonté de l'interprète de la loi[1213] d'adapter celle-ci aux réalités économiques de la publicité ciblée, conduisent à se demander si le législateur ne devrait pas à nouveau intervenir pour préciser l'équilibre entre les intérêts de la personne concernée et les intérêts économiques du responsable de traitement. Si les rôles du législateur créateur de droit et du juge interprète hérités de Montesquieu se sont révélés maintes fois dépassés en matière de protection des données à caractère personnel[1214], laisser au juge ou à l'autorité de contrôle le devoir d'arbitrer la question de la publicité ciblée risque de transformer « ce qui devrait être un choix collectif et politique en une multitude d'arbitrages individuels »[1215]. Or, ces arbitrages montrent déjà l'embarras de l'interprète de la loi, face à une pratique encore légale, mais dont le régime met en danger sa survie :

> « Google, pour assurer une acceptation totalement libre, doit alors proposer ses services « gratuits » en priant humblement chaque utilisateur de bien vouloir cocher une case relative à la publicité personnalisée. Celui qui refusera en conscience, ou plus vraisemblablement parce qu'il a cliqué sur le bouton « suivant » sans lire bénéficiera pleinement du service, mais sans subir aucun *tracking*. Qui, dans ces conditions, « choisira », de manière éclairée et sans équivoque, d'être pisté ? C'est évidemment la fin d'un modèle d'affaires, une interdiction de fait qui ne dit pas son nom »[1216].

602. Dans ce contexte, les interprétations proposées par le juge et les autorités de contrôle semblent être autant de bricolages juridiques et d'appels du pied au législateur, afin de créer un cadre juridique satisfaisant sur la publicité ciblée. La réaction de la CNIL face à la décision du Conseil d'État rejetant l'illicéité de principe des *cookies paywall* est symptomatique de la

---

[1212] Union française du Marketing Direct, *Charte sur la publicité ciblée et la protection des internautes,* 2010. Élaborée suite à une consultation publique à l'initiative de Nathalie Kosciusko-Morizet, la Charte comporte des recommandations à l'égard des acteurs du marketing en ligne. La recommandation n° 2, intitulée « permettre le libre choix des internautes », est formulée ainsi : « Les Associations professionnelles recommandent que différents moyens, selon la publicité diffusée, soient mis à la disposition des utilisateurs pour leur permettre […] d'accepter ou de refuser la diffusion à leur égard de contenus publicitaires adaptés à leur comportement de navigation ».

[1213] Dans le premier cas, le juge à travers le Conseil d'État ; dans le second cas, l'autorité de contrôle à travers la Commission de protection des données (CPD).

[1214] Montesquieu, *De l'Esprit des Lois,* Tome Premier, Éditions Gallimard, 1995, pp. 112-117.

[1215] NETTER Emmanuel, avril 2021, *op. cit.*, p. 226.

[1216] NETTER Emmanuel, novembre 2020, *op. cit.*, p. 611.

nécessité de disposer d'un cadre juridique plus pérenne sur la publicité ciblée : l'autorité de contrôle française annonce devoir poursuivre « son analyse à la lumière de l'arrêt du Conseil d'État pour déterminer les cas justifiant la présence d'un mur de traceurs au regard des alternatives disponibles pour la personne »[1217] tout en espérant à demi-mot que le futur règlement *e-privacy* permette de « fixer des règles plus précises en la matière »[1218].

603. Le législateur européen paraît en effet vouloir préciser dans une certaine mesure le régime de la publicité comportementale. La proposition de règlement *e-privacy* prévoit, dans son article 8, une liste de bases légales sur lesquelles le responsable de traitement peut utiliser les informations stockées dans les équipements terminaux des utilisateurs finaux. Le juriste retrouve la logique du règlement dans le choix de ses bases légales, puisque parmi elles figurent le consentement de l'utilisateur[1219], expressément interprété comme le consentement RGPD[1220], et le traitement « nécessaire pour fournir un service de la société de l'information demandé par l'utilisateur final »[1221]. Si retrouver la logique du RGPD est rassurant du point de vue de la cohérence de l'arsenal législatif européen en matière de protection des données, force est de constater que l'arbitrage entre les intérêts de la personne concernée et les intérêts économiques du responsable de traitement est encore une fois méticuleusement évité et renvoyé à l'interprétation des autorités de contrôle et des juges en la matière. Tout au plus, la proposition de règlement pourrait traduire une volonté du législateur de fonder la publicité ciblée sur le consentement RGPD dans le considérant 18 :

> « L'utilisateur final peut consentir au traitement de ses métadonnées afin de bénéficier de services spécifiques comme des services de protection contre les autorités frauduleuses (par l'analyse en temps réel des données d'utilisation et de localisation et du compte client. Dans l'économie numérique, les services sont souvent fournis moyennant une contrepartie non pécuniaire, par exemple, l'exposition de l'utilisateur final aux publicités. Aux fins du présent règlement, le consentement de l'utilisateur final, que celui-ci soit une personne physique ou morale, devrait avoir le même sens et être soumis aux mêmes conditions que le consentement de la personne concernée en vertu du règlement (UE) 2016/679 »[1222].

604. La confusion du lecteur de ce considérant traduit probablement les difficultés du législateur à appréhender la question de la publicité ciblée. Il serait difficile de voir, dans ces

---

[1217] CNIL, « Cookie walls et monétisation des données personnelles : les enjeux juridiques et éthiques », *CNIL.fr*, 31 mai 2021, disponible sur https://www.cnil.fr/fr/cookie-walls-et-monetisation-des-donnees-personnelles-les-enjeux-juridiques-et-ethiques (consulté en novembre 2021).
[1218] *Ibidem.*
[1219] Commission européenne, COM/2017/010 final, *op. cit.*, Article 8.
[1220] *Idem,* Article 9.
[1221] *Idem,* Article 8.
[1222] *Idem,* considérant 18.

réflexions si décousues, une volonté expresse du législateur d'inscrire la publicité ciblée sous le régime du consentement RGPD. Cependant, ce considérant pourrait traduire la volonté du législateur de faire sortir la publicité ciblée de la base légale du traitement nécessaire à la fourniture du service afin de le faire entrer exclusivement dans la base légale du consentement RGPD. Une telle interprétation peut être soutenue par la proposition du Conseil de l'Union européenne d'ajouter un nouveau considérant, prenant en compte la situation du marché :

> « Contrairement à l'accès au contenu d'un site web fourni contre un paiement monétaire, quand l'accès est fourni sans paiement monétaire direct et est dépendant du consentement de l'utilisateur final au stockage et à la lecture de cookies à des fins supplémentaires, exiger un tel consentement ne serait normalement pas considéré comme privant l'utilisateur final d'un véritable choix s'il est en mesure de choisir entre les services, sur la base d'une description claire, précise et *user-friendly* des informations sur les finalités des cookies et techniques similaires, entre d'une part, une offre qui inclut le consentement à l'utilisation des cookies à des fins supplémentaires et d'autre part, une offre équivalente du même prestataire qui n'implique pas de consentir à l'utilisation des données à des fins supplémentaires, d'autre part. À l'inverse, dans certains cas, rendre l'accès au contenu du site dépendant du consentement à l'utilisation de tels cookies peut être considéré, en présence d'un net déséquilibre entre l'utilisateur final et le fournisseur de services, comme privant l'utilisateur final d'un véritable choix. Ce serait normalement le cas pour les sites web fournissant certains services, comme ceux fournis par les pouvoirs publics. De même, un tel déséquilibre pourrait exister lorsque l'utilisateur final n'a que peu ou pas d'alternatives au service, et donc n'a pas vraiment le choix quant à l'utilisation des cookies, par exemple en cas de services de prestataires en position dominante »[1223].

Combiné avec la proposition du Conseil de l'Union européenne de préciser la base légale de la fourniture du service par la formule « strictement nécessaire pour fournir un service de la société de l'information spécifiquement demandé par l'utilisateur final »[1224], ce considérant a le mérite de préciser où doit se situer l'arbitrage de l'interprète de la loi. Premièrement, il semble

---

[1223] « In contrast to access to website content provided against monetary payment, where access is provided without direct monetary payment and is made dependent on the consent of the end-user to the storage and reading of cookies for additional purposes, requiring such consent would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice. This would normally be the case for websites providing certain services, such as those provided by public authorities. Similarly, such imbalance could exist where the end-user has only few or no alternatives to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a dominant position » [traduction libre]. Conseil de l'Union européenne, 2017/0003 (COD), *op. cit.,* considérant (20 aaa).

[1224] *Idem,* article 8.

bien que le législateur rejette bel et bien l'hypothèse de fonder la publicité sur la base de l'exécution du contrat ou de la fourniture du service, dont l'application stricte et spécifique de la nécessité est très clairement rappelée par le Conseil. Deuxièmement, le Conseil de l'Union européenne confirme la solution du Conseil d'État[1225], en affirmant clairement que la liberté du consentement ne s'oppose pas à proposer une offre payante exempte de tout consentement au placement de cookies, en parallèle d'une offre gratuite dépendante du consentement de la personne concernée. Dès lors, le fait de devoir payer l'accès à un service ne s'analyse pas forcément, selon la proposition du législateur, comme un préjudice au sens du considérant 42 du RGPD[1226]. D'après la proposition du Conseil, un tel préjudice naîtrait dans le cas où le fournisseur de service dont le service est soit incontournable (par exemple, le service offert par les pouvoirs publics) soit si dominant sur le marché qu'il n'existe pas réellement d'alternatives pour le consommateur (la situation du fournisseur de service en position dominante).

605. L'analyse proposée par le Conseil de l'Union européenne n'est pas sans rappeler le lien entre données à caractère personnel, droit de la concurrence et droit de la consommation. En 2018, le TGI de Paris avait condamné Twitter sur le fondement des clauses abusives, y compris les dispositions de sa politique de confidentialité[1227]. En 2019, l'autorité fédérale de la concurrence allemande (*Bundeskartellamt*) avait condamné Facebook pour abus de position dominante, considérant que l'entreprise américaine avait utilisé sa position dominante sur le marché des réseaux sociaux pour croiser un grand nombre de données, violant ainsi les règles européennes de protection des données[1228]. Concernant la liberté de choix de la personne concernée, l'analyse du marché par le Conseil de l'Union européenne paraît pertinente dans la mesure où, dans le cadre de la fourniture de service, cette analyse prend en compte la double nature de l'utilisateur, à la fois personne concernée et consommateur. Dès lors, l'autorité de contrôle et le juge devront interpréter la notion de liberté de consentement au placement de cookies à finalité publicitaire à la fois sur le fondement de la validité du consentement RGPD et de la situation économique de la personne concernée et du responsable de traitement.

[1225] CE, 19 juin 2020, n° 434684, *op. cit.*.

[1226] « Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice ». RGPD, 27 avril 2016, considérant 42.

[1227] TGI Paris, 7 août 2018, *op. cit.*

[1228] Bundeskartellamt, « Bundeskartellamt prohibits Facebook from combining user data from different sources », *Bundeskartellamt.de*, 7 février 2019, disponible sur https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (consulté en novembre 2021).

606. Conclusion de Section. – La distinction de la base légale du consentement et la base légale contractuelle est l'objet d'une distinction textuelle explicite, mais dont les contours font l'objet de contestations dans la pratique. Il revient dès lors au législateur de prendre en compte les difficultés posées par la distinction entre consentement RGPD et consentement contractuel, notamment en précisant le régime juridique de la pratique qui se situe au nœud du problème. : la publicité comportementale. Ces précisions sont d'autant plus souhaitables que le contrat n'est pas le seul fondement dont la frontière avec le consentement doit être clarifiée puisqu'il semble que le fondement de l'intérêt légitime fasse également l'objet d'une confusion avec le consentement.

Section 2 — Le consentement et l'intérêt légitime

607. L'intérêt légitime est l'une des six bases légales prévues par l'article 6 du RGPD permettant de fonder un traitement de données à caractère personnel. En effet, l'article 6 (1) (f) dispose :

> « 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 ».

608. Contrairement au consentement et au contrat, il paraît *a priori* que le consentement et l'intérêt légitime ne sont pas des bases légales difficiles à distinguer, tant elles ne procèdent pas des mêmes intérêts et des mêmes logiques. D'un côté, le consentement s'inscrit dans une logique d'autonomie personnelle, permettant à la personne concernée d'avoir le contrôle de ses données à caractère personnel. De l'autre, l'intérêt légitime résulte d'une logique de marché intérieur, permettant au responsable de traitement de traiter des données à caractère personnel dans le cadre de son activité économique.

609. Si, à première vue, ces deux bases légales ne devraient pas être confondues, la pratique de l'intérêt légitime par les responsables de traitement a contribué à rendre les contours de la distinction entre les bases légales vagues en pratique. En ce sens, certains commentateurs du RGPD ont été très critiques avec la base légale de l'intérêt légitime, considérant qu'il s'agissait en pratique d'un vide juridique [« *loophole* »] exploitable pour contourner le RGPD[1229]. De plus, l'utilisation de la base légale de l'intérêt légitime comporte un élément hérité de la logique d'autonomie personnelle. En basant le traitement sur le fondement de l'intérêt légitime, le responsable de traitement soumet celui-ci au régime du droit d'opposition. Ainsi, la personne concernée possède la possibilité de s'opposer à tout moment à un traitement fondé sur la base légale de l'intérêt légitime, ce qui, en cas d'intérêt légitime conçu comme important, s'assimile à un mécanisme d'*opt-out* en faveur de la personne concernée.

610. Par conséquent, l'intérêt légitime doit faire l'objet d'une évaluation de la part du responsable de traitement, dans la mesure où il doit répondre à certaines conditions afin de pouvoir constituer la base légale du traitement (§1). Or, la part de subjectivité dans l'évaluation

[1229] KAMARA Irene, DE HERT Paul, « Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach, *Brussels Privacy Hub*, Vol. 4, n°12, août 2018, Working paper disponible sur ssrn : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228369 (consulté en novembre 2021).

du responsable de traitement a pu faire craindre l'utilisation de la base légale de l'intérêt légitime comme base légale de convenance (§2).

§1 — Les conditions d'application de la base légale de l'intérêt légitime

611. Pour pouvoir fonder un traitement sur la base légale de l'intérêt légitime, le responsable de traitement doit remplir trois conditions : la légitimité du traitement, la nécessité du traitement et la mise en balance des droits et intérêts en cause[1230].

612. La première condition, la légitimité du traitement, ne pose pas de difficultés particulières. En effet, le G29 considère que « la notion d'intérêt légitime pourrait inclure des intérêts très variés, qu'ils soient futiles ou incontestables, évidents ou plus controversés »[1231] : la légitimité de l'intérêt est donc une notion vaste[1232]. En réalité, pour être légitime, l'intérêt doit remplir trois conditions. Premièrement, l'intérêt légitime doit être licite[1233] au sens d'« acceptable au regard du droit » (*in accordance with the law*). Le G29 précise que l'appréciation de la licéité de l'intérêt légitime doit être identique à celle de la licéité de la finalité du traitement[1234]. Il en résulte que la licéité de l'intérêt doit s'évaluer non seulement au niveau du droit de la protection des données à caractère personnel, mais aussi à l'égard de « toutes formes de droit écrit ou de *common law*, primaire ou de droit dérivé, arrêtés municipaux, précédents judiciaires, principes constitutionnels, droits fondamentaux et autres principes juridiques ainsi que de la jurisprudence »[1235]. Deuxièmement, l'intérêt légitime doit « être formulé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée »[1236]. Cette condition, d'ordre formel, permet le contrôle de l'intérêt légitime vis-à-vis sa nécessité et de sa prévalence vis-à-vis des intérêts, libertés et droits fondamentaux de la personne concernée. Troisièmement, il doit être « réel et présent »[1237], c'est-à-dire que le responsable de traitement

---

[1230] V. notamment CNIL, « L'intérêt légitime : comment fonder un traitement sur cette base légale ? », *CNIL.fr*, 2 décembre 2019, disponible sur https://www.cnil.fr/fr/les-bases-legales/interet-legitime (consulté en octobre 2021).
[1231] Groupe de travail, WP 217, *op. cit.*, p. 27.
[1232] Par exemple, la Commission européenne et le Conseil d'État néerlandais ont annulé la décision de l'autorité de protection néerlandaise (l'Autoriteit Persoongegevens), qui affirmait qu'un intérêt purement commercial ne pouvait constituer un intérêt légitime. V. Rechtbank Midden-Nederland, 23/11/2020, *VoetbalTV BV et Autoriteit Persoonsgegevens*, UTR20/23/15 ; Raad van State, 27/07/2022, *VoetbalTV BV et Autoriteit Persoonsgegevens*, 20100045/1/43 ; Commission européenne, *Lettre ouverte destinée à Mr Aleid Wofsen*, Bruxelles, 06/03/2020, (2020) 1417369.
[1233] Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 27.
[1234] *Idem*, p. 28, note de bas de page 48.
[1235] Groupe de travail « Article 29 », WP 203, *op. cit.*, p. 20.
[1236] Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 28.
[1237] *Ibidem.*

ne doit pas invoquer un intérêt légitime hypothétique qui pourrait naître dans le futur pour fonder un traitement.

613. La deuxième condition est celle de la nécessité du traitement : le traitement ne peut être fondé sur la base légale de l'intérêt légitime que si ce traitement est nécessaire pour atteindre l'objectif poursuivi[1238]. La nécessité est évaluée en deux temps. Tout d'abord, il convient de vérifier l'existence d'un lien entre le traitement et l'objectif poursuivi (l'intérêt légitime)[1239]. Ensuite, la notion de nécessité est interprétée de manière classique, c'est-à-dire que l'évaluateur va chercher « s'il existe d'autres moyens plus respectueux de la vie privée susceptibles de servir la même finalité »[1240].

614. Enfin, la dernière condition est la plus subjective et demande un effort de mise en balance des intérêts par le responsable de traitement. En effet, l'article 6 (1) (f) précise que la base légale de l'intérêt légitime ne peut être invoquée qu'à la condition que ne prévalent pas les intérêts ou les droits et libertés de la personne concernée. Le responsable de traitement doit alors s'efforcer d'identifier les intérêts ou les droits et libertés de la personne concernée avant d'évaluer la valeur de l'intérêt légitime et la gravité des incidences du traitement sur les intérêts et droits de la personne concernée.

615. Le responsable de traitement a la charge d'identifier les droits fondamentaux ou les libertés de la personne concernée. Contrairement au libellé de la directive 95/46/CE dont l'article 7 (f) limitait les droits et libertés de la personne concernée à évaluer par le responsable de traitement à ceux inscrits à l'article 1 (1) de la directive[12411242], le RGPD ne restreint pas le champ des droits et libertés à prendre en compte[1243]. Les droits et libertés de la personne concernée ne se restreignent dès lors pas aux droits habituellement liés à la protection des données à caractère personnel, tels que le droit à la vie privée ou encore la liberté d'expression. Par exemple, il a été mis en valeur par les instances de l'Union européenne et du Conseil de

---

[1238] *Idem*, p. 32
[1239] *Ibidem.*
[1240] *Ibidem.*
[1241] L'article 7 (f) de la directive 95/46/CE dispose : « Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que […][s'il] est nécessaire 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 fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1 ». Directive 95/46/CE, 24 octobre 1995, Article 7(f).
[1242] L'article 1 (1) de la directive 95/46/CE dispose : « Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel ». Directive 95/46/CE, 24 octobre 1995, Article 1 (1)
[1243] Si dans l'article 7 (f) de la directive, la restriction des droits et libertés par la mention de l'article 1 (1) paraît superfétatoire tant l'article 1 (1) est rédigé dans des termes vagues et larges, il est tout de même utile de mentionner cette évolution puisqu'aucun moyen se fondant sur une telle restriction ne pourra désormais être soulevé.

l'Europe que les traitements de données à caractère personnel dans le cadre de l'intelligence artificielle faisaient courir aux personnes concernées des risques importants de discrimination[1244].

616. Le responsable de traitement doit également identifier les intérêts de la personne concernée[1245]. Le G29 interprète la notion d'intérêts de la personne concernée de manière parallèle avec la notion d'intérêts du responsable de traitement :

> « Si le responsable de traitement — ou le tiers en cas de communication des données — peut poursuivre n'importe quel intérêt, pour autant qu'il ne soit pas illégitime, la personne concernée devrait aussi pouvoir s'attendre à ce que ses intérêts de toutes sortes soient pris en considération et mis en balance avec ceux du responsable du traitement, pour autant qu'ils soient pertinents dans le champ d'application de la directive ».[1246]

617. Une fois que le responsable de traitement a identifié l'ensemble des intérêts et libertés et droits fondamentaux de la personne concernée sur lesquels le traitement pourrait avoir une incidence, le responsable de traitement doit appliquer le critère de mise en balance. Il s'agit de la condition la plus complexe selon la CNIL[1247]. Le responsable de traitement va devoir mesurer, au cas par cas, l'ampleur de l'intrusion du traitement sur les intérêts et droits de la personne concernée[1248], afin de déterminer leur place sur un spectre gradué de l'incidence anodine à l'incidence très préoccupante[1249]. Pour ce faire, le responsable de traitement doit prendre en compte différents critères, qui peuvent inclure la nature des données traitées (publiques, sensibles, données concernant des personnes vulnérables, etc.)[1250], les attentes raisonnables de la personne concernée[1251] ou encore le pouvoir de négociation du responsable

---

[1244] V. Conseil de l'Europe, *Discrimination, intelligence artificielle, et décisions algorithmiques,* étude du Professeur Frederik ZUIDERVEEN BORGESIUS, Strasbourg, Publication de la Direction générale de la Démocratie, Conseil de l'Europe, 2018, 99 pages ; Commission européenne, COM (2020) 65 final, *op. cit.*, pp. 12-14.

[1245] À l'origine, au sein de la directive 95/46/CE, la version anglaise de l'article 7 (f) de la directive mentionnait les *« interests for fundamental rights and freedoms of the data subject* » (les intérêts pour les droits fondamentaux ou les libertés de la personne concernée). Or, lors des négociations dans d'autres langues (notamment le français, l'italien ou l'allemand), cette expression a été traduite dans le sens des intérêts ou des droits fondamentaux de la personne concernée. Lors de l'adoption du RGPD, le « ou » a été retenu et est désormais intégré à la version anglaise de l'article 6 (1) (f) : « *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, 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* ». Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 32.

[1246] *Idem,* p. 33.

[1247] CNIL, « L'intérêt légitime, comment fonder un traitement sur cette base légale ? », *CNIL.fr*, 2 décembre 2019, disponible sur https://www.cnil.fr/fr/les-bases-legales/interet-legitime (consulté en novembre 2021).

[1248] *Ibidem.*

[1249] Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 34.

[1250] Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 43-44 ; CNIL, « L'intérêt légitime,… », *op. cit.*

[1251] Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 44-45.

de traitement sur la personne concernée.[1252] Le responsable de traitement devra également mesurer l'importance de l'intérêt légitime sur un spectre échelonné de l'intérêt minime à l'intérêt impérieux[1253].

618. Le travail d'identification et de mesure effectué, le responsable de traitement devra déterminer si les intérêts et droits et libertés fondamentales de la personne concernée prévalent ou non sur les intérêts légitimes sur lesquels il souhaite fonder le traitement. Ainsi, si l'intérêt légitime du responsable de traitement est impérieux et que le traitement est une intrusion anodine dans les intérêts et droits de la personne concernée, il sera aisé de démontrer que la base légale de l'intérêt légitime peut servir à fonder le traitement. *A contrario*, la base légale de l'intérêt légitime ne sera pas valable s'il existe un intérêt légitime minime et que le traitement constitue une intrusion préoccupante dans les intérêts et droits de la personne concernée.

619. L'appréciation de la validité de la base légale de l'intérêt légitime procède donc d'un travail éminemment subjectif de mise en balance des intérêts par le responsable de traitement, qui pourra ensuite être vérifiée par l'autorité de contrôle ou la juridiction saisie en cas de conflit. Étant donné la nature très casuistique d'une telle appréciation, il n'est pas étonnant que la méthodologie proposée par le G29 reste très générale et ne doive sa précision qu'à une énumération d'exemples.[1254] La jurisprudence peut également être une source de précision. Par exemple, la CNIL a considéré que la société Monsanto pouvait, sur la base légale de l'intérêt légitime, détenir un « fichier contenant les données personnelles de plus de 200 personnalités politiques, ou appartenant à la société civile […] susceptibles d'influencer le débat ou l'opinion publique sur le renouvellement de l'autorisation du glyphosate en Europe »[1255]. Le Conseil d'État a également eu l'occasion de contrôler la mise en balance des intérêts effectuée par Cdiscount et en a déduit que la conservation du numéro de carte bancaire du client pour faciliter les achats ultérieurs ne pouvait pas être fondée sur l'intérêt légitime en raison de « la sensibilité de ces informations bancaires et des préjudices susceptibles de résulter pour [les clients] de leur

[1252] *Idem*, p. 45.
[1253] *Idem*, p. 34.
[1254] Ainsi, une offre promotionnelle d'une chaîne de pizzéria peut répondre à un intérêt légitime lorsque la collecte des données est limitée aux coordonnées de contact et à la consommation de pizzas (selon le couple intérêt non impérieux – ingérence faible), mais ne répond plus à ce même intérêt si elle utilise des traitements aux fins de publicité ciblée (selon le couple intérêt non impérieux – ingérence préoccupante). *Idem*, pp. 35-36.
[1255] CNIL, « Fichier de lobbying : sanction de 400 000 euros à l'encontre de la société MONSANTO », *CNIL.fr*, 28 juillet 2021, disponible sur https://www.cnil.fr/fr/fichier-de-lobbying-sanction-de-400-000-euros-lencontre-de-la-societe-monsanto (consulté en novembre 2021).

captation et d'une utilisation détournée », ainsi que l'absence d'une attente raisonnable des clients de voir leurs données bancaires conservées[1256].

620. L'approche très casuistique a d'ailleurs été explicitement rappelée par la Cour de Justice de l'Union européenne, qui considère que la mise en balance des intérêts « dépend, en principe, des circonstances concrètes du cas particulier concerné et dans le cadre de laquelle la personne ou l'institution qui effectue la pondération doit tenir compte de l'importance des droits de la personne concernée résultant des articles 7 et 9 de la Charte des droits fondamentaux »[1257]. Or, cette approche subjective et casuistique de la validité de la base légale des intérêts légitimes a fait également craindre la pratique d'une base légale « de convenance ».

§2 — Le risque d'une base légale « de convenance »

621. La méfiance envers le potentiel de contournement des instruments de protection des données à caractère personnel de la base légale de l'intérêt légitime n'est pas propre à la rédaction du RGPD. À titre d'exemple, sous l'égide de la directive 95/46/CE, l'Espagne n'avait ouvert la possibilité aux responsables de traitement de baser leurs traitements sur l'intérêt légitime que dans la situation où les données à caractère personnel provenaient de « sources accessibles au public », condition que la CJUE avait rejetée en 2011[1258]. Des restrictions plus sectorielles avaient aussi été mises en place par l'Allemagne[1259].

622. Lors des négociations aboutissant à l'adoption du RGPD, la base légale de l'intérêt légitime avait également fait l'objet de crainte de la part d'une partie des députés européens. Par conséquent, lors des négociations du Parlement européen sur le projet de Règlement proposé par la Commission européenne, le projet de rapport de la Commission LIBE avait proposé une série d'amendements du RGPD ayant pour objectif de restreindre à la fois le champ d'application de la base légale de l'intérêt légitime et l'insécurité juridique résultant de la mise en balance des intérêts[1260]. Le champ d'application de la base légale de l'intérêt légitime se trouvait notamment fortement limité par l'amendement 100 qui proposait l'application de cette base légale uniquement si aucune autre base juridique ne pouvait fonder le traitement à caractère

---

[1256] CE, 10e et 9e chambres réunies, 10 décembre 2020, n° 429571.
[1257] CJUE, 24 novembre 2011, *ASNEF et FECEMD c. Administración del Estado*, C-468/10 et C-469/10.
[1258] *Ibidem.*
[1259] CJUE, 19 octobre 2016, *Breyer*, C-582/14, §50-64.
[1260] Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures, *Projet de rapport 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)*, 16 janvier 2013, COM (2012) 0011 – C7-0025/2012, pp. 77-81.

personnel[1261]. L'amendement 875 proposait aussi une telle limitation, justifiée par une définition « intrinsèquement vague » des intérêts légitimes[1262]. L'amendement 879 proposait un champ d'application encore plus limité, puisqu'il prévoyait que la base légale de l'intérêt légitime ne pouvait « s'appliquer que de manière restrictive, dans la mesure où il est strictement nécessaire à la finalité de l'intérêt légitime et quand il n'existe aucun autre fondement juridique pour cette finalité spécifique »[1263]. Les amendements 101 et 102, quant à eux, avaient pour objectif d'assurer une certaine sécurité juridique aux responsables de traitements en leur offrant une liste de traitements dont les intérêts légitimes du responsable de traitement « prévalent en principe » sur les intérêts ou libertés et droits fondamentaux de la personne concernée et inversement[1264].

623. Cependant, à la suite de nombreuses critiques quant à la possibilité de délimiter de telles listes de traitements, le Parlement européen est revenu à une base légale non hiérarchisée et à une mise en balance casuistique des intérêts[1265]. Au plus, la méfiance du Parlement européen quant à la base légale de l'intérêt légitime pourrait se deviner au considérant 47 du RGPD qui appelle les responsables de traitement à la prudence lors du choix de la base légale de l'intérêt légitime, choix qui « devrait faire l'objet d'une évaluation attentive »[1266].

624. Les risques de base légale de convenance sont aussi exprimés dans les lignes directrices du G29 adoptées en 2014[1267]. Le G29 semblait déjà conscient des questions que soulevait « le caractère ouvert »[1268] de la base légale de l'intérêt légitime. Deux pratiques à risques sont alors identifiées dans les lignes directrices : la base légale de la « dernière chance » et la base légale de convenance. Le premier risque est lié à la pratique du responsable de traitement qui utiliserait la base légale des intérêts légitimes soit uniquement pour des « situations rares et imprévues », soit en « dernière chance si aucun autre motif ne s'applique »[1269]. Cette pratique est problématique, dans la mesure où elle inverse la logique de choix de la base légale du traitement. Plutôt que de rechercher si un traitement nécessaire à ses intérêts légitimes est

[1261] *Idem*, pp. 77-78.
[1262] *Idem*, amendement 875.
[1263] *Idem*, amendement 879.
[1264] *Idem*, pp. 79-81.
[1265] DE TERWANGNE Cécile, ROSIER Karen, *op. cit.*, §63.
[1266] RGPD, 27 avril 2016, article 47.
[1267] L'EDPB a commencé son travail de consultation dans l'objectif d'actualiser des lignes directrices sur l'intérêt légitime adoptées en 2014. EPDB, « EDPB Stakeholder Workshop on Legitimate Interest », edpb.europa.eu, 16 novembre 2020, disponible sur https://edpb.europa.eu/news/news/2020/edpb-stakeholder-workshop-legitimate-interest_en (consulté en novembre 2021).
[1268] Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 10.
[1269] *Ibidem.*

conforme aux conditions du RGPD, le responsable de traitement va rechercher en quoi le traitement peut remplir un intérêt légitime. Ce faisant, le responsable de traitement court-circuite la notion de « nécessité » étudiée dans le paragraphe précédent : il sera dès lors très probable que le traitement peine à respecter les principes de limitation des finalités et de minimisation des données. Le second risque est le risque inverse. Le responsable de traitement, considérant la base légale de l'intérêt légitime comme moins contraignante que les autres, considère celle-ci comme « une option privilégiée »[1270]. Cette pratique est également questionnable puisque, comme nous l'avons étudié précédemment, fonder un traitement de données à caractère personnel sur la base légale de l'intérêt légitime suppose « un examen attentif de la part de l'organisme et le suivi d'une méthodologie rigoureuse »[1271].

625. Ces deux risques sont analysés par certains auteurs comme constituant un « vide juridique » (*loophole*) dans le RGPD ou encore une possibilité de « contournement » (*bypass*) des règles européennes de protection des données[1272]. Plusieurs arguments peuvent en effet faire craindre une pratique de convenance, qui sont liés soit au contrôle effectué sur le responsable de traitement (A), soit à la tentation du responsable du traitement face à la flexibilité de la notion (B).

A. Le contrôle du responsable de traitement dans la mise en balance des intérêts

626. Le responsable de traitement peut se faire contrôler par l'autorité de contrôle ou par le juge. Il s'agit d'un contrôle classique, de nature juridictionnelle, durant lequel l'autorité de contrôle ou le juge vérifiera la conformité des traitements effectués par le responsable de traitement aux règles de protection des données à caractère personnel dans le cadre d'une décision.

627. Ce contrôle n'a désormais lieu qu*'a posteriori* dans la mesure où il n'existe pas de supervision du responsable de traitement dans la mise en balance des intérêts. En effet, la logique d'*accountability* du RGPD s'oppose à la logique de supervision *a priori* de la pertinence des bases légales choisies par le responsable de traitement pour fonder ses traitements de données à caractère personnel. Le RGPD s'inscrit au contraire dans une logique de

---

[1270] *Ibidem.*

[1271] CNIL, « L'intérêt légitime, comment fonder un traitement sur cette base légale ? », *CNIL.fr*, 2 décembre 2019, disponible sur https://www.cnil.fr/fr/les-bases-legales/interet-legitime (consulté en novembre 2021).

[1272] De tels écrits sont très présents dans le milieu professionnel. v. par exemple MADGE Robert, « Five Loopholes in the GDPR », *Medium.com*, 27 août 2017, disponible sur https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b (consulté en novembre 2021) ; S.S. Rana & Co, « Loopholes in the General Data Protection Regulation », *Lexology.com*, 4 juin 2018, https://www.lexology.com/library/detail.aspx?g=95a63603-1714-444f-be36-28e3006ac734 ;

responsabilisation, sonnant le glas de toute logique de contrôle *a priori* présente dans la directive 95/46/CE (et notamment aux déclarations préalables de traitement). Le responsable de traitement peut ainsi rapidement mettre en place un traitement sans formalités administratives, mais doit créer une documentation précise justifiant ses choix, étant donné que « le responsable de traitement doit être en mesure de démontrer la validité du recours à cette base légale »[1273].

628. Le responsable de traitement est donc contrôlé dans le cadre des missions de contrôle mises en place par les autorités pour vérifier la mise en conformité des traitements avec le RGPD. En France, la CNIL effectue différentes missions de contrôle d'origines différentes : les contrôles s'inscrivant dans le programme annuel des contrôles, les contrôles dit « initiatives » qui sont des contrôles liés à des thématiques d'actualité (par exemple, les traitements dans le cadre de la lutte contre le COVID-19, les contrôles des dispositifs de vidéo protection, les contrôles de mise en conformité des responsables de traitement ayant déjà fait l'objet d'une procédure de contrôle et enfin, les contrôles ayant pour origine les réclamations et les signalements[1274]. Ces derniers constituent la plus grande partie des contrôles effectués par la CNIL depuis la mise en œuvre du RGPD, puisqu'ils représentaient 40 % des contrôles en 2020[1275] et 43 % en 2019[1276], contre 22 % en 2018[1277] et 17 % en 2017[1278]. Les contrôles ayant pour source les réclamations et les signalements ont pour origine le mécontentement des personnes concernées ayant repéré un traitement illicite, ou soupçonnant un responsable de traitement de ne pas être conforme au RGPD. La capacité pour les personnes concernées d'effectuer un contrôle sur les traitements de données à caractère personnel qui les concernent est inextricablement liée à l'obligation de transparence du responsable de traitement.

629. Or, dans le cadre de la mise en balance effectuée par le responsable de traitement, la personne concernée n'est pas informée des motifs ayant poussé le responsable de traitement à considérer que la base légale de l'intérêt légitime s'applique dans le cadre du traitement. Pourtant, plusieurs amendements du Parlement européen avaient proposé d'insérer au sein du RGPD l'obligation pour le responsable de traitement de publier « les motifs qu'il a de croire

---

[1273] CNIL, « L'intérêt légitime… », *op. cit.*

[1274] CNIL, « Comment se passe un contrôle de la CNIL ? », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/comment-se-passe-un-controle-de-la-cnil (consulté en novembre 2021).

[1275] CNIL, *Rapport d'activité 2020*, Paris, La Documentation française, mai 2021, p. 94.

[1276] CNIL, *Rapport d'activité 2019*, Paris, La Documentation française, juin 2020, p. 91

[1277] CNIL, *Rapport d'activité 2018*, Paris, La Documentation française, 2019, p. 69.

[1278] CNIL, *Rapport d'activité 2017*, Paris, La Documentation française, 2018, p. 95.

que ses intérêts prévalent sur les intérêts ou les libertés et les droits fondamentaux de la personne concernée »[1279].

630. Cependant, il est important de remarquer ici que le responsable de traitement est tout de même soumis à l'obligation de transparence inscrite aux articles 13 et 14 du RGPD. La CNIL a notamment rappelé, à l'occasion de l'affaire Monsanto, que « la fourniture de ces informations permet l'exercice par la personne concernée de ses droits auprès du responsable de traitement »[1280], condamnant alors la société de ne pas avoir informé les personnes concernées par leur traitement fondé sur l'intérêt légitime, même si les données collectées étaient publiques[1281]. Une telle information est assurément indispensable à la mise en place du droit d'opposition. Inscrit à l'article 21 du RGPD, le droit d'opposition offre à la personne concernée la possibilité de « s'opposer à tout moment, pour des raisons à sa situation particulière, à un traitement des données à caractère personnel la concernant ». En matière de prospection (y compris au moyen de profilage), la personne concernée dispose de la possibilité de « s'opposer à tout moment » au traitement, ce qui lui offre un mécanisme d'*opt-out* sur les traitements de données à caractère personnel basé sur l'intérêt légitime en matière de prospection.

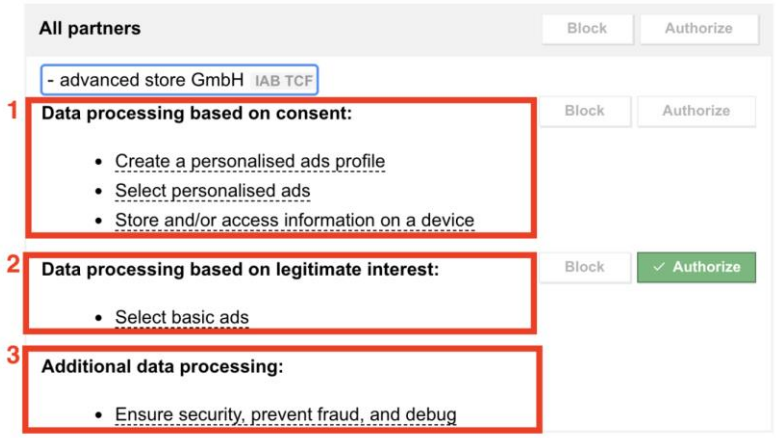

Figure 4 - Bannière de cookies ayant un mécanisme d'opt out pour les traitements fondés sur l'intérêt légitime[1282]

631. Pour l'ensemble des autres traitements fondés sur l'intérêt légitime, il semble que le droit d'opposition ait été substantiellement renforcé par le RGPD. L'article 21 (1) dispose que

---

[1279] Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures, COM(2012)0011 – C7-0025/2012, *op. cit.*, Amendement 100, Amendement 875.
[1280] CNIL, Délibération de la formation restreinte n°SAN-2012-012 du 26 juillet 2021 concernant la société MONSANTO COMPANY, §79
[1281] *Idem*, §85.
[1282] DIDOMI, « Some cookies are dropped on my website before consent », disponible sur https://support.didomi.io/some-cookies-are-dropped-on-my-website-before-consent

« le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou par la constatation, l'exercice ou la défense de droits en justice ». Le RGPD inverse la charge de la preuve concernant l'exercice du droit d'opposition. Quand la directive 95/46/CE exigeait de la personne concernée la démonstration de « raisons prépondérantes et légitimes tenant à sa situation particulière »[1283], le RGPD exige du responsable de traitement la démonstration de « motifs légitimes et impérieux »[1284]. De plus, cet inversement de la charge de la preuve inverse également le standard d'évaluation du droit d'opposition. Désormais, l'élément de référence n'est plus l'impact de l'exercice du droit d'opposition sur les motifs légitimes du responsable de traitement (référence largement héritée de la logique de marché intérieur), dont des raisons prépondérantes et légitimes de la personne concernée constitueraient l'exception à la règle. Depuis le RGPD, les intérêts et les droits fondamentaux de la personne concernée constituent le standard à protéger, que seuls « des motifs légitimes et impérieux » pourront dépasser.

632. La notion de « motifs légitimes et impérieux » permet de restreindre les exceptions à la possibilité pour le responsable de traitement de continuer le traitement de données à caractère personnel. Sous le régime de la directive 95/46/CE, le droit d'opposition ne paraissait pas avoir beaucoup d'effet sur le responsable de traitement. Le G29 lui-même considérait alors le droit d'opposition comme « une possibilité *supplémentaire* de marquer son opposition, pour des motifs liés à sa situation particulière »[1285] et invitait les responsables de traitement à « proposer une option de refus qui serait plus large, et qui n'exigerait aucune démonstration supplémentaire d'un intérêt légitime (prépondérant ou autre) de la part de la personne concernée »[1286]. L'article 21 du RGPD a partiellement répondu à cette invitation puisque le responsable de traitement est tenu de cesser le traitement de données à caractère personnel si la personne concernée exerce son droit d'opposition, à moins qu'il ne démontre la présence de « motifs légitimes et impérieux »[1287]. Le terme « impérieux » avait déjà été utilisé dans les lignes directrices du G29 pour qualifier les intérêts légitimes les plus importants du spectre[1288]. Ainsi, il ne suffit pas pour un intérêt légitime d'être manifeste pour être impérieux, le G29 distinguant

[1283] Directive 95/46/CE, 24 octobre 1995, article 14 (a) ; Groupe de travail « Article 29 », WP 217, *op. cit.,* p. 50.
[1284] RGPD, 27 avril 2016, article 21 (1).
[1285] Groupe de travail « Article 29 », WP 217, *op. cit.* p. 50.
[1286] *Ibidem.*
[1287] RGPD, 27 avril 2016, article 21 (1).
[1288] Groupe de travail « Article 29 », WP 217, *op. cit.*, p. 34.

ces termes[1289]. Les exemples d'intérêt impérieux fournis par le G29 donnent un indice de l'importance que doit revêtir l'intérêt légitime pour être considéré comme impérieux : le G29 cite en effet des intérêts qui seraient « profitables à la société en général, comme l'intérêt de la presse à publier des informations sur des faits de corruption dans l'administration ou l'intérêt d'effectuer des recherches scientifiques (sous réserve de garanties appropriées) »[1290]. Le caractère strict de l'interprétation de la notion de motif impérieux est renforcé par son caractère d'exception dans la mesure où, en vertu de l'adage *exception est strictissimae interpretationis* (l'exception est d'interprétation stricte), l'inversement du standard d'évaluation peut être interprété comme une traduction de la volonté du législateur de privilégier les droits fondamentaux de la personne concernée. Il n'est dès lors pas déraisonnable de considérer que le droit d'opposition ne pourra pas être limité par des considérations uniquement économiques.

633. L'absence de contrôle de la mise en balance de l'intérêt légitime semble donc, en théorie, contrebalancée par la possibilité pour la personne concernée d'exercer son droit d'opposition au travers d'un mécanisme d'*opt-out*. Néanmoins, il ressort de la pratique que les responsables de traitement sont tentés de privilégier la base légale de l'intérêt légitime en raison de sa flexibilité, ce qui aboutit à des situations rendant plus poreuse la protection des données à caractère personnel.

B. Une flexibilité tentante

634. L'intérêt légitime peut apparaître pour le responsable de traitement comme une base légale privilégiée du fait de sa flexibilité. Cette flexibilité est perçue comme d'autant plus avantageuse depuis que le RGPD a renforcé les conditions relatives à la validité du consentement. Il n'est dès lors pas étonnant que depuis l'adoption du RGPD, de nombreux articles comparant les deux bases légales aient été publiés en direction des professionnels[1291]. La lecture de ces articles est intéressante puisqu'elle permet de sonder à la fois l'enthousiasme des responsables de traitement face à une base légale suffisamment flexible pour répondre à

[1289] *Idem,* p. 39.

[1290] *Idem,* p. 27.

[1291] V. par exemple : Le Journal du Net, « Le consentement aux données est-il vraiment nécessaire », *JournalduNet.com*, 14 septembre 2018, disponible sur https://www.journaldunet.com/solutions/cloud-computing/1211333-le-consentement-aux-donnees-est-il-vraiment-necessaire/ (consulté en novembre 2021) ; Desmarais Avocats, « RGPD : le consentement n'est pas systématique », *Desmarais-Avocats.fr*, disponible sur https://www.desmarais-avocats.fr/rgpd-le-consentement-nest-pas-systematique/ (consulté en novembre 2021) ; Convert, « Consent vs. Legitimate Interest: Which Should You Choose for Marketing? », *Convert.com,* 5 juin 2019, disponible sur https://www.convert.com/blog/privacy/consent-vs-legitimate-interest/ (consulté en novembre 2021) ; Proviti, « GDPR: Legitimate Interest vs. Consent », *Blog.proviti.com*, 6 juin 2018, disponible sur https://blog.protiviti.com/2018/07/06/gdpr-legitimate-interest-vs-consent/ (consulté en novembre 2021).

leurs besoins et l'appréhension de ces mêmes responsables de traitement face à une base légale dont les contours sont difficiles à cerner. Ainsi, comme le remarquent Elena Fil González et Paul de Hert, « le concept d'intérêt légitime est peut-être l'un des concepts les plus confus de la protection des données à caractère personnel, aimé et détesté dans une égale mesure »[1292].

635. Le principe d'*accountability* qui irrigue le RGPD, dont l'entrée en vigueur ne date que de mai 2018, rend difficile une étude de l'impact de la flexibilité de la base légale de l'intérêt légitime sur la protection des données à caractère personnel, et en particulier de son articulation avec le consentement. Cependant, deux indices du caractère séduisant de la base légale de l'intérêt légitime seront ici analysés : la différence de périmètre entre le consentement et l'intérêt légitime et la multiplication problématique des bases légales sur lesquelles sont fondés les traitements.

636. Si les bases légales décrites à l'article 6 (1) du RGPD n'ont aucune hiérarchie entre elles, cela ne signifie pas que ces bases légales puissent être utilisées pour les mêmes traitements. Cette affirmation est évidente pour les bases légales dont le périmètre est déjà limité par défaut à l'existence d'une condition « extérieure » au traitement, comme le traitement nécessaire à l'exécution d'un contrat [article 6 (1) [b]], le traitement nécessaire au respect d'une obligation légale [article 6 (1) [c]], le traitement nécessaire à la sauvegarde des intérêts vitaux de la personne concernée [article 6 (1) [d]] ou encore, le traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement [article 6 (1) [e]]. En effet, c'est l'existence d'un contrat, d'une obligation légale, d'une situation mettant en danger la vie de la personne concernée ou d'une mission d'intérêt public qui conditionne le recours à la base légale concernée. Le consentement et l'intérêt légitime sont également des bases légales soumises à des conditions, mais ces conditions sont plus intrinsèques au traitement. Ainsi, le consentement est approprié quand le responsable de traitement est en mesure de respecter l'ensemble des conditions de validité du traitement. L'intérêt légitime est, quant à lui, approprié lorsque le responsable de traitement est en mesure de démontrer un intérêt légitime qui prévaut sur les intérêts, libertés et droits fondamentaux de la personne concernée.

637. Ainsi, une première limite à l'intérêt légitime est le domaine réservé du consentement. L'intérêt légitime ne peut pas être utilisé par le responsable de traitement comme fondement si

[1292] « The concept of a «legitimate interest' may be among the mest confusing in the data protection framework, loved, and loathed in equal measure » [traduction libre]. GIL GONZÁLEZ Elena, DE HERT Paul, « Understanding the legal provisions that allow processing and profiling of personal data – an analysis of GDPR provisions and principles », *ERA Forum*, Springer, 2019, p. 603.

les textes requièrent comme base légale le consentement. C'est notamment ce que la CNIL a rappelé dans sa décision à l'encontre de la société Nestor SAS en date du 8 décembre 2020. En l'espèce, la société Nestor soutenait que « la base légale du traitement ayant pour finalité la prospection commerciale des personnes, effectué sur leur adresse électronique personnelle est l'intérêt légitime du responsable de traitement », dans la mesure où il était « vital […] d'acquérir une base de clients professionnels potentiels » dans le domaine de la livraison de déjeuner d'affaires[1293]. Or, comme la CNIL le remarque dans sa délibération, la prospection commerciale relève de l'article L.34-5 du Code des postes et des communications électroniques, qui dispose :

> « Est interdite la prospection directe au moyen de système automatisé de communications électroniques […], d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen ».

Dès lors, la prospection commerciale ne peut relever que de la base légale du consentement, excluant de fait la possibilité de recourir à l'intérêt légitime du responsable de traitement. La même solution a été adoptée par l'autorité de contrôle de Berlin, qui a condamné la société eBay à ce titre. L'autorité de contrôle allemande précise alors que si la notion d'intérêt légitime peut être interprétée de manière large, l'intérêt légitime ne peut être présumé lorsque le traitement de données à caractère personnel viole d'autres normes juridiques[1294].

638. Le champ d'application du consentement et de l'intérêt légitime paraît à première vue plus large que celui des autres bases légales. Il existe d'ailleurs de nombreuses situations dans lesquelles les deux bases légales peuvent fonder le même traitement de données à caractère personnel. Dans le cas où le responsable de traitement peut fonder une même finalité d'un même traitement sur plusieurs bases légales, la CNIL rappelle à plusieurs reprises que le responsable de traitement doit choisir la base légale la plus appropriée à cette finalité[1295]. Cette interprétation restrictive de l'article 6 par la CNIL et le G29 se justifie tout à fait en matière de consentement dont les conditions de validité et la possibilité de retrait le rendent incompatible avec une autre base légale[1296]. Toutefois, dans la pratique, plusieurs bannières de consentement aux cookies

---

[1293] CNIL, SAN-2020-018, 8 décembre 2020, *op. cit.*

[1294] Berliner Beauftrage für Datenschutz und Informationsfreheit (BlnBDI), 15 octobre 2021, décision 521.13874.13 (en allemand) ; résumé en anglais disponible sur GDPRHub : https://gdprhub.eu/index.php?title=BlnBDI_(Berlin)_-_521.13874 (consulté en décembre 2021).

[1295] V. par exemple CNIL, « La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD », *CNIL.fr*, 2 décembre 2019, disponible sur https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales (consulté en décembre 2021) ; CNIL, Délibération n°2020-046 du 24 avril 2020, *op. cit.*

[1296] LÉONARD Thierry, « Yves, si tu exploitais tes données ? », *in* DE TERWANGNE Cécile *et al.* (dir.), *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde*, 1re édition, Bruxelles, Larcier, 2018, p. 662

ne respectent pas ce principe, préférant fonder le traitement sur les deux bases légales. Le juriste imagine alors aisément le motif du responsable de traitement. En effet, le consentement relevant d'un mécanisme d'*opt-in* et l'intérêt légitime d'un mécanise d'*opt-out*, le responsable de traitement prend moins de risques de voir le traitement de données proposé refusé par la personne concernée[1297].

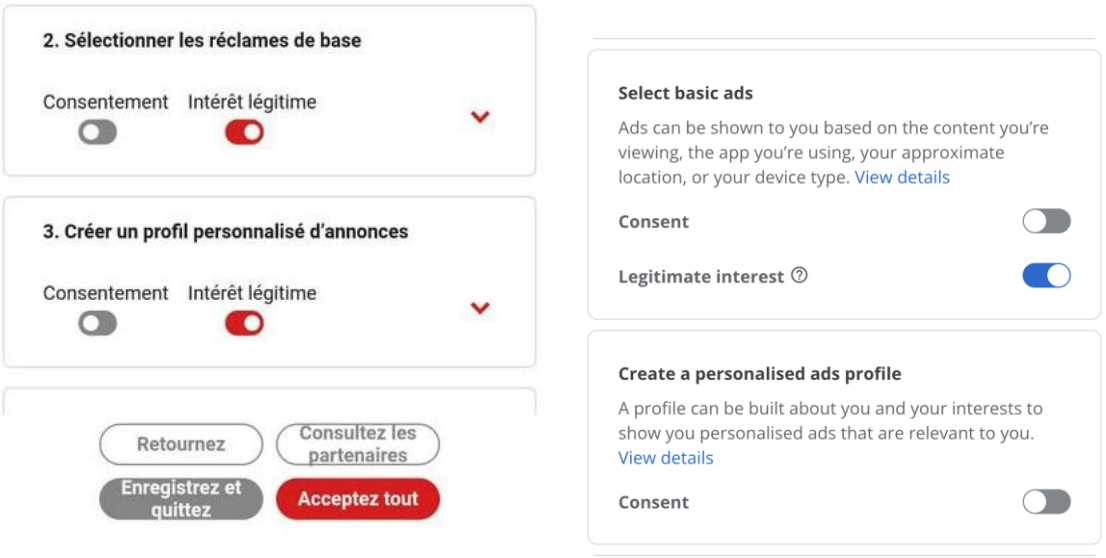

Figure 5 — Bannière de cookies de fancypantshomes et wordreference

639. Cette pratique est pourtant problématique. Dans le cas où la personne concernée accepte de donner son consentement, le traitement est fondé sur plusieurs bases légales qui ne répondent pas au même régime. D'une part, lorsqu'un traitement est fondé sur le consentement, la personne concernée dispose du droit de retirer son consentement à tout moment, ce qui entraîne automatiquement l'effacement de ces données[1298]. D'autre part, quand un traitement est fondé sur les intérêts légitimes du responsable de traitement, la personne dispose d'un droit d'opposition, que le responsable de traitement devra respecter « à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et les libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice »[1299]. Seul le cas du traitement de données à caractère personnel à des fins de prospection commerciale entraîne automatiquement la fin du traitement de données à

[1297] De nombreuses études démontrent que le mécanisme d'*opt out* résulte en un taux d'engagement plus important que le mécanisme d'*opt in*. Par exemple, en matière de donation d'organes, le taux d'engagement dans les pays ayant mis en place un mécanisme d'*opt out* est supérieur de 25 à 30 % à celui des pays ayant mis en place un mécanisme d'*opt in*. CIVANER Murat, ALPINAR Zümrüt, ÖRS Yaman, « Why Would Opt-Out System for Organ Procurement Be Fairer ? », *Synthesis Philosophica*, 2010, n°2, p. 371.
[1298] RGPD, 27 avril 2016, Article 7 (1), Article 17 (1) (b).
[1299] RGPD, 27 avril 2016, Article 21 (1).

caractère personnel[1300]. Ainsi, dans le cas où la personne concernée retire son consentement, le responsable de traitement pourra toujours théoriquement continuer à traiter ses données à caractère personnel sur la base des intérêts légitimes, annihilant les effets du retrait du consentement. En se comportant ainsi, le responsable de traitement contourne les conditions de validité du consentement, et conduit la personne concernée dans l'erreur de penser que le consentement constitue la base légale du traitement. Le G29 avait pourtant bel et bien identifié ce risque dans ses lignes directrices relatives au consentement dans le RGPD, et appelait les responsables de traitement à respecter le choix des personnes concernées lorsque le traitement est fondé sur le consentement :

> « Il est important de noter que si un responsable de traitement choisit de se fonder sur le traitement pour une partie du traitement, il doit être prêt à respecter ce choix et à interrompre le traitement si un individu retire son consentement. Indiquer que les données seront traitées sur la base du consentement, alors que le traitement se fonde sur une autre base juridique, serait fondamentalement déloyal envers les personnes concernées »[1301].

Dès lors, si, dans l'hypothèse d'un retrait de consentement, le responsable de traitement continue à traiter les données à caractère personnel des personnes concernées sur la base légale de l'intérêt légitime, la base légale du consentement est factice et ne constitue pas une base légale valide au sens de l'article 6 (1) (a) du RGPD. De plus, le responsable de traitement ne respecte pas les principes de loyauté et de transparence[1302] : la personne concernée va être informée d'une base légale factice qui ne lui permettra pas d'exercer facilement ses droits, ce qui est contraire à l'esprit du RGPD.

640. Enfin, il est surprenant de constater que certains responsables de traitement fondent leur traitement de données à caractère personnel relatif à la publicité ciblée sur la base des intérêts légitimes[1303]. En effet, il ne semble pas que le caractère très intrusif d'un tel traitement puisse

---

[1300] RGPD, 27 avril 2016, Article 21 (2) et Article 21 (3).
[1301] Groupe de travail « Article 29 », WP259 rév. 01, *op. cit.*, p. 27.
[1302] RGPD, article 5 (1) (a).
[1303] L'exemple de Tik Tok illustre la volonté de certains acteurs de court-circuiter le consentement à travers la base légale des intérêts légitimes. L'entreprise chinoise a en effet annoncé fonder désormais ses services de publicité comportementale sur la base de ses intérêts légitimes et de ceux de ses partenaires, plutôt que sur le consentement. L'autorité de contrôle italienne (la Garante per la protezione dei dati personali) a quelques jours plus tard adopté une décision en urgence, prévenant TikTok qu'il s'agissait d'une pratique allant à l'encontre de la lecture conjointe du RGPD et de la directive *ePrivacy*. TikTok a depuis annoncé suspendu la mise à jour de sa politique de confidentialité. v. Le Monde, « Tiktok change ses conditions d'utilisation au mépris du consentement de ses utilisateurs », *LeMonde*.fr, 9 juin 2022, disponible sur https://www.lemonde.fr/pixels/article/2022/06/09/tiktok-change-ses-conditions-d-utilisation-au-mepris-du-consentement-de-ses-utilisateurs_6129594_4408996.html (consulté en août 2022) ; GPDP, « Tik Tok : Italian SA warns against « personalised » ads based on legitimate interest », 12 juillet 2022, disponible sur https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9788342#english (consulté en août 2022) ; Le Figaro, « TikTok suspend une mise à jour imposant

être suffisamment contrebalancé par l'existence d'un intérêt légitime du responsable de traitement, fusse-t-il considéré comme impérieux (par exemple, le financement exclusif d'un service par la publicité comportementale). Le G29 avait été très clair sur la nécessité d'obtenir un consentement dans le cadre d'un traitement de données de publicité comportementale, invoquant à la fois le caractère très intrusif du traitement et la directive *e-privacy,* qui crée, à la charge du responsable de traitement, l'obligation d'obtenir le consentement pour le dépôt de cookies dans l'équipement terminal de l'utilisateur[1304]. De plus, si ces arguments ne parvenaient pas à convaincre le responsable de traitement de l'illicéité d'un tel traitement, force est de constater que l'utilisation de la base légale de l'intérêt légitime pour fonder un traitement ayant pour finalité la publicité ciblée est illicite au regard de l'article 9 du RGPD. La précision de plus en plus accrue des techniques de publicité comportementale permet au responsable de traitement de déduire des données sensibles concernant la personne concernée, telles que ses opinions politiques, son orientation sexuelle ou encore son état de santé[1305]. Or, ces données sont protégées par l'article 9 du RGPD qui restreint les bases légales sur lesquelles peuvent être fondés les traitements de ces données : un traitement de données sensibles ne peut pas être fondé sur la base de l'intérêt légitime[1306].

641. La tentation de fonder le traitement sur la base de l'intérêt légitime, plutôt que sur la base du consentement, se révèle dans l'attitude des responsables de traitement de vouloir utiliser la base légale de l'intérêt légitime dans des domaines réservés au consentement ou en plus du consentement, afin de bénéficier d'une sécurité juridique plus grande. Cependant, s'il ne semble pas pour l'instant exister de jurisprudence sur le sujet du cumul des bases juridiques du consentement et de l'intérêt légitime, le texte et l'esprit du RGPD, ainsi que les différentes interprétations proposées par les autorités de contrôle paraissent s'opposer à une telle pratique. Il sera intéressant de suivre l'évolution des contrôles et des jurisprudences relatifs à la base légale de l'intérêt légitime, afin de déterminer si les craintes de court-circuit du consentement relèvent d'une pratique illicite minoritaire ou d'une pratique réellement diffuse, profitant de l'absence de contrôle *a priori* des traitements fondés sur l'intérêt légitime du responsable de traitement.

---

la publicité ciblée en Europe », *LeFigaro.fr*, 12 juillet 2022, disponible sur https://www.lefigaro.fr/flash-eco/tiktok-suspend-une-mise-a-jour-imposant-la-publicite-ciblee-en-europe-20220712 (consulté en août 2022).

[1304] Groupe de travail « Article 29 », WP 217, *op. cit.*, pp. 51-52.

[1305] V. par exemple CNIL, « Publicité ciblée en ligne : quels enjeux pour la protection des données personnelles ? », *CNIL.fr*, 14 janvier 2020, disponible sur https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles (consulté en décembre 2021).

[1306] RGPD, 27 avril 2016, Article 9 (1).

642. Conclusion de Section. — La confusion des bases légales de l'intérêt légitime et du consentement est principalement motivée par des intérêts d'ordre économique et par la création par le législateur d'une base légale presque « fourre-tout », permettant aux responsables de traitement de fonder de nombreux traitements sur la base d'une balance, réalisée par le responsable de traitement, de ses intérêts et des intérêts, libertés et droits des personnes concernées. L'intérêt légitime relevant uniquement d'un contrôle *a priori* en raison de la logique d'*accountability* qui traverse le RGPD, il n'est pas étonnant de constater que les responsables de traitement souhaitent se fonder sur cette base juridique très flexible plutôt que sur la base du consentement, dont les conditions de validité sont rigides et la durée de validité incertaine. Une clarification du régime de l'intérêt légitime par le législateur ou par la Cour de Justice de l'Union européenne permettrait ainsi de tracer une frontière plus nette en ce qui concerne le domaine réservé du consentement, et les domaines dans lesquels le responsable de traitement est fondé à utiliser la base légale de l'intérêt légitime.

Conclusion du Chapitre 2

643. La base légale du consentement contient fondamentalement le risque, pour le responsable de traitement, du refus ou du retrait du consentement de la personne concernée. Dès lors, le consentement subit la concurrence de bases légales perçues comme moins risquées et moins conditionnées à la seule volonté expresse de la personne concernée, telles que la base légale du contrat ou celle des intérêts légitimes du responsable de traitement. Si certaines de ces interprétations relèvent tout simplement d'une pratique illicite et contraire au RGPD, d'autres sont présentées comme une interprétation possible du RGPD par ses adeptes, voire comme une interprétation nécessaire pour que le RGPD s'applique de manière satisfaisante aux réalités du marché des données à caractère personnel, à l'image de la question de la publicité comportementale. L'interprétation proposée par les autorités de contrôle et la Cour de Justice de l'Union européenne, ainsi que les évolutions législatives attendues (comme le règlement *e-privacy*) seront des éléments de réponse qui permettront soit de consolider encore la force du consentement RGPD, soit de tracer plus nettement la ligne qui sépare l'autonomie personnelle des intérêts du marché.

Conclusion du Titre 1

644. Le consentement RGPD est une notion complexe qui s'accommode difficilement avec certaines pratiques des responsables de traitement et certaines dispositions mêmes du RGPD. Ces notions d'ombre et d'hésitation fragilisent le consentement de la personne concernée dans des contextes pourtant omniprésents sur le marché des données à caractère personnel, tels que les transferts de données à caractère personnel, l'intelligence artificielle ou encore la publicité comportementale. Que le consentement soit demandé dans un contexte ne permettant pas à la personne concernée d'exercer un choix réel et informé ou qu'il soit évité dans des situations où le traitement est si intrusif que le législateur ait préféré le fonder sur le consentement, la personne concernée se trouve dans l'incapacité d'exercer correctement son droit à la protection des données à caractère personnel. Néanmoins, cette conclusion ne peut être que provisoire, tant les jurisprudences à venir ainsi que les textes législatifs en discussion (Règlement *e-privacy*, règlement sur l'intelligence artificielle ou même le *Digital Service Act* et le *Digital Market Act*) apporteront très certainement des réponses à ces différentes pratiques, légitimant certaines, excluant d'autres.

645. Les questions concernant le consentement ne se limitent pas à la question de l'adéquation ou non de la base légale du consentement à certains traitements. En effet, même dans des contextes où le consentement est demandé de manière adéquate avec la nature du traitement de données à caractère personnel, des questionnements persistent quant à la possibilité pour la personne concernée d'exercer un consentement libre et éclairé.

TITRE 2 — UNE PROTECTION DÉCONNECTÉE DU CONTEXTE DE LA PERSONNE CONCERNÉE

646. Le consentement permet à la personne concernée de contrôler l'utilisation de ses données à caractère personnel par les responsables de traitement. Il s'agit de la traduction, en matière de protection des données à caractère personnel, de la doctrine de l'*empowerment*, qui a pour vocation de recentrer l'individu au centre des décisions qui le concernent. Dans le RGPD, la prise de décision est conçue comme un comportement rationnel et raisonnable : suffisamment libre et informée, la personne concernée prend les décisions qui sont les meilleures pour elle. Cette conception est classique en matière économique, traversée par le paradigme de l'*homo oeconomicus* « présumé capable de faire des choix optimaux en s'appuyant sur un calcul approprié »[1307]. La rationalité a aussi eu une place importante dans le domaine de la philosophie, à travers l'influence d'Aristote, Descartes ou encore Kant[1308]. En droit, le raisonnable constitue « un standard d'appréciation des comportements »[1309], à l'image de la réforme du Code civil préférant à la figure du bon père de famille l'importation du standard anglo-américain de la personne raisonnable[1310].

647. La personne raisonnable est définie dans le langage courant comme la personne « dont la pensée, le comportement, les choix sont guidés par la raison, la sagesse, la mesure ; qui sait rester maître de ses impulsions, de ses passions, de son imagination »[1311]. Le standard de la rationalité présuppose la capacité du sujet de se détacher de ses passions, voire conditionne certains effets de droit à celle-ci. Or, le standard de la rationalité est aujourd'hui rejeté par une partie de la doctrine, à l'image des nouvelles disciplines de l'économie comportementale ou de l'analyse comportementale du droit[1312]. L'objectivisation des méthodes d'interprétation par le standard de la personne raisonnable a notamment été critiquée comme une limite à l'autonomie de la volonté[1313].

[1307] LAGUEUX Maurice, *op. cit.*, p. 143.
[1308] DEMEULANAERE Pierre, *Les normes sociales. Entre accords et désaccords*, Presses Universitaires de France, 2003, p. 65.
[1309] JOLY Laurène, « Handicap – L'obligation de fournir un aménagement raisonnable », *Répertoire de droit du travail*, §117.
[1310] HUET Jérôme, « Adieu bon père de famille », *D.*, 2014, p. 505.
[1311] CNRTL, « Raisonnable », *CNRTL.fr*, Lexicographie, disponible sur https://www.cnrtl.fr/definition/raisonnable (consulté en décembre 2021).
[1312] AUDIT Pierre-Emmanuel, « De quelques enseignements de l'analyse comportementale du droit en matière d'information du contractant », *RTD civ., 2021,* p. 545.
[1313] MARTIAL-BRAZ Nathalie, *op. cit.*

648. L'étude du consentement ne peut dès lors pas se passer de l'étude de la situation de la personne concernée au moment de l'expression de son consentement. Il s'agit moins de se positionner sur le débat de l'adéquation du standard du raisonnable dans le système juridique que d'étudier les « conditions par lesquelles un milieu de vie soutient la capacité à consentir ou au contraire la tronque, substituant parfois à l'adhésion du sujet qu'il suscite, des formalisations ou des recommandations qui, mine de rien, lissent le caractère abrasif de ce milieu pour en faire un monde où le consentement s'étiole, n'étant plus qu'une formalité »[1314]. Le Titre propose ainsi de s'intéresser à deux limites du caractère raisonnable du comportement de la personne concernée.

649. La première limite s'intéresse à la personne concernée elle-même. Octroyer à la personne concernée le contrôle de ses données à caractère personnel n'est pas dépourvu de conséquences quant à l'effort qu'elle doit fournir, notamment en termes d'information et de compréhension des risques. Si cet effort peut paraître *a priori* raisonnable, en est-il réellement sur un univers caractérisé par la multiplicité de ses acteurs, le caractère immédiat des interactions ou encore l'interconnexion des traitements de données de plus en plus présents sur le marché numérique ? Le premier chapitre de ce titre s'efforcera de répondre à ces questionnements dans la mesure où le RGPD demande en pratique aux personnes concernées de fournir un effort excessif afin de protéger correctement leurs données à caractère personnel (Chapitre 1).

650. La seconde limite s'intéresse à la situation dans laquelle la personne concernée se trouve. En effet, le RGPD présuppose le caractère raisonnable du comportement de la personne concernée dans un contexte d'une relation horizontale, voire d'égal à égal, avec le responsable de traitement. Or, la dimension économique des données à caractère personnel tend à relativiser toute horizontalité de la relation entre la personne concernée et le responsable de traitement : sur le marché numérique, l'asymétrie de pouvoir entre la personne concernée et le responsable de traitement tend à remettre en question la possibilité pour les personnes concernées d'émettre un consentement valide au regard de la liberté de choix prônée par le Règlement (Chapitre 2).

[1314] PIERRON Jean-Philippe, « Le chemin trouble du consentement. Du consentement formel au consentement existentiel », *Les cahiers de la justice*, 2021, p. 563.

CHAPITRE 1 – L'EFFORT EXCESSIF DEMANDÉ À LA PERSONNE CONCERNÉE

651. La personne concernée est limitée par ses propres capacités : capacité de compréhension, de prise de recul, de gestion de l'information, capacités financières ou encore de gestion de son temps. Ces capacités sont prises en compte par le législateur[1315] afin d'équiper la personne concernée de l'ensemble des « armes » nécessaires à l'émission d'un consentement valide : facilité à consentir et à refuser, fourniture des informations nécessaires à un consentement éclairé, facilité de retrait du consentement, etc. Or, si ces garanties sont nécessaires, elles ne semblent pas pour autant suffisantes.

652. En effet, l'obligation de transparence a pour conséquence de fournir de nombreuses informations à la personne concernée afin qu'elle puisse consentir en toute connaissance de cause. Cependant, cette obligation s'adapte mal à la multiplicité des acteurs numériques et des traitements de données à caractère personnel mis en place, d'autant plus que certains responsables de traitement ont mis en place des stratégies d'influence du choix de la personne concernée. Dès lors, « même lorsqu'elles ont officiellement reçu une forme ou l'autre de "notification" et qu'elles ont eu l'occasion de "consentir" aux conditions générales, les personnes se retrouvent souvent dans un système conçu pour maximiser la monétisation des données à caractère personnel, sans leur laisser vraiment ni le choix ni une possibilité de contrôle »[1316]. Ce phénomène a pour conséquence de limiter la capacité des personnes concernées à s'informer et à comprendre les informations délivrées, créant le besoin d'une simplification de l'information (Section 1).

653. De plus, la personne concernée est confrontée à la multiplication des demandes de consentement, notamment lors de sa navigation sur internet. Or, la répétition de la tâche de consentir peut rapidement être ressentie comme un fardeau : il ne faut pas oublier que l'objectif premier de la personne concernée est d'accéder à un contenu sur internet. La protection des données à caractère personnel doit donc être perçue par la personne concernée non pas comme un obstacle, mais comme un véritable droit, ce qui nécessite une simplification de l'exercice du consentement (Section 2).

[1315] V. *supra* Partie 1.

[1316] EDPS, *Avis 9/2016 sur les systèmes de gestion des informations personnelles. Vers une plus grande autonomie des utilisateurs dans la gestion et le traitement des données à caractère personnel*, 20 octobre 2016, p. 6.

Section 1 — La simplification nécessaire de l'information

654. Il a été vu précédemment que le législateur s'efforce de protéger la compréhension, par la personne concernée, de l'information délivrée par le responsable de traitement.

Pourtant, le déséquilibre cognitif n'est pas absent des discours politiques. De l'aveu même de la présidente de la Commission européenne, Ursula Von Der Leyen, « chaque fois que nous sommes sur un site web et que nous sommes invités à créer une nouvelle identité numérique ou que nous nous connectons par l'intermédiaire d'une grande plateforme, nous n'avons, en réalité, aucune idée de ce que deviennent nos données »[1317]. Au niveau national, Annie Blandin, membre du Conseil national du numérique, s'inquiète de « l'emprise remarquable », du « contrôle » du système cognitif des internautes par les plateformes numériques, qui peut aller « jusqu'à la création d'addictions, comme le décrit fort bien la théorie de l'attention »[1318]. Or, ce déséquilibre cognitif entraîne des répercussions importantes sur la protection des données à caractère personnel. Juste avant sa nomination au poste de commissaire européen chargé de la politique industrielle, du marché intérieur, du numérique, de la défense et de l'espace, Thierry Breton déclarait au Sénat que, la mise en œuvre du RGPD étant « quelque peu détournée par les utilisateurs qui acceptent d'accéder aux services, sans prendre le temps de lire les conditions générales d'utilisation […], on se donne certes bonne conscience, mais au final, nos données partent n'importe où et ce, avec notre consentement ! »[1319]

655. Si les conséquences de cette asymétrie conduisent à se demander si le consentement peut raisonnablement être donné librement, ses causes sont diverses et peuvent être classifiées en deux catégories : l'asymétrie cognitive intentionnelle et l'asymétrie cognitive non intentionnelle. Nous désignons par asymétrie cognitive intentionnelle l'attitude du responsable de traitement cherchant à manipuler la personne concernée en exploitant ses biais cognitifs afin de lui « arracher » son consentement. Ces pratiques, appelées *dark patterns* sont certes interdites par le texte du RGPD, mais restent difficiles à identifier (§1). L'asymétrie cognitive non intentionnelle, quant à elle, relève de la difficulté à concilier l'exhaustivité de l'information avec la simplicité de sa compréhension. Cette conciliation est rendue d'autant plus ardue du fait des nombreuses demandes de consentement dans un environnement demandant une prise de

---

[1317] VON DER LEYEN Ursula, « Ce qui est interdit dans le monde réel doit être aussi interdit en ligne », *Le Figaro*, 29 janvier 2021, disponible sur https://www.lefigaro.fr/vox/monde/ursula-von-der-leyen-ce-qui-est-interdit-dans-le-monde-reel-doit-etre-aussi-interdit-en-ligne-20210129 (consulté en avril 2021).
[1318] Sénat, *Rapport fait au nom de la commission d'enquête sur la souveraineté numérique,* 1er octobre 2019, Session ordinaire, disponible sur https://www.senat.fr/rap/r19-007-2/r19-007-2.html (consulté en avril 2021).
[1319] *Ibidem.*

décision rapide, ce qui nécessite un travail de simplification de l'information par la labellisation (§2).

§1 — La lutte contre les dark patterns

656. Selon les lignes directrices du G29 sur le consentement, « toute pression ou influence inappropriée exercée sur la personne concernée (pouvant se manifester de différentes façons) l'empêchant d'exercer sa volonté rendra le consentement non valable »[1320]. L'emploi de l'adjectif « inappropriée » est révélateur de la tolérance de l'influence sur la question du consentement. C'est cette tolérance qui sera questionnée : à partir de quel degré d'influence peut-on s'interroger sur la validité du consentement ? (A).

657. À la suite de ce travail, nous nous interrogerons sur les formes d'influence du consentement qui nous paraissent être les plus problématiques vis-à-vis du consentement. Qu'elles soient tout à fait légales, profitent d'une absence de régulation ou flirtent avec l'illégalité, il sera démontré que leur existence peut neutraliser l'effet protecteur du RGPD au profit des plateformes numériques (B).

A. Les limites du consentement : à la recherche de la définition de « l'influence inappropriée »

658. La multiplication des techniques d'influence omniprésentes dans le milieu numérique et notamment sur internet a conduit à une réflexion sur le fondement même du consentement. Nombreux sont les ouvrages, articles, billets alarmistes sur la question du consentement : notre libre arbitre n'existerait plus, internet exerçant désormais le rôle traditionnellement accordé à Dieu[1321], il serait « aspiré par internet »[1322]. Le nouvel environnement numérique, par ses nombreux stimuli de l'internaute, interroge ainsi sur les notions classiques de libre arbitre, de liberté et d'autonomie de la volonté, de consentement. Nous ne prétendrons pas ici trouver la solution au « problème fondamental de l'éthique »[1323] : notre objectif est plus modestement de questionner l'adéquation du consentement dans le milieu numérique.

659. Comme il l'a été vu précédemment, le consentement, en matière de protection des données à caractère personnel, a été renforcé par l'adoption du RGPD dont l'objectif est

---

[1320] Groupe de travail « Article 29 », WP259 rév. 01, *op. cit.*, p. 6.
[1321] REMACLE Julien, *Et internet recréa Dieu : Notre libre arbitre n'existe plus*, Rinfini, 2014, 188 p.
[1322] AMIECH Matthieu, « Groupe Marcuse : Notre libre arbitre est aspiré par Internet », *Marianne*, 19 août 2019, disponible sur https://www.marianne.net/agora/entretiens-debats/groupe-marcuse-notre-libre-arbitre-est-aspire-par-internet (consulté en avril 2021).
[1323] OSIER Étienne, *Préface in* SCHOPENHAUER Arthur, *Sur la liberté de la volonté*, Hermann, 2011, Traduit de l'allemand par OSIER Étienne, p. 6.

notamment de faire correspondre au mieux la volonté et le consentement. Or, lorsque cet objectif n'est pas rempli, « le recours au consentement en matière de protection des données personnelles ne constitue pas nécessairement un renforcement des droits des personnes »[1324]. La nécessité de l'adéquation du consentement et de la volonté en matière de protection des données à caractère personnel est reliée à l'évolution du droit à la vie privée : la personne concernée, décrite comme ayant un pouvoir unilatéral de choisir le degré d'exposition de son intimité quand désormais, les traitements de données à caractère personnel s'inscrivent dans une relation bilatérale dans laquelle la personne concernée et le responsable de traitement cherchent à protéger leurs intérêts[1325].

660. En garantissant que le consentement soit l'expression de la volonté de la personne concernée, le RGPD entend garantir la liberté de la personne concernée face aux plateformes numériques. Or, l'influence exercée par ces plateformes, qui se définit par « l'action (généralement graduelle et imperceptible) qui s'exerce sur les dispositions psychiques, sur la volonté de telle personne »[1326], questionne la liberté réelle des personnes concernées. Dans la mesure où « ce qui fait peur dans le fait d'être influencé, c'est de perdre sa liberté »[1327], l'influence semble être un point de friction avec la notion du consentement qui s'entoure « de principes politiques avérés, la liberté, la liberté de choisir, la liberté offerte par notre droit »[1328].

661. Toute influence n'invalide cependant pas le consentement. Dans un cas contraire, il n'aurait pas été possible d'ériger le consentement comme le principe irrigant notre droit, symbole de l'émancipation de la personne, de la liberté et de l'égalité entre les individus. Il y a des influences jugées positives. Ainsi, l'influence n'est pas forcément antinomique de la volonté puisqu'une influence peut également être « volontairement subie », ou encore désigner le « pouvoir reconnu ou conféré »[1329]. De plus, l'influence est indissociable de la nature sociale de l'homme, de sa capacité et de son besoin de communiquer. Selon Alex Mucchielli, « toute parole est tentative d'influence d'autrui »[1330]. L'influence est aussi un métier : un « nouveau »

[1324] DEBAETS Émilie, *op. cit.*, p. 346.
[1325] US Department of Health, Education & Welfare, «Records Computers and the Rights of Citizens», *Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, 1973, p. 48, disponible sur https://www.justice.gov/opcl/docs/rec-com-rights.pdf (consulté en avril 2021).
[1326] CNRTL, « Influence », *Lexicographie*, disponible sur https://www.cnrtl.fr/definition/influence (consulté en avril 2021).
[1327] DE SAINT-MAURICE Thibault, « Être influençable, est-ce vraiment grave ? », *La Petite Philo*, France Inter, 21 mars 2019, disponible sur https://www.franceinter.fr/emissions/la-petite-philo/la-petite-philo-21-mars-2019 (consulté en avril 2021).
[1328] FRAISSE Genevève, *op. cit.*, p. 14.
[1329] CNRTL, « Influence », *Lexicographie*, disponible sur https://www.cnrtl.fr/definition/influence (consulté en avril 2021).
[1330] MUCCHIELLI Alex, *L'art d'influencer*, Paris, 2009, p. 7.

métier à travers l'influenceur dont le métier s'exerce sur les réseaux sociaux, un métier « traditionnel » à travers le lobbying (ou « influençage »[1331]), dont le métier s'exerce à destination des pouvoirs publics ou encore la publicité. Dès lors, il est indispensable de déterminer les limites de l'influence « acceptable » et de l'influence « inacceptable ». À partir de quel degré l'influence devient-elle inacceptable au point de mettre en danger notre liberté ? L'influence étant une action, la réflexion se portera, dans un premier temps, sur la nature de cette action (1), avant de porter, dans un second temps, sur son objet (2).

1. L'influence appropriée par l'action

662. L'influence peut être inappropriée, car elle limite notre liberté, la liberté de notre volonté, et donc notre capacité à donner un consentement valide. La question de la liberté a été abondamment traitée en philosophie. En tant que juriste, il ne s'agit pas de déterminer quelle conception de la liberté nous semble la plus juste, mais plutôt quelle conception nous semble reçue dans le droit positif. Ainsi il s'agit de déterminer ce que la liberté est et n'est pas en droit, pour ensuite déterminer les frontières acceptables et inacceptables de l'autonomie de la volonté, source du consentement.

663. Intéressons-nous tout d'abord à la distinction proposée par Isaiah Berlin entre le sens positif et le sens négatif de la liberté. La liberté positive se définit par une adéquation parfaite entre la volonté propre de l'individu et les décisions de ce dernier :

> « Le sens "positif" du mot liberté découle du désir d'un individu d'être son propre maître. Je souhaite que ma vie et mes décisions dépendent de moi, et non de forces extérieures quelles qu'elles soient. Je désire être l'instrument de ma propre volonté et non celui de la volonté et non celui de la volonté des autres ; je désire être un sujet et non un objet ; être mû par des raisons et des mobiles conscients qui soient les miens, et non par des causes pour ainsi dire extérieures »[1332].

La liberté négative se définirait quant à elle comme la capacité d'agir indépendamment de l'intervention des autres :

> « Je suis libre, dit-on généralement, dans la mesure où personne ne vient gêner mon action […]. La contrainte implique l'intervention délibérée d'autrui dans l'espace à l'intérieur duquel je pourrais normalement agir »[1333].

[1331] RIVAL Madina, « Vers un lobbying éthique ? Ou comment pratiquer l'influence sans corruption », *Entreprise éthique,* Association Francophone de Comptabilité, 2006, n° 24, p. 20.
[1332] BERLIN Isahia, *Éloge de la liberté,* Calmann-Lévy, 1994, p. 179.
[1333] *Idem,* p. 171.

664. Il est évident que la conception de la liberté positive ne peut pas être retenue en droit. Le sens positif de la liberté relève ici de l'intime, de ce qui ne peut être sondé que par l'individu lui-même. Le droit n'a les moyens ni de contrôler ni de protéger cette liberté. De plus, le droit est une cause extérieure : les règles de droit limitent la liberté de l'individu, même s'il y a consenti directement (manifestation de la volonté individuelle) ou indirectement (manifestation de la volonté collective). Par ailleurs, cette conception ne permettrait pas l'exercice des professions fondées sur l'influence, et notamment de la publicité, très présente sur l'environnement numérique[1334]. Par exemple, la directive 2005/29/CE du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs admet les pratiques publicitaires « qui peuvent légitimement influencer la perception d'un produit par le consommateur ainsi que son comportement, sans altérer son aptitude à prendre une décision en connaissance de cause »[1335].

665. La notion de la liberté négative semble quant à elle correspondre à la philosophie de notre droit positif. On retrouve dans les vices du consentement la volonté de non-ingérence d'un contractant sur l'autre à travers le dol et la violence. L'influence inappropriée serait une ingérence dont le motif est de gêner l'action de la personne concernée, en la conduisant à exercer son consentement du fait de la tromperie, de la ruse ou de la contrainte. Dans une perspective kantienne, seule la manœuvre frauduleuse peut rendre l'influence appropriée, l'homme ayant le pouvoir de se défaire de sa paresse et de sa lâcheté afin de sortir de sa minorité :

> « La *minorité* consiste dans l'incapacité où il est de se servir de son intelligence sans être dirigé par autrui. Il doit *s'imputer à lui-même* cette minorité, quand elle n'a pas pour cause le manque d'intelligence, mais l'absence de la résolution et du courage nécessaires pour user de son esprit sans être guidé par un autre. *Saper aude*, aie le courage de te servir de ta *propre* intelligence ! »[1336].

666. Ainsi, l'influence semble être licite pour autant que la personne concernée ait les moyens de s'en défaire par un effort raisonnable, à la portée du « consommateur moyen ». La directive

---

[1334] Sur l'influence de la publicité sur internet, v. FOURQUET-COURBET Marie-Pierre, « Influence attendue et influence effective de la publicité sur l'internet. Des représentations sociales des producteurs aux modèles scientifiques », *Question de communication*, 2005, n° 5, pp. 31-53.

[1335] Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/550/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) no 2006/2004 du Parlement européen et du Conseil (« directive sur les pratiques commerciales déloyales »), Considérant 6.

[1336] KANT Emmanuel, *Éléments métaphysiques de la doctrine du droit (Première partie de la Métaphysique des mœurs suivis d'un essai philosophique sur la paix perpétuelle et d'autres petits écrits relatifs au droit naturel*, traduit de l'allemand par BARNI Jules, Paris, Auguste Durand, 1853, p. 281

sur les pratiques commerciales déloyales n'interdit que les « pratiques qui altèrent de manière significative la liberté du choix du consommateur », dont les pratiques incluant « une influence injustifiée »[1337] qui se définit comme « l'utilisation d'une position de force vis-à-vis du consommateur de manière à faire pression sur celui-ci, même sans avoir recours à la force physique ou menacer de le faire, de telle manière que son aptitude à prendre une décision en connaissance de cause soit limitée de manière significative »[1338]. Si l'influence injustifiée est difficile à définir, on peut y voir « un écho à l'infraction de manipulation mentale »[1339] en ce qu'elle fausse le jugement de la personne concernée, s'opposant au postulat de liberté posé par notre droit positif[1340]. L'influence injustifiée présuppose à la fois une manœuvre frauduleuse et un degré d'influence capable d'altérer le consentement du consommateur moyen, c'est-à-dire du « consommateur raisonnablement attentif et avisé »[1341].

667. Par analogie, l'influence inappropriée serait une influence exercée sur la personne concernée qui n'altère pas de manière indépassable le consentement de la personne concernée raisonnable ou ne constitue pas une manœuvre frauduleuse du responsable de traitement ayant pour fin de forcer le consentement de la personne concernée. Ainsi, l'influence ne doit pas s'exercer de manière à empêcher la personne concernée d'opter pour un choix alternatif[1342]. Nous adhérons à la thèse de Yashar Saghai selon laquelle « l'influence ne préserve pas suffisamment la liberté de choix si nous ne sommes pas capables de lui résister facilement »[1343]. La capacité de résister se manifeste notamment par la capacité d'être conscient de l'influence exercée ou encore la capacité d'inhiber le désir né de l'influence exercée[1344].

668. Il nous semble en effet que le fait pour la personne concernée de pouvoir résister facilement à l'influence exercée sur elle est dans la continuité des recommandations de la CNIL concernant les cookies, pour qui « refuser les traceurs doit être aussi simple que de les accepter »[1345]. L'exemple donné par l'autorité de contrôle française est d'ailleurs très révélateur

---

[1337] Directive 2005/29/CE, 11 mai 2005, Considérant 16.
[1338] *Idem*, Article 2 (k).
[1339] AMBROISE-CASTELOT Coralie, « Les nouvelles pratiques commerciales déloyales après la loi LME du 4 août 2008 », *AJ Pénal*, 2009, n° 1, p. 22.
[1340] BELLIVIER Florence, « Guillaume-Xavier BOURIN, *Contribution à l'étude du délit de manipulation mentale préjudiciable* », *RTD civ.*, 2005, p. 206.
[1341] STUYCK Jules, *Fasc. 2000 : Politique européenne de la consommation*, JurisClasseur Europe Traité, 14 avril 2020, § 3.
[1342] VUGTS Anastasia *et al.*, «How autonomy is understood in discussions on the ethics of nudging», *Behavioural Public Policy*, 2008, Volume 4, Issue 1, p. 116.
[1343] SAGHAI Yashar, «Salvaging the concept of nudge», *Journal of Medical Ethics*, 2013, n° 39, p. 488.
[1344] *Idem*, p. 489.
[1345] CNIL, « Nouvelles règles pour les cookies et autres traceurs : bilan de l'accompagnement de la CNIL et actions à venir », 2 avril 2021, disponible sur https://www.cnil.fr/fr/nouvelles-regles-cookies-et-autres-traceurs-bilan-accompagnement-cnil-actions-a-venir (consulté en mai 2021).

de la nécessité de limiter l'influence exercée sur la personne concernée à une influence à laquelle elle peut facilement résister :

> « La seule présence d'un bouton "Paramétrer" en complément du bouton "Tout accepter" tend, en pratique, à dissuader le refus et ne permet donc pas de se mettre en conformité avec les exigences posées par le RGPD »[1346].

669. Ainsi, nous avons déterminé ce que pouvait recouvrir l'action d'influence « appropriée » dans les lignes directrices de l'EDPB. Il s'agit désormais de se demander si l'influence peut également être appropriée dans son objectif, ce que nous appellerons par la suite « l'influence éthique ».

2. L'influence éthique ?

670. L'éthique « implique une appréciation concernant le bien et le mal des actions »[1347] : l'influence appropriée par l'éthique supposerait alors de légitimer l'influence que le responsable de traitement aurait sur le consentement de la personne concernée lorsque le but de cette influence serait considéré comme étant « le bien ». Le débat qui oppose traditionnellement libéraux et paternalistes a notamment ressurgi depuis la théorie du paternalisme libéral tel que développé par Cass Sustein et Richard Thaler (prix Nobel d'économie de 2017). La théorie du paternalisme libéral considère que l'influence est justifiée dès lors que l'influence pousse l'agent à choisir la meilleure action pour ses propres intérêts et est suffisamment faible pour ne pas restreindre sa liberté[1348].

671. Les partisans du paternalisme ne se réclament pas de la théorie de l'individu raisonnable sur le plan économique. En matière de protection des données à caractère personnel, cela implique le rejet du « pragmatique de la vie privée » (« *privacy pragmatist* ») qui, selon la théorie d'Alan Westin, désigne les agents qui, « tournés vers l'avenir, maximisent l'utilité et fondent leur décision sur le partage de leurs données sur leurs préférences en matière de confidentialité »[1349]. Il semble donc y avoir une contradiction entre le libéralisme, qui promeut l'autonomie de la volonté, la liberté de choix et le paternalisme dont les partisans sont réticents à l'idée d'une liberté de choix illimitée[1350]. Ces derniers affirment, à l'instar de Robert Goodin,

---

[1346] *Ibidem.*
[1347] HADOT Pierre, LAUGIER Sandra, DAVIDSON Arnold, « Qu'est-ce que l'éthique ? », *Cités*, 2001/1, n° 5, p. 129.
[1348] ARNESON Richard J., «Nudge and Shove», *Social Theory and Practice*, Vol. 41, N° 4, 2016, p. 668.
[1349] WALDMAN Ari Ezra, «Cognitive biases, dark patterns, and the "privacy paradox"«, *Current Opinion in Psychology*, Volume 31, 2020, p. 105.
[1350] SUSTEIN Cass R., THALER Richard H., «Libertarian Paternalism is Not an Oxymoron», *The University of Chicago Law Review*, 2003, n° 70(4), p. 1160.

qu'il est possible pour une autorité publique de mieux respecter les propres préférences d'un individu que l'aurait fait un individu lui-même à travers ses propres actions[1351]. Les libéraux se fonderaient sur le postulat erroné selon lequel un agent prend toujours des décisions dans leur meilleur intérêt[1352]. Le paternalisme asymétrique et le paternalisme libéral se présentent comme une solution pour combler les effets de l'irrationalité de l'agent économique, qui résulte notamment de l'acrasie (la faiblesse de la volonté). L'acrasie (du grec ancien ἀκράτεια puis ἀκρασία[1353]) est un concept philosophique notamment développé par les philosophes de l'antiquité grecque, et souvent illustré par les dires attribués par Ovide au personnage de Médée,

> « Je vois des actes meilleurs, je les approuve, et pourtant je fais ceux qui sont moins bons »[1354].

672. Néanmoins, l'acrasie ne fait pas l'unanimité chez les philosophes. Le philosophe moraliste R.M. Hare considère qu'il est profondément illogique de vouloir faire quelque chose et de faire autre chose[1355]. Déniant toute faiblesse de volonté ou acrasie, il lie toute situation apparente d'acrasie à une situation d'incapacité (telle Médée, incapable de faire l'acte meilleur, car dépassée par la colère[1356]) ou à une situation d'hypocrisie (l'agent n'évalue pas réellement l'action comme meilleure, même s'il le dit)[1357]. Selon lui, séparer l'action du jugement évaluatif de l'agent n'est pas acceptable dans la mesure où cette séparation conduit à la « perte de la rationalité humaine », aussi appelée « externalisme extrême »[1358]. De même, Platon considère que l'acrasie, si elle existe, est de la responsabilité de l'agent. C'est par sa propre ignorance que l'agent choisit l'action qui lui est la moins favorable, il est responsable de son propre préjudice :

[1351] GOODIN Robert E., «Permissible Paternalism: In Defense of the Nanny State», *Responsive Community*, 1991, n° 42, p. 44.

[1352] SUSTEIN Cass, THALER Richard, , «Libertarian Paternalism», *The American Economic Review*, Vol. 93, No. 2, Papers and Proceedings of the One Hundred Fifteenth Annual Meeting of the American Economic Association, Washington, DC, January 3–5, 2003, p. 175.

[1353] Le terme ἀκρασία signifie en grec ancien « intempérie », et se confond, à partir du IVe siècle, avec le terme ἀκράτεια qui désigne l'impuissance à se gouverner ou à se maîtriser. V. LOAYZA Daniel, « Dionysos au ventre. Notre sur le châtiment du vin dans Le Cyclope d'Euripide », *Odysseum — ministère de l'Éducation nationale et de la Jeunesse,* 25 octobre 2019, disponible sur https://eduscol.education.fr/odysseum/dionysos-au-ventre (consulté en août 2022) ; BOQUER Antoine, GEORGES Benjamin, Application Bailly disponible sur https://bailly.app/ (consulté en août 2022).

[1354] Ovide, Métamorphoses, VII, 20-2, trad. Lafaye G., Paris, Gallimard, 1992, p. 220.

[1355] KUBARA Michael, «Acrasia, Human Agency and Normative Psychology», *Canadian Journal of Philosophy*, octobre 1975, vol. 5, No. 2, p. 223.

[1356] FERREIRA Anthony, « Addiction et faiblesse de la volonté », 2019, Institut de Recherches Philosophiques, Université Paris Nanterre, disponible sur https://chaire-philo.fr/wp-content/uploads/2019/11/Addiction-et-faiblesse-de-la-volont%C3%A9.pdf (consulté en mai 2021).

[1357] STROUD Sarah, SVIRSKY Larisa, « Weakness of Will », Stanford Encyclopedia of Philosophy, publié le 14 mai 2008, révisé le 4 septembre 2019, disponible sur https://plato.stanford.edu/entries/weakness-will/ (consulté en mai 2021).

[1358] FERREIRA Anthony, « Addiction et faiblesse de la volonté », 2019, Institut de Recherches Philosophiques, Université Paris Nanterre, disponible sur https://chaire-philo.fr/wp-content/uploads/2019/11/Addiction-et-faiblesse-de-la-volont%C3%A9.pdf (consulté en mai 2021).

> « Si donc l'agréable est bon, l'homme qui sait ou qui s'imagine qu'une autre action est meilleure que celle qu'il accomplit, et possible, renonce alors à ce qu'il fait là, puisqu'il peut faire mieux : céder à soi-même n'est rien d'autre qu'ignorance tandis que se dominer est sagesse »[1359].

673. Ainsi, le droit doit placer le curseur entre la protection de la personne (par exemple, l'obligation de porter une ceinture de sécurité) et le respect de l'autonomie de sa volonté. La question de l'objectif de l'influence a alors une importance primordiale puisque seront rejetées les influences « ayant des buts illégitimes » ou les influences poussant l'agent à choisir une option qui paraît en contradiction avec les intérêts et valeurs de la majorité des agents[1360]. Une autre limite de l'influence éthique semble se trouver dans le concept de « paternalisme asymétrique » tel que développé par Colin Camerer *et al*. : l'influence doit « créer de larges bénéfices pour ceux qui font des erreurs, tout en imposant peu ou pas de conséquence sur les individus totalement rationnels »[1361]. Une telle philosophie semble avoir guidé la rédaction de l'article 25 du RGPD sur la protection des données par défaut. En mettant à la charge du responsable de traitement l'obligation de minimiser les données à caractère personnel collectées par défaut, le législateur européen veut influencer la personne concernée à protéger ses données à caractère personnel. En effet, la protection maximale de données à caractère personnel sera l'option la plus simple à choisir pour la personne concernée.

674. Le législateur peut-il aller plus loin que l'article 25 du RGPD ? L'équipe de chercheurs d'Alessandro Acquisti a tenté de définir dans quelle mesure l'influence exercée sur la personne concernée pouvait être éthique[1362]. Cependant, ces derniers constatent la difficulté de transposer le paternalisme asymétrique à l'environnement numérique. En effet, l'équipe refuse l'approche « trop simpliste » considérant que la meilleure action se situe dans l'exposition minimale de la vie privée et la sécurisation maximale des données des individus[1363]. Selon eux, non seulement l'action est difficile à évaluer en termes de bien et de mal en raison de coûts d'exposition « intangibles ou difficiles à mesurer », mais l'agent doit aussi prendre en compte le fait qu'augmenter ses risques relatifs à la protection de sa vie privée résulte aussi en « des gains économiques, sociaux ou personnels »[1364] : dès lors, l'approche simpliste aurait également des conséquences négatives sur l'agent. Partant, est-il possible d'exercer une influence éthique sur

---

[1359] Platon, *Protagoras,* 358 b 3-5, trad. Trédé M. Demont P., Paris, Poche, 1993, p. 143.
[1360] SUSTEIN Cass R., « Do People Like Nudges? », *Administrative Law Review,* Vol. 68, n° 2, p. 195.
[1361] CAMERER Colin *et. al.,* «Regulation for Conservatives: Behavioral Economics and the Case for "Asymetric Paternalism"«, *University of Pennsylvania Law Review*, 2003, Vol. 151, p. 1211.
[1362] ACQUISTI Alessandro *et al.,* «Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online», *ACM Computing Surveys*, Vol. 50, 2017, n° 3, article 44.
[1363] *Idem,* p. 44:28.
[1364] *Ibidem.*

le choix de la personne concernée de donner ou de refuser de donner son consentement au traitement de ses données à caractère personnel ? L'équipe d'Alessandro Acquisti propose deux objectifs éthiques : minimiser le regret et aligner le comportement de l'agent avec des préférences que l'agent aurait exprimées[1365]. Le premier objectif vise à minimiser les risques qui peuvent être évalués comme les plus importants par l'agent, puisqu'il s'agit de comportements qui seraient très probablement regrettés dans le futur : l'article donne l'exemple d'une exposition décidée « sous influence de l'alcool ou de drogues », de l'utilisation d'un langage inapproprié et vulgaire, ou encore de l'exposition d'opinion sur des « questions politiques controversées »[1366].

675. Une autre analyse, développée par Eoin Carolan et Alessandro Spina, considère que l'approche de l'autonomie de la volonté telle que développée par le droit européen de la protection des données à caractère personnel était pertinente aux débuts d'internet, mais pas à l'ère du *big data* et des algorithmes[1367]. L'inadéquation du consentement avec l'environnement numérique actuel est liée à l'imprévisibilité des conséquences de l'exposition des données à caractère personnel des personnes concernées : « une exposition limitée à certains peut facilement, et de manière imprévisible, devenir une information intéressant tout le monde l'an prochain »[1368]. Par exemple, la tendance générale des personnes concernées à faire plus attention au partage de données considérées comme pouvant les stigmatiser ou les embarrasser (par exemple le poids ou l'âge[1369]) ne semble plus correspondre à la réalité des risques actuels en matière de protection des données à caractère personnel. De plus, la conséquence du consentement au traitement de données à caractère personnel est difficile à prévoir du fait que, comme le rappelle l'arrêt *Digital Rights Ireland*,

> « Ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci »[1370].

[1365] *Idem*, 44:29.
[1366] *Ibidem.*
[1367] CAROLAN Eoin, SPINA Alessandro, «Behavioural Sciences and EU Data Protection Law: Challenges and Opportunities», *in* ALEMANNO Alberto, SIBONY Anne-Lise (dir.), *Nudge and the Law: A European Perspective*, Oxford, Hart Publishing, 2015, p. 169.
[1368] *Ibidem.*
[1369] HUBERMAN Bernado A. « Valuating Privacy », *IEEE Security & Privacy*, 2005, pp. 22-25.
[1370] CJUE, Gde ch., 8 avril 2014, *Digital Rights Ireland Ltd*, C-293/12, § 27.

Enfin, selon les deux auteurs, le consentement est biaisé par les « externalités de nos choix » : dans le contexte numérique, aucun choix ne serait neutre[1371]. Par exemple, une personne ne s'inscrivant pas sur Facebook peut également être profilée comme une personne « timide, isolée socialement, ou manquant de compétences techniques »[1372]. Ainsi, fonder les traitements de données à caractère personnel sur le consentement aurait un effet contre-productif quant à l'autonomie des personnes concernées puisque ces dernières ne peuvent pas anticiper les conséquences de leurs actions. Dès lors, influencer les personnes concernées à protéger de manière plus importante leurs données à caractère personnel permettrait à celles-ci de mieux contrôler leurs données. Une telle approche permettrait de protéger la personne concernée à la fois avec les objectifs annoncés par le RGPD[1373] et avec les valeurs de la majorité des Européens[1374].

676. Si l'influence éthique semble séduire une partie de la doctrine, majoritairement anglo-saxonne[1375], l'influence exercée sur le consentement de la personne concernée doit tout de même être limitée, en ce qu'elle s'oppose à l'autonomie de sa volonté et à sa liberté. Preuve en est, la CNIL considère que le consentement libre signifie que « le consentement ne doit pas être contraint ni influencé »[1376]. L'influence considérée comme éthique présente de plus des difficultés puisqu'elle nécessite un jugement de valeur quant à des intérêts légitimes et contradictoires qui sont la protection des données à caractère personnel et la protection de la liberté d'entreprendre. Elle impliquerait dès lors un jugement au cas par cas qui ne serait pas envisageable dans l'environnement numérique. Ainsi, après avoir étudié les fondements théoriques permettant de définir qu'une influence est acceptable, nous nous intéresserons à la question de l'influence dans la pratique de l'environnement numérique.

[1371] CAROLAN Eoin, SPINA Alessandro, *op. cit.*, p. 172.
[1372] *Ibidem.*
[1373] RGPD, 27 avril 2016, Considérant 7.
[1374] 67 % des européens se disaient concernés de ne pas avoir un contrôle total sur les informations qu'ils fournissent en ligne. Commission européenne : *Special Eurobarometer 431: Data Protection*, 2015, question 5, disponible sur https://data.europa.eu/data/datasets/s2075_83_1_431_eng?locale=fr (consulté en mai 2021).
[1375] On notera ici que la doctrine française a une vision très négative du paternalisme : le paternalisme est un « mal », « éloigné de l'égalité républicaine » (MUCHIELLI Julien, « Achat de votes à Corbeil : "On n'a jamais vu en France une ville livrée à un tel degré de corruption" », *Dalloz actualité*, 3 novembre 2020) ; le paternalisme est dangereux (BATIFOULIER Philippe, « Développer le marché de l'assurance pour le "bien" du patient : les dangers d'un paternalisme marchand », *RDSS*, 2019, p. 819) ; il est un « fléau » (MOULY Jean, « Vie privée des salariés handicapés et information du comité d'entreprise : contresens sur l'article 8 de la Convention européenne des droits de l'homme », *D.*, 2005, p. 469.).
[1376] CNIL, « Conformité RGPD : Comment recueillir le consentement des personnes ? », 3 août 2018, disponible sur https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes (consulté en mai 2021).

B. Les dark patterns

677. Le laboratoire d'innovation de la CNIL s'est longuement penché sur la question des *dark patterns* et s'est proposé d'étudier les interfaces numériques au-delà de leur aspect ergonomique, s'intéressant aux enjeux « en termes de capacité à agir et de configuration des possibilités de choix »[1377]. Les *dark patterns* sont un procédé volontaire, ayant pour objectif « de faire en sorte que le *design*, l'ergonomie des services en lignes créent chez l'utilisateur des biais cognitifs, c'est-à-dire des pensées illogiques, irrationnelles, générées par le contexte dans lequel est immergé l'utilisateur »[1378]. L'utilisation de tels procédés nécessite une réflexion sur la manière de les réguler : à partir de quel moment un design franchit-il la frontière entre la simple influence et la manipulation ? Comment le régulateur peut-il détecter et démontrer le caractère trompeur ou manipulateur d'une interface, d'un design ?[1379].

678. La nécessité de réguler de telles interfaces est liée à la fois aux notions juridiques de consentement et de traitement loyal. La loyauté s'oppose à la volonté malicieuse de manipuler le consentement de la personne concernée. Nous traiterons ici uniquement la question du consentement. Une première piste de réponse se trouve dans le cahier IP6 du laboratoire d'innovation de la CNIL qui considère que « le design abusif ou trompeur […] des services numériques peut engendrer divers troubles au consentement, d'une nature suffisamment objective et démontrable pour qu'il entraîne sa validité »[1380] et lie de tels comportements à la notion d'influence inappropriée de l'EDPB.

679. Le laboratoire LINC définit le design abusif comme un design utilisant « les limites et les biais cognitifs des individus pour les amener à effectuer des actions sur lesquels ils n'ont pas de contrôle »[1381]. Le témoignage de Tristan Harris, ancien « *design ethicist* » de Google, fournit un point de vue intéressant, à travers la métaphore du magicien. Ainsi comme le magicien, le *designer* va chercher les « angles morts », les vulnérabilités et les limites de la perception de la personne concernée, « afin de pouvoir l'influencer sans qu'elle ne le réalise »[1382]. La personne concernée aura l'impression d'exercer un consentement valable, de

---

[1377] LINC, « La forme des choix. Données personnelles, design et frictions désirables », *Cahiers IP Innovation & Prospective*, n° 6, p. 7.
[1378] GROFFE-CHARRIER, « La loi est-elle dictée par le code ? », *Dalloz IP/IT*, 2020, p. 602.
[1379] HARY Estelle, « Dark patterns: quelle grille de lecture pour les réguler ? », 2 septembre 2019, disponible sur https://linc.cnil.fr/dark-patterns-quelle-grille-de-lecture-pour-les-reguler (consulté en mai 2021).
[1380] LINC, *op. cit.*, p. 40.
[1381] *Idem*, p. 27.
[1382] HARRIS Tristan, « How Technology is Hijacking Your Mind – from a Magician and Google Design Ethicist », *Medium*, disponible sur https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3 (consulté en mai 2021).

choisir librement, tout en ignorant que ses choix sont manipulés par l'élaboration et le design du menu, de telle façon que le designer « gagnera » toujours, peu importe le choix de la personne concernée[1383]. Le design va ainsi entraîner des conséquences sur la personne concernée, notamment en affaiblissant la validité du consentement. Il s'agira notamment des paramètres par défaut qui exposent la personne concernée (désormais interdits par l'article 25 du RGPD), de la difficulté d'accès des paramètres les plus protecteurs des données à caractère personnel, ou encore de l'utilisation d'un langage jouant sur l'émotion de la personne concernée pour la dissuader de protéger ses données à caractère personnel[1384].

680. Une première piste de distinction entre l'influence appropriée et le *dark pattern* est la notion d'influence éthique étudiée précédemment. Selon l'agence norvégienne de protection des consommateurs, la différence entre le « *nudging* » comme promu par le Nobel de l'économie Richard Thaler et les *dark patterns* est l'objectif de l'influence[1385]. Le « *nudging* », issu de travaux dans le domaine de l'économie comportementale, désigne les méthodes de manipulation douce en vue d'inciter les individus à adopter de meilleurs comportements[1386]. Si l'influence a pour objet de bénéficier au responsable de traitement et non à la personne concernée, il s'agira d'un *dark pattern* « éthiquement problématique »[1387]. La différence entre le *nudge* et le *dark pattern* est que le premier identifie une vulnérabilité et travaille à la rectifier tandis que la seconde identifie la vulnérabilité pour l'exploiter[1388]. En effet, l'agence norvégienne rappelle l'asymétrie de l'information et de pouvoir entre la personne concernée et le responsable de traitement[1389] qui justifie que le droit doive se saisir de la possibilité pour le responsable de traitement d'abuser de son pouvoir pour tromper la personne concernée sans qu'elle ne s'en rende compte. Shoshana Zuboff attribue l'influence non éthique au capitalisme de surveillance qui, collectant « les données comportementales les plus prédictives », les utilise

---

[1383] *Ibidem.*

[1384] MATHUR Arunesh *et al.*, « What Makes a Dark Pattern… Dark? Design Attributes, Normative Considerations, and Measurements Methods», *CHI Conference on Human Factors in Computing Systems (CHI'21)*, 8–13 mai 2021, Yokohama, Japon, New York, ACM, p. 14.

[1385] La philosophie du « nudging » consiste à créer des architectures de choix permettant aux personnes de faire des meilleurs choix, tels qu'ils l'auraient eux-mêmes jugé. THALER Richard H., « Nudge, not sludge », *Science*, vol. 361, issue 6401, p. 431.

[1386] Le Monde, « Le "nudging" ou comment inciter les individus à adopter des comportements écoresponsables », *LeMonde.fr*, 7 avril 2022, disponible sur https://www.lemonde.fr/planete/article/2022/04/07/le-nudging-ou-comment-inciter-les-individus-a-adopter-des-comportements-ecoresponsables_6121043_3244.html (consulté en août 2022).

[1387] ForbrukerRådet, *Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*, 27 juin 2018, p. 7.

[1388] SUSSER Daniel *et al.*, «Technology, autonomy, and manipulation», *Internet Policy Review*, 2019, vol. 8, issue 2, p. 6.

[1389] ForbrukerRådet, *Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*, 27 juin 2018, p. 7.

pour « inciter (*nudge*), et influencer, ajuster (*tune*) et aiguillonner (*herd*) le comportement vers des résultats rentables » pour le responsable de traitement[1390]. La situation est encore plus hasardeuse lorsque les personnes concernées font confiance au responsable de traitement au point de penser que celui-ci défendra leurs intérêts, ce qui conduisait 95 % des utilisateurs d'applications à ne jamais changer les paramètres de confidentialité en 2011[1391].

681. Une seconde distinction se situerait au niveau de la conscience que la personne concernée aurait de l'influence exercée par elle : « contrairement à ceux qui persuadent ou contraignent, les manipulateurs [altèrent la décision de leur cible] à son insu »[1392]. Ainsi, quand l'influence est incompatible avec la vision kantienne de la rationalité, la manipulation est à proscrire puisque l'individu qui ne peut pas être rationnel ne peut pas être libre. Le *dark pattern*, en influençant la décision de la personne concernée à son insu, détériore « sa capacité à avoir des opinions et prendre des décisions informées de façon indépendante »[1393]. En créant des croyances chez la personne concernée, il court-circuite sa réflexion et délibération internes[1394]. Le *dark pattern* n'altère pas les options offertes à la personne, mais « pervertit la façon dont la personne aboutit à une décision, crée des préférences ou lui fait adopter des objectifs »[1395]. Les recherches sur la contagion émotionnelle menées sur le réseau social Facebook en sont une illustration : selon ses auteurs, les résultats de l'étude « montrent la réalité d'une contagion émotionnelle de masse via les réseaux sociaux »[1396]. C'est cette absence de conscience de l'influence exercée sur les choix de la personne manipulée qui explique que la manipulation provoque chez sa cible un sentiment de « trahison *ex post* »[1397].

682. Ces deux caractéristiques différenciant l'influence appropriée de la manipulation sont présentes dans la proposition de loi américaine appelée « DETOUR Act » (*Deceptive Experiences To Online Users Reduction Act*), introduite devant le Sénat en septembre 2019[1398].

[1390] ZUBOFF Shoshana, *op. cit.*, p. 30.

[1391] UIE, « Do users change their settings? », *uie.com*, 14 septembre 2011, disponible sur https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/ (consulté en mai 2021).

[1392] SUSSER Daniel *et al.*, «Online Manipulation: Hidden Influence in a Digital World», *Georgetown Law Technology Review*, 2019, vol. 4.1, p.38

[1393] KILOVATY Ido, «Legally Cognizable Manipulation», *Berkeley Technology Law Journal*, 2019, vol. 34, p. 469.

[1394] *Ibidem.*

[1395] RAZ Joseph, *The Morality of Freedom*, Oxford University Press,1986, p. 379.

[1396] Le Monde, « Des utilisateurs de Facebook "manipulés" pour une expérience psychologique », *LeMonde.fr*, Pixels, 30 juin 2014, disponible sur https://www.lemonde.fr/pixels/article/2014/06/30/des-utilisateurs-de-facebook-manipules-pour-une-experience-psychologique_4447625_4408996.html (consulté en mai 2021).

[1397] SUSTEIN Cass R., « Fifty Shades of Manipulation », *J. Behavioral Marketing*, 2016, vol. 213, p .6.

[1398] Senate of the United States, S.1084, *A Bill to Prohibit the Usage of Exploitative and Deceptive Practices by Large Online Operators and to Promote Consumer Welfare in the Use of Behavioural Research by Such Providers*, introduite devant le Sénat le 9 avril 2019, 116e Congrès, 1e session, disponible sur https://www.congress.gov/bill/116th-congress/senate-bill/1084/text (consulté en mai 2021).

Le DETOUR Act a pour objet d'interdire l'utilisation de pratiques trompeuses par les grands opérateurs numériques (plus de 100 millions d'authentifications sur 30 jours) : est interdit le fait de « concevoir, modifier ou manipuler une interface utilisateur en ayant pour but ou effet substantiel d'obscurcir, de subvertir ou de compromettre l'autonomie de l'utilisateur, sa prise de décision » ou son choix de consentir ou de partager des données[1399]. Cette proposition de loi est intéressante à deux titres. D'une part, en limitant le champ d'application de cette loi aux grands opérateurs numériques, la proposition de loi cible les situations dans lesquelles l'utilisateur fait face à un déséquilibre très important de pouvoir et d'information. D'autre part, la proposition de loi s'intéresse à la fois à l'effet de perte d'autonomie de l'utilisateur et à l'intention malveillante de l'opérateur de court-circuiter le processus interne de décision de l'utilisateur. Bien que la proposition soit toujours en phase de négociation, les membres du Congrès constatent dans les débats « un consensus grandissant […] sur le fait que les Américains devraient pouvoir faire des choix éclairés quant à la transmission de leurs données »[1400].

683. La régulation des *dark patterns* a aussi été discutée au niveau fédéral. Le *Colorado Privacy Act* définit les *dark patterns* comme une interface « conçue ou manipulée pour avoir l'effet substantiel de subvertir ou entraver l'autonomie, la prise de décision ou le choix de l'utilisateur »[1401] et affirme explicitement que les accords obtenus à l'aide de *dark patterns* ne constituent pas un consentement[1402]. Le *California Consumer Privacy Act* (CCPA) consacre l'interdiction d'utiliser des méthodes dont le but ou l'effet est de subvertir ou entraver le choix d'un consommateur de s'opposer à la vente de ses données[1403]. La loi californienne illustre l'interdiction d'une série d'exemples : le fait que le processus d'*opt-out* à la vente de ses données comporte plus d'étapes que le processus d'*opt-in*[1404], le fait que le responsable de traitement utilise un langage peu clair ou déroutant comme l'utilisation de doubles négatifs[1405], le fait de soumettre au consommateur une liste de raisons pour lesquelles ils ne devraient pas refuser la vente de leurs données[1406], le fait de demander des données à caractère personnel

[1399] *Idem*, Sec. 3 (a) (1) (A).
[1400] WARNER R. Mark, « Lawmaker Announce Additional Support for Bipartisan, Bicameral Legislation to Ban Manipulative "Dark Patterns" », *Communiqué de presse*, 15 juin 2022, disponible sur https://www.warner.senate.gov/public/index.cfm/2022/6/lawmakers-announce-additional-support-for-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns (consulté en août 2022).
[1401] Colorado Privacy Act, 6-1-1303 (9).
[1402] *Idem*, 6-1-1303 (5) (c).
[1403] California Consumer Privacy Act, § 999,306 (h).
[1404] *Idem*, § 999,306 (h) (1).
[1405] *Idem*, §999 306 (h) (2).
[1406] *Idem*, §999 306 (h) (3).

supplémentaires et non nécessaires au processus d'*opt out*[1407] et le fait de noyer le lien d'*opt out* dans une politique de confidentialité ou tout document similaire[1408]. De plus, si ces deux législations semblent être les seules à explicitement proscrire les *dark patterns*, d'autres législations pourraient également implicitement les interdire à travers leur définition du consentement[1409].

684. Des récentes études montrent la nécessité pour le législateur européen (ou les autorités de contrôle) de se saisir de la question des *dark patterns*, non seulement à cause des conséquences problématiques portées sur le consentement, mais aussi par rapport à la prolifération de comportements pourtant déjà plus ou moins explicitement interdits par le RGPD. Par exemple, une équipe de chercheurs anglo-américaine a montré que 50,1 % des sites internet les plus populaires au Royaume-Uni ne proposaient pas à la personne concernée de rejeter tous les cookies en un clic (mais proposaient néanmoins à la personne concernée de tous les accepter en un clic)[1410].

Figure 6 — Bannière de cookies non conforme au RGPD (Pull and Bears)

Face à cette pratique, la CNIL a explicitement affirmé que « la seule présence d'un bouton "Paramétrer" en complément du bouton "Tout accepter" tend, en pratique, à dissuader le refus

[1407] *Idem*, §999 306 (h) (4).
[1408] *Idem*, §999 306 (h) (5).
[1409] Par exemple, le cabinet d'avocats HuchBlackwell considère que le *Virginia Consumer Data Protection Act* (VCDPA) pourrait implicitement interdire les *dark patterns* à travers sa définition du consentement. HuckBlackwell, « How do the CPRA, CPA, and VCDPA treat dark patterns », *JDSupra*, 17 mars 2022, disponible sur https://www.jdsupra.com/legalnews/how-do-the-cpra-cpa-and-vcdpa-treat-5714239/ (consulté en septembre 2022).
[1410] NOUWENS Midas *et al.*, « Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence », *CHI Conference on Human Factors in Computing Systems*, 25-30 avril 2020, Honolulu, p. 5.

et ne permet donc pas de se mettre en conformité avec les exigences posées par le RGPD »[1411]. En effet, il a notamment été démontré que retirer le bouton « Rejeter tout » de la première page augmentait la probabilité pour la personne concernée de consentir d'environ 22 à 23 %[1412]. Plus largement, le Conseil d'État appelait également en 2015 à aligner les architectures de choix sur les intérêts des utilisateurs :

> « Parce que l'autonomie individuelle, pour peu qu'elle existe, n'est pas une capacité purement psychique, mais qu'elle dépend de facteurs socio-économiques, éducatifs, de "design", les "architectures" du choix individuel — telles que les systèmes de règles par défaut — fondées sur des acquis de la psychologie sociale ou sur une détection algorithmique du profil psychologique de celui qu'on appelle l'utilisateur, devraient faire l'objet d'évaluations rigoureuses, spécialement lorsqu'elles sont l'œuvre d'acteurs dont les intérêts ne sont pas alignés sur ceux des "utilisateurs" ».[1413]

685. L'évolution des réflexions sur les *dark patterns* proviendra peut-être de la jurisprudence. En octobre 2019, une Cour régionale allemande avait réaffirmé que la seule présence d'un bouton « accepter tout » à côté d'un bouton « détails » permettant de désélectionner les cookies individuels était contraire au RGPD[1414]. En effet, la Cour a considéré que « le consommateur moyen ne se donnera pas la peine de le faire et appuiera plutôt sur le bouton sans avoir lu les détails [ce qui] signifie que le consommateur ne connaît pas les conséquences de sa déclaration[1415]. De plus, le fait que l'option « accepter seulement les cookies nécessaires » « s'estompe en arrière-plan » à côté du bouton « accepter tous les cookies » constitue également une violation du RGPD dans la mesure où d'une part, l'option « accepter tous les cookies » apparaît comme présélectionné et d'autre part, ce design ne permet pas aux consommateurs de percevoir l'option « accepter seulement les cookies nécessaires » comme une « option de consentement équivalente »[1416].

686. L'action d'associations de protection des personnes concernées telles que *None of your business* (Noyb) permet déjà d'obtenir des résultats sur certains acteurs numériques à travers

---

[1411] CNIL, « Nouvelles règles pour les cookies et autres traceurs : bilan de l'accompagnement de la CNIL et actions à venir », *CNIL.fr*, 2 avril 2021, disponible sur https://www.cnil.fr/fr/nouvelles-regles-cookies-et-autres-traceurs-bilan-accompagnement-cnil-actions-a-venir (consulté en mai 2021).
[1412] NOUWENS Midas *et al., op. cit.*, p. 8.
[1413] Conseil d'État, *Le numérique et les droits fondamentaux*, Documentation Française, Les rapports du Conseil d'État, 2015, p. 411.
[1414] LG Rostock, 15 septembre 2020, 3 O 762/19.
[1415] JDSSupra, « The end of dark patterns in "cookie walls": German court bans deceptive design », *Jdsupra.com*, 21 janvier 2021, disponible sur https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/ (consulté en août 2022).
[1416] *Ibidem.*

une stratégie contentieuse de masse ciblant les bannières de consentement aux cookies[1417]. L'association a ainsi déposé 456 plaintes[1418] lors de sa première vague de ciblage des bannières de consentement aux cookies et 226 lors de sa deuxième[1419]. Cette stratégie devrait aboutir à l'apparition d'une série de jurisprudence qui permettra de préciser ce qui relève de l'influence acceptable et ce qui relève du *dark pattern*, dans la mesure où l'action contentieuse de Noyb a abouti à la création par l'EDPB d'une « *task force* » permettant de coordonner les réponses des autorités de contrôle aux plaintes déposées par l'association[1420].

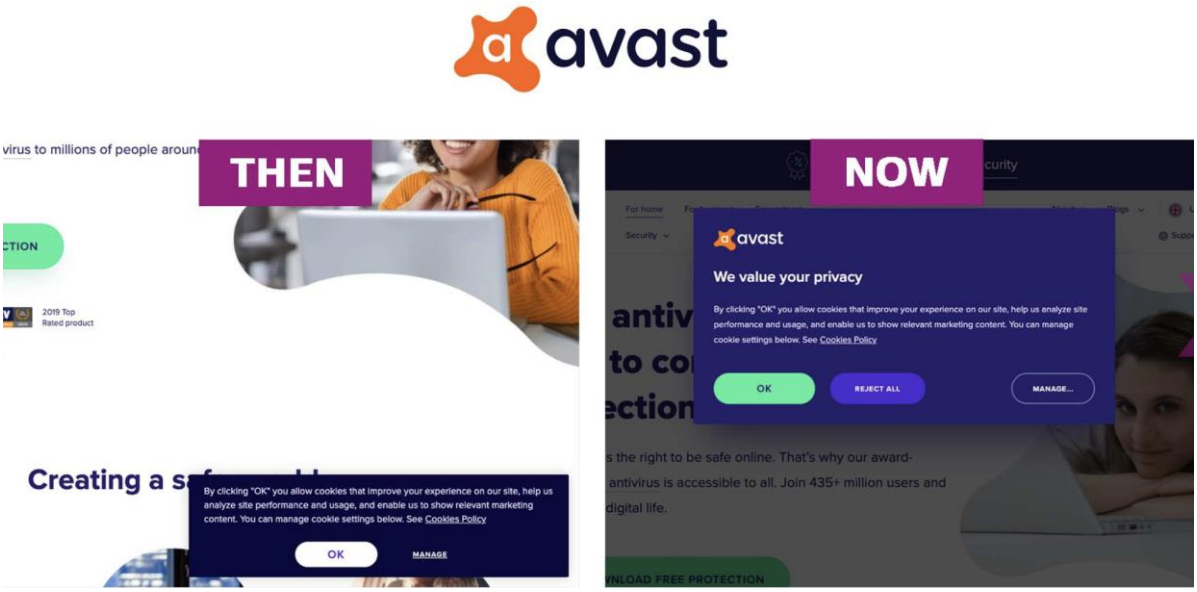

Figure 7 — Exemple de changement de design d'Avast à la suite de la stratégie contentieuse de Noyb

687. De plus, en 2020, le Comité européen sur la protection des données a dénoncé les « interfaces truquées, qui sont contraires à l'esprit de l'article 25 » du RGPD, sur la protection des données à caractère personnel dès la conception et par défaut[1421]. L'EDPB fait une lecture croisée de l'obligation de loyauté et de l'article 25 du RGPD pour en déduire l'illicéité des *dark*

[1417] L'association None of your business s'est donné comme mission de mettre fin à la « terreur des bannières de cookies » en 2021. Elle a, pour ce faire, créé un système de production automatique de plainte à la suite du scanner automatisé des bannières de cookies. Le projet de plainte est ensuite envoyé par mail aux sites internet concernés, qui disposent d'une période de grâce d'un mois pour modifier leur bannière. Faute de modification satisfaisante, l'association dépose une plainte devant l'autorité de contrôle compétente. None of your business, «Noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints», 31 mai 2021, disponible sur https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints (consulté en août 2022).

[1418] None of your business, «More Cookie Banners to go: Second wave of complaints underway», *noyb.eu*, 4 mars 2022, disponible sur https://noyb.eu/en/more-cookie-banners-go-second-wave-complaints-underway (consulté en août 2022).

[1419] None of your business, «226 complaints lodged against deceptive cookie banners», *noyb.eu*, 9 août 2022, disponible sur https://noyb.eu/en/226-complaints-lodged-against-deceptive-cookie-banners (consulté en août 2022).

[1420] EDPB, « EDPB establishes cookie banner taskforce« , *op. cit.*

[1421] EDPB, *Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par* défaut, version 2.0, adoptées le 20 octobre 2020, p. 22.

patterns. Dans son cahier sur la forme des choix, le laboratoire d'innovation de la CNIL appelle à « faire entrer le design et l'analyse des interfaces dans le champ de l'analyse de conformité des régulateurs »[1422], invitant les autorités de contrôle à contrôler la conformité au RGPD sous le prisme du « triangle de régulation » associant analyse juridique, analyse technique et analyse de design[1423]. Les travaux de la doctrine sur la classification des *dark patterns*[1424] ou encore les travaux créant des outils automatiques d'identification des *dark patterns* en vue de leur utilisation par des autorités de contrôle[1425].

688. En mars 2022, le Comité européen sur la protection des données (EDPB) a défini la notion de *dark patterns* comme des "interfaces et expériences utilisateur […] qui conduisent les utilisateurs à prendre des décisions de manière non intentionnelle, involontaire et potentiellement préjudiciable au regard de leurs données à caractère personnel"[1426]. Ce faisant, le Comité oppose directement l'existence de *dark patterns* à l'exercice d'un consentement libre et éclairé, qu'il s'agisse de consentement à un traitement de données à caractère personnel ou même un consentement en matière de contrat à la consommation[1427]. De la même manière que les législations américaines en la matière, le *dark pattern* n'est pas défini par une description de procédé, mais par son effet. Une telle définition évolutive permet de prendre en compte une variété de pratiques, allant de la demande répétitive de consentement au traitement de données supplémentaires[1428] à la direction émotionnelle par la culpabilité ou l'anxiété[1429], en passant par la décontextualisation des émotions[1430]. Une telle définition a été accueillie positivement par certains acteurs comme permettant de protéger les personnes concernées particulièrement vulnérables à certains facteurs d'influence comme les adolescents vis-à-vis de la pression sociale[1431]. D'un autre côté, une telle définition du *dark pattern* pourrait aboutir à des effets négatifs en créant une situation d'insécurité juridique au regard des responsables de traitement.

[1422] LINC, *op. cit.*, p. 38.
[1423] LINC, *op. cit.*,, p. 39.
[1424] V. par exemple MATHUR Arunesh *et al.*, « Dark Patterns at Scale: Findings from a Crawl of 11K Schopping Websites », *Proc. ACM Human-Comunter Interactions 3*, CSCW, article 81, novembre 2019, 32 p.; BÖSCH Christoph *et al.*, « Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns « , *Proceedings on Privacy Enhancing Technologies*, 2016, n°4, pp. 237-254.
[1425] NOUWENS Midas *et al.*, *op. cit.*
[1426] EDPB, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them»*, 14 mars 2022, version 1.0, p. 7.
[1427] *Ibidem.*
[1428] *Idem*, p. 14.
[1429] *Idem*, p. 16.
[1430] *Idem*, p. 63.
[1431] v. Amurabi SAS, *A user-centric perspective – Guidelines 3/2022 on Dark Patterns in social media platform interfaces*, 2 mai 2022, disponible sur https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/AmurabiUserCentricPerspectiveDarkPatternsGuidelines.pdf (consulté en août 2022).

Par exemple, l'association finlandaise *Data & Marketing* regrette que l'EDPB n'ait pas pris en compte les bénéfices de certains traitements de données à caractère personnel pour les utilisateurs dans ses lignes directrices sur les *dark patterns*[1432]. Ainsi, la distinction entre discours commercial et *dark pattern* fait l'objet d'une discussion multipartite, essentielle pour déterminer les contours de ce que la société européenne considère comme constitutif ou non d'un consentement libre et éclairé[1433]. Une telle discussion suppose un dialogue interdisciplinaire entre les juristes, les professionnels concernés, les psychologues, les associations de défense des consommateurs et les concepteurs de parcours utilisateurs[1434].

689. L'entrée du design dans le champ d'application de la conformité au RGPD est ainsi essentielle pour protéger le réel consentement de la personne concernée. Or, la situation actuelle est loin d'être satisfaisante. Pour aboutir à un contrôle satisfaisant du design et protéger ainsi le processus de décision de la personne concernée, il faut que les autorités de contrôle et le législateur se saisissent de la question. En effet, il s'agira d'une part, de préciser les contours de l'influence appropriée vis-à-vis du design, et d'autre part, d'effectuer un contrôle efficace dissuadant les responsables de traitement d'avoir recours à des pratiques *a priori* conformes aux exigences du RGPD, mais dont le design leurre, trompe ou manipule la personne concernée. Ces solutions doivent être complétées par des mécanismes de simplification de l'information, avec en premier lieu, la labellisation de l'information.

[1432] Data & Marketing Association Finland, *DMA Finland opinion on EDPB draft Guidelines 3/2022 on Dark Patterns in social media platform interfaces: How to recognize and avoid them*, 2 mai 2022, disponible sur https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/DMA%20Finland_EDPB_Dark_Patterns_02042022.pdf (consulté en août 2022).

[1433] V. par exemple l'association de professionnels Spolek pro ochranu osobních údajů qui suggère de ne pas considérer toute répétition de la demande de consentement comme un *dark pattern*. Ainsi, le curseur entre *dark pattern* et pratique commerciale doit être discutée au niveau européen afin de déterminer les pratiques acceptables sous le régime du RGPD. Spolek pro ochranu osobních údajů, *Comments on the EDPB's draft 'Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*, 2 mai 2022, disponible sur https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2022_05_02%20-%20SpOOU_EFDPO%20-%20EDPB_Guidelines_dark_patterns%20%28final%20-%20en%29.pdf (consulté en août 2022).

[1434] La conception de parcours utilisateurs (UX design) est considéré comme un moyen d'accentuation ou de rééquilibrage des pouvoirs entre le responsable de traitement et la personne concernée. V. par exemple VON GRAFENSTEIN Max, JAKOBI Tibo, STEVENS Gunnar, « Effective data protection by design through interdisciplinary research methods: The example of *effective* purpose specification by applying user-Centred UX-design methods », *Computer Law & Security Review*, vol. 46, septembre 2022, pp. 1-22 ; GRAY Colin M., «The Dark (Patterns) Side of UX Design», *CHI'18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, avril 2018, n° 534, pp. 1–14.

§2 — La labellisation de l'information

690. Le développement des standards, certifications et labels a pour origine plusieurs constats. Le premier est que « les éléments graphiques attirent plus que les textes »[1435]. Le deuxième est que la labellisation de l'information est un facteur de rationalité du comportement du consommateur sur le marché, transformant la poursuite d'objectifs perçus positivement par les consommateurs (écologie, nutrition, sécurité, protection des données à caractère personnel, etc.) en avantage concurrentiel[1436]. Enfin, le troisième constat est que l'univers numérique est un lieu où l'immédiat a occupé une place importante : la délivrance d'une information graphique standardisée permet à la personne concernée de s'informer rapidement et de façon fiable afin de consentir sans que ce consentement soit perçu comme un obstacle à son objectif primaire, l'accès à un bien, service ou site internet.

691. S'appuyant sur ces constats, le RGPD instaure, à la charge des États, des autorités de contrôle, du Comité européen de protection des données et de la Commission européenne, une obligation d'encourager la création et l'utilisation de mécanismes de certification[1437]. Le développement des certifications en est encore à ses balbutiements, mais certains éléments méritent d'être analysés pour déterminer en quoi ce mécanisme peut contribuer à la simplification de la personne concernée (A).

692. De plus, au-delà de la certification, le RGPD laisse timidement une place à la normalisation d'éléments graphiques permettant à la personne concernée de disposer d'une information visuelle standardisée au niveau national, voire au niveau de l'Union européenne (B).

A. La certification volontaire prévue par le RGPD

693. L'article 42 du RGPD introduit un mécanisme de « certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent » le RGPD[1438] ou encore de "démontrer que des responsables du traitement ou des sous-traitants qui ne sont pas soumis [au RGPD] fournissent des garanties appropriées dans le

---

[1435] RODRIGUES Rowena *et al.*, *EU Privacy seals project: Inventory and analysis of privacy certification schemes. Final Report*, Luxembourg, 2013, Publications Office of the European Union, p. 18.
[1436] BOY Laurence, « Labels écologiques et alimentaires : les enjeux de la réglementation européenne », *Journal de droit européen*, 2013, n° 195, p. 2.
[1437] Commission européenne, *Data Protection Certification Mechanisms. Study on Article 42 and 43 of the Regulation (EU) 2016/679*, Final Report, février 2019, p. 19.
[1438] RGPD, 27 avril 2016, article 42 (1).

cadre de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale"[1439]. L'article 42 (3) du RGPD ajoute que « la certification est volontaire et accessible via un processus transparent ». Ainsi, la certification comme prévue par l'article 42 du RGPD présente trois caractéristiques principales : elle peut prendre la forme d'une certification, d'un label ou d'une marque, elle peut démontrer soit le respect de dispositions de RGPD par un responsable de traitement soit la présence de garanties appropriées dans le cadre d'un transfert fondé sur l'article 46 du RGPD, et enfin, elle est volontaire.

694. L'utilisation des termes de certification, label et marque pose la question de savoir s'il s'agit d'une différence sémantique purement rhétorique ou, au contraire, d'une réelle volonté de la part du législateur européen de permettre aux acteurs de la certification d'adopter la forme juridique qu'il estime la plus opportune. Cependant, il semble que l'énumération des termes exprime uniquement la volonté du législateur européen de prendre en compte tous les libellés présents dans les droits nationaux des États membres[1440]. En attestent les propos de l'EDPB, qui, dans ses lignes directrices à la certification, envisage ces termes collectivement comme faisant partie d'un même processus :

> "Un certificat est une attestation de conformité. Un label ou une marque font généralement référence à un logo ou à un symbole dont la présence (en plus d'un certificat) indique que l'objet de la certification a été soumis à une évaluation indépendante dans le cadre d'une procédure de certification et qu'il est conforme à des exigences spécifiées, énoncées dans des documents tels que des règlements, des normes ou des spécifications techniques."[1441]

695. La certification volontaire s'inscrit dans la logique d'*accountability* qui irrigue le règlement[1442]. En effet, un des principaux changements qu'a initié le RGPD par rapport à la directive 95/46/CE est le passage d'une logique administrative de déclaration préalable des traitements (méthode de contrôle *ex-ante*) à une logique d'*accountability* dans laquelle le responsable de traitement doit mette en place des mesures structurelles et organisationnelles pour démontrer sa conformité au règlement (méthode de contrôle *ex-post*)[1443]. Il s'agit de présenter à la personne concernée une sorte de « présomption de preuve »[1444] que le responsable

---

[1439] RGPD, 27 avril 2016, article 42 (2).
[1440] Devant une telle confusion des termes, le terme « certification » sera utilisé dans la suite de la démonstration comme englobant les termes « certification », « label » et « marque » au sens de l'article 42 du RGPD.
[1441] EDPB, *Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement*, 4 juin 2019, version 3.0, p. 9.
[1442] LEVALLOIS-BARTH Claire, « Les mécanismes de labellisations issus du Règlement général sur la protection des données (RGPD) », *in* LEVALLOIS-BARTH Claire (dir.), *Signes de confiance. L'impact des labels sur la gestion des données personnelles*, Paris, Institut Mines-Télécom, 2018, p. 138.
[1443] Commission européenne, février 2019, *op. cit.*, p. 16.
[1444] LEVALLOIS-BARTH Claire, 2018, *op. cit.* p. 138.

de traitement a effectivement mis en place des mesures structurelles et organisationnelles lui permettant de respecter certains standards, et notamment les dispositions du RGPD.

696. La certification est volontaire, ce qui signifie qu'il s'agit d'un mécanisme qui « repose sur une logique incitative » permettant aux responsables de traitement de « choisir eux-mêmes la voie qui leur permettra de se conformer à leurs obligations »[1445]. En effet, le mécanisme de certification « mise et joue sur la volonté que manifestent les acteurs pour se positionner et se distinguer les uns par rapport aux autres dans un champ concurrentiel donné […] afin de les orienter, de manière souple, vers des options que l'action publique [considère] comme collectivement bénéfiques »[1446]. Ainsi, la certification s'adresse à des acteurs voulant se distinguer sur le marché européen comme respectueux de la protection des données au sens du droit européen.

697. De plus, les mécanismes de certification visent à susciter la confiance de la personne concernée ou du consommateur[1447]. Cette confiance est suscitée par une information délivrée de manière simple et rapidement compréhensible, qui aura auparavant été vérifiée par un organisme indépendant de confiance qui aura « mesuré » la qualité d'un produit. Ainsi, comme le souligne Jean-Marie Pontier, la certification s'inscrit dans la continuité des outils de mesures utilisés par les hommes lors d'une transaction :

> « Dès qu'il y eut échanges, les hommes cherchèrent à se doter d'instruments de mesure destinés à rendre ces échanges possibles, à défaut d'être vraiment équilibrés. La balance fut l'un de ces instruments utilisés dès la plus haute antiquité. Elle est tellement liée à cette idée de mesure d'une contrepartie que, sous la forme d'une balance romaine, elle est devenue l'un des symboles de la justice. Beaucoup plus tardivement, on s'est préoccupé des caractéristiques présentées par les produits et les services et, la concurrence se développant et les exigences des consommateurs aidant, de l'harmonisation de ces caractéristiques techniques »[1448].

[1445] TAMBOU Olivia, « L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ? », *Revue Lamy de Droit de l'Immatériel*, avril 2016, disponible sur ssrn (consulté en septembre 2021).

[1446] BERGERON Henri, CASTEL Patrick, DUBUISSON-QUELLIER Sophie, « Gouverner par les labels. Une comparaison des politiques de l'obésité et de la consommation durable », *Gouvernement et action publique*, 2014, vol. 3, p. 7.

[1447] « On constate en effet que les règles de droit ne sont plus désormais caractérisées par la seule contrainte, mais qu'elles cherchent également à orienter les comportements. Dans ce contexte, le label occupe une place particulière, en tant que signe extérieur et visible de la confiance ». LEVALLOIS-BARTH Claire, « La confiance saisie par le droit » *in* LEVALLOIS-BARTH Claire (dir.), *Signes de confiance. L'impact des labels sur la gestion des données personnelles*, Paris, Institut Mines-Télécom, 2018, p .30.

[1448] PONTIER Jean-Marie, « La certification, outil de la modernité normative », *Recueil Dalloz*, 1996, p. 355.

L'objectif de permettre à la personne concernée de « mesurer » rapidement le niveau de protection des données à caractère personnel offert par le responsable de traitement est d'ailleurs expressément affirmé par le considérant 100 du RGPD :

> « Afin de favoriser la transparence et le respect du présent règlement, la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question »[1449].

698. Quatre ans après l'entrée en vigueur du RGPD, le mécanisme de certification de l'article 42 n'a pas rencontré un grand succès auprès des autorités de contrôle, dont la priorité se situait probablement dans le contentieux et la sensibilisation. En 2022, le premier schéma de certification RGPD a vu le jour sous l'impulsion de l'autorité de contrôle luxembourgeoise, le CNPD[1450]. La certification « GDPR CARPA » proposée par le CNPD permet aux responsables de traitement de prouver que leur conformité RGPD est effective et pérenne dans le temps (à travers de nombreux processus documentés), ce qui permet par conséquent aux personnes concernées de s'assurer que le responsable de traitement respecte ses engagements vis-à-vis du règlement[1451]. Puisque la première certification RGPD est trop récente pour pouvoir faire l'objet d'une évaluation, l'identification de ses bénéfices pour le consentement des personnes concernées serait prématurée. Cependant, il est possible de se fonder sur l'expérience des certifications de nature privée pour identifier d'une part les facteurs clés de succès d'une certification volontaire (1) et d'autre part, les effets bénéfiques qu'une telle certification peut créer vis-à-vis de la réalité du consentement de la personne concernée au traitement de ses données à caractère personnel (2).

1. L'identification des facteurs clés de succès d'une certification volontaire

699. Il existe déjà sur le marché de nombreux mécanismes de certifications prenant la forme de labels, certifications ou encore marques[1452]. En 2018, Claire Levallois-Barth et Delphine Chauvet recensaient « sans prétendre à l'exhaustivité » l'existence de soixante-quinze labels de

---

[1449] RGPD, 27 avril 2016, considérant 100.

[1450] CNPD, « Le schéma de certification "GDPR CARPA" », *cnpd.public.lu*, disponible sur https://cnpd.public.lu/fr/professionnels/Certification/gdpr-carpa.html (consulté en août 2022).

[1451] CNPD, *GDPR-Certified Assurance Report Based Processing Activities*, Document to the attention of organizations that want to obtain certification of processing activities under the GDPR-CARPA certification mechanism, v. 1.0, 29 p.

[1452] LEVALLOIS-BARTH Claire, CHAUVET Delphine, « Panorama national et international des labels relatifs aux données personnelles », *in* LEVALLOIS-BARTH Claire (dir.), *Signes de confiance. L'impact des labels sur la gestion des données personnelles*, Paris, Institut Mines-Télécom, pp. 64-90.

protection des données européens, dont cinq labels de dimension européenne[1453]. Ce marché se caractérise par une très grande hétérogénéité des certifications : de très générales à très spécifiques, de régionales à internationales, de très peu de certifiés à plusieurs centaines de milliers, etc.[1454]

700. Pour identifier les facteurs clés de succès d'une certification volontaire, il faut en déterminer les objectifs principaux. S'agissant de la capacité d'une personne concernée d'exercer son consentement, la certification volontaire permet à la personne concernée de s'éclairer sur le traitement de données à caractère personnel qui lui est proposé de manière simple et rapide. Face à une politique de protection des données longue et détaillée, la certification permet de « démontrer rapidement et sans grand effort de l'utilisateur que la pratique de protection des données de l'entité certifiée répond à certains standards à la satisfaction de l'organisme de certification »[1455]. Cet objectif est renforcé par le fait que la visibilité et la couverture médiatique accordées aux certifications permettent de sensibiliser les personnes concernées à l'importance du droit à la vie privée et à la protection des données à caractère personnel[1456]. De plus, en encourageant la mise en conformité des responsables de traitement au sein de l'Union européenne, ce mécanisme permet également d'augmenter la confiance de la personne concernée, consommatrice sur le marché numérique[1457], en conformité avec les objectifs annoncés par la Commission européenne lors de sa communication établissant une stratégie européenne pour les données[1458]. Les certifications visent aussi à réduire le coût de la mise en œuvre du règlement sans en compromettre la conformité, incitant les responsables de traitement à mettre en place et à maintenir des mesures de protection des données, qui, en échange, obtiendront un avantage de réputation et de compétitivité sur le marché[1459].

701. Examinons désormais les avantages du mécanisme de certification. Tout d'abord, les certifications s'inscrivent dans une démarche de transparence vis-à-vis des personnes

---

[1453] *Idem*, p. 66.
[1454] RODRIGUES Rowena *et al.*, *op. cit.* 90 p.; LEVALLOIS-BARTH Claire, CHAUVET Delphine, *op. cit.*, pp. 64-90.
[1455] « The privacy seal demonstrates, rapidly, and without much effort to the users, that the certified entity's data protection practice meets certain standards to the satisfaction of the certifying body » [traduction libre]. RODRIGUES Rowena *et al.*, «The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR», *International Review of Law, Computers & Technology*, 2016, n° 30(3), p. 249.
[1456] RODRIGUES Rowena *et al.*, 2013, *op. cit.*, p. 17.
[1457] *Idem*, p. 12.
[1458] « Les citoyens ne feront confiance aux innovations fondées sur les données et ne les adopteront que s'ils sont convaincus que tout partage de données à caractère personnel dans l'UE sera subordonné à la pleine conformité avec les règles strictes de l'Union en matière de protection de la vie privée ». Commission européenne, COM (2020) 66 final, *op. cit.*, p. 1.
[1459] RODRIGUES Rowena *et al.*, 2016, *op. cit.*, p. 249 ; RODRIGUES Rowena *et al.*, 2013, *op. cit.*, p. 12.

concernées[1460]. En effet, par l'adoption d'un référentiel et d'un logo, les certifications permettent à la personne concernée de déterminer par un simple coup d'œil que le responsable de traitement respecte un certain nombre d'exigences qui ont été préalablement évaluées par un organisme spécialisé[1461]. La personne concernée a ainsi accès à une information normalisée et simplifiée par l'utilisation d'une information graphique dont elle percevra facilement la valeur.

Figure 8 - Exemples de logo de certifications

De plus, selon la CNIL, la certification permet de « communiquer auprès du grand public et de ses partenaires à partir d'une marque de confiance » tout en « valorisant le résultat d'une démarche de mise en conformité au RGPD »[1462]. Dès lors, en prouvant la conformité de ses traitements au RGPD, le responsable gagne la confiance des personnes concernées et se dote par conséquent d'un avantage compétitif de réputation. Enfin, le régulateur encourage le respect et le maintien d'un certain niveau de protection des données à caractère personnel en s'appropriant une forme plus souple de régulation, lui permettant également de déléguer une partie du contrôle de ces mesures à des organismes privés.

702. Cependant, si l'on regarde les mécanismes de certification déjà présents sur le marché, force est de constater que ces certifications présentent certaines faiblesses. En effet, les personnes concernées ne connaissent pas ou pas bien les certifications de protection des données[1463]. De plus, la normalisation de l'information n'est pas atteinte puisqu'il existe de nombreux formats de certification qui présentent des différences de référentiels, de codes graphiques, de zone géographique, de mécanismes de contrôle, etc. En outre, certains auteurs

---

[1460] CNIL, « Ce qu'il faut savoir sur la certification », *CNIL.fr*, 17 février 2021, disponible sur https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-la-certification (consulté en septembre 2021).
[1461] LEVALLOIS-BARTH Claire, CHAUVET Delphine, *op. cit.*, p. 82.
[1462] CNIL, « Ce qu'il faut savoir sur la certification », *CNIL.fr*, 17 février 2021, disponible sur https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-la-certification (consulté en septembre 2021).
[1463] RODRIGUES Rowena, WRIGHT David, WADHWA Kush, «Developing a privacy seal scheme (that works)», *International Data Privacy Law*, Volume 3, Issue 2, mai 2013, p. 106.

dénoncent le manque de crédibilité des certifications. En effet, il faut noter que les organismes de certifications peuvent se trouver dans une situation de conflit d'intérêts puisque le responsable de traitement candidat est également le client de l'organisme de traitement[1464]. Dès lors, les organismes de certification peuvent être réticents à appliquer sévèrement leurs critères et à révoquer l'un de leurs membres[1465].

703. Pourtant, le mécanisme de certification présente des opportunités intéressantes pour la protection des données à caractère personnel au sein de l'Union européenne. En effet, en simplifiant l'information, la certification augmente considérablement la force de choix et le caractère éclairé du consentement de la personne concernée quant au traitement de ses données à caractère personnel. Une certification efficace permet également de susciter de la confiance, un élément qui a été considérablement mis à mal par les nombreux scandales liés à la protection des données de ces dernières années, tels que les révélations d'Edward Snowden et, plus récemment, l'affaire Cambridge Analytica. La confiance des personnes concernées envers les acteurs numériques est dès lors devenue un des objectifs clés de la Commission européenne dans sa stratégie numérique[1466]. La profonde méfiance des personnes concernées envers les responsables de traitement a notamment été mise en évidence par un sondage mené par BCG dans différents États. Dans cette étude, 62 % des Français interrogés ont répondu qu'ils considéraient que les entreprises ne leur disaient pas comment elles utilisent réellement les données à caractère personnel qu'elles collectent[1467].

[1464] *Idem*, p. 108.
[1465] *Idem*, p. 107.
[1466] V. par exemple Commission européenne, COM (2020) 66 final, *op. cit*.
[1467] BCG, *Leveraging GDPR to Become a Trusted Data Steward,*

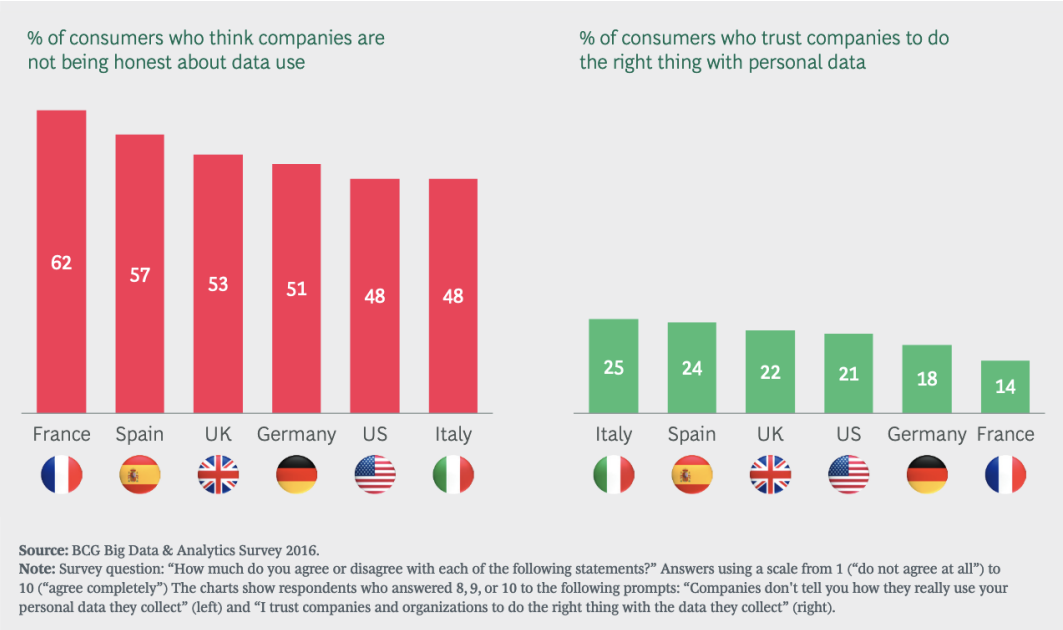

Figure 9 - BCG, Leveraging GDPR to Become a Trusted Data Steward, 2016

La certification apparaît ainsi comme un investissement intéressant du point de vue du responsable de traitement, puisque la confiance des personnes concernées génère un attrait moins grand pour les concurrents et produits de substitution ne présentant pas de garanties similaires, et une barrière à l'entrée plus grande des nouveaux entrants sur le marché. Enfin, l'opportunité pour le régulateur d'avoir recours à la certification est la valeur incitative de la certification quant à la mise en conformité des responsables de traitement avec le RGPD, ainsi que l'appui des organismes de certification dans le contrôle de la conformité des traitements avec le règlement.

704. Néanmoins, il faut garder à l'esprit que le mécanisme de certification peut également générer certaines menaces quant à l'effectivité de la protection des données à caractère personnel. La principale menace est le manque d'effectivité de la certification : dans ce cas, la certification échoue à attester de la conformité au règlement des traitements effectués par le responsable de traitement[1468]. Dans une telle situation, en raison de leur faible crédibilité, les labels de certification ne seront pas fiables[1469]. Il serait alors encore difficile pour la personne concernée de s'éclairer sur la fiabilité du responsable de traitement. Aussi, le responsable de

[1468] RODRIGUES Rowena, WRIGHT David, WADHWA Kush, *op. cit.* p. 106.

[1469] «This was especially true of the TRUST-e seal, based on the follow-up question asked, "If the TRUST-e logo was on the site, or had been on the site, what would this suggest to you, if anything?" Many simply said they didn't know or that it meant nothing, and a large number also gave answers that were negative toward the site, such as that the vendor was only trying to make it appear that the site guarded users' privacy, whether it did or not. ». MCKNIGHT D. Harrison, KACMAR Charles J., CHOUDHURY Vivek, «Shifting Factors and the Ineffectiveness of Third-Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business», *Electronic Markets*, Vol. 14, n° 3, 2010, p. 261.

traitement ne pourra pas profiter de la confiance des responsables de traitement et d'un avantage compétitif de réputation sur le marché, annihilant ainsi le retour sur investissement de la certification. Pire encore, la certification non effective, voire factice, peut avoir un effet réduisant la capacité de choix de la personne concernée en matière de protection des données à caractère personnel. En effet, la confiance mal placée favorise des consentements mal éclairés quant à la fiabilité du responsable de traitement. Le domaine de l'alimentaire constitue un bon exemple des effets négatifs du manque de crédibilité d'une certification, puisque la question de la fiabilité des labels est de plus en plus dénoncée par les associations des consommateurs[1470].

705. Pour conclure, la certification semble répondre à la matrice SWOT suivante :

Forces	**Faiblesses**
Information normalisée et simplifiée Confiance des personnes concernées vis-à-vis du responsable de traitement certifié Avantage compétitif de réputation Outil incitatif de conformité et de maintien de la conformité au règlement	Manque de connaissance par les personnes concernées de la valeur de la certification Manque de cohérence et d'harmonisation des certifications Conflit d'intérêts des organismes certificateurs Manque de contrôle d'ensemble de l'autorégulation
Opportunités	**Menaces**
Renforcement du contrôle des données à caractère personnel par les personnes concernées Augmentation de la confiance sur le marché européen du numérique Investissement pouvant devenir incontournable pour accéder à certains marchés Contrôle étendu de la conformité au règlement	Manque d'effectivité de la certification Perte de crédibilité des labels Effet contre-productif de la confiance mal placée Retour sur investissement trop limité

Figure 10 - Matrice SWOT des certifications de protection des données à caractère personnel

706. La certification se révèle donc être un outil particulièrement intéressant pour permettre une information fiable et efficace de la personne concernée. Cependant, mal utilisée, elle peut avoir l'effet inverse et induire la personne concernée en erreur. Il est donc essentiel que les

[1470] WWF, Greenpeace, BASIC, *Étude des démarches de durabilité dans le domaine alimentaire*, Rapport d'analyse transverse, juin 2021, 58 p., UFC Que Choisir, « Labels alimentaires et signes de qualité. Promesses non tenues : une révision s'impose ! », *QueChoisir.org*, 28 septembre 2021, disponible sur https://www.quechoisir.org/action-ufc-que-choisir-labels-alimentaires-et-signes-de-qualite-promesses-non-tenues-une-revision-s-impose-n94920/ (consulté en décembre 2021).

autorités de contrôle se saisissent de la question afin de permettre aux personnes concernées d'exercer sans difficulté l'autonomie de leur volonté.

2. La certification renforçant le consentement

707. Il faut rappeler en premier lieu que le RGPD ne crée ni de droit à la certification ni d'obligation de certification[1471]. Tout au plus, l'article 42 crée une obligation de moyens à la charge des États membres, des autorités de contrôle, du comité européen de la protection des données et de la Commission, d'encourager la mise en place de mécanismes de certification, labels et marques de respect du RGPD[1472]. L'effort de certification repose donc principalement sur les acteurs des politiques publiques de protection des données à caractère personnel, avec un rôle particulier accordé aux autorités de contrôle qui doivent approuver les critères de certification[1473]. Il est difficile aujourd'hui de dresser un bilan de l'effort de ces acteurs en matière de certification, le RGPD étant encore relativement jeune face au processus de certification qui doit demander un certain niveau de maturité aussi bien au niveau des critères d'évaluation que de la possibilité pour un organisme de certification de les évaluer[1474]. L'étude des documents préparatoires au RGPD se révèle également peu éclairante dans la mesure où le mécanisme de certification avait été peu étudié pendant les négociations concernant le RGPD, un seul *workshop* ayant été organisé par la Commission européenne sur le sujet en avril 2014[1475].

708. Malgré le peu de recul que nous disposons sur les certifications, certaines faiblesses et craintes ont d'ores et déjà fait leur apparition. Nous nous intéresserons aux trois principaux critères qui peuvent particulièrement influencer la qualité du consentement : le contenu de la certification, l'indépendance des organismes de certification et la présentation de la certification aux personnes concernées.

709. Premièrement, notons que le RGPD n'est pas restrictif quant aux éléments susceptibles d'être certifiés. La principale condition semble être que « l'accent soit mis sur la démonstration du respect de ce règlement par les responsables du traitement et les sous-traitants pour ce qui a

---

[1471] EDPB, *Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement*, 4 juin 2019, version 3.0, p. 5.
[1472] RGPD, article 42.
[1473] RGPD, article 42 (5) ; article 57 (1) (n).
[1474] V. Commission nationale pour la protection des données (CNPD), « Agrément des organismes de certification », disponible sur https://cnpd.public.lu/fr/professionnels/Certification/agrement.html (consulté en décembre 2021).
[1475] LACHAUD Eric, «Why the certification process defined in the General Data Protection Regulation cannot be successful», *Computer Law & Security Review,* Volume 32, Issue 6, décembre 2016, pp. 814–826.

trait à leurs opérations de traitement »[1476]. Aussi, l'EDPB note que la certification ne peut être délivrée qu'aux responsables de traitement et aux sous-traitants, « ce qui exclut par exemple la certification des délégués à la protection des données »[1477]. Une telle restriction n'a pas empêché la création de certifications DPO sur d'autres fondements que la certification RGPD, comme en atteste le référentiel de la CNIL[1478] ou celui de l'AEPD, l'autorité de contrôle espagnole[1479].

710. Plutôt que de se restreindre à un champ matériel déterminé, le contenu de la certification devra respecter certains critères permettant à la certification d'être efficace et transparente. En effet, le contenu devra être suffisamment précis et vérifiable pour permettre à la fois l'évaluation par l'organisme de contrôle et le respect des critères de la certification par le responsable de traitement et les sous-traitants. À ce titre, l'EDPB conseille de « se concentrer sur le caractère vérifiable, l'importance et la pertinence des critères de certification destinés à démontrer le respect du règlement »[1480]. Il est également conseillé de prendre en compte l'ensemble de l'environnement dans lequel se déroule le traitement de données à caractère personnel, y compris les systèmes techniques et les processus et procédures liés aux opérations de traitement[1481]. Les critères de certification doivent donc faire l'objet d'une réflexion suffisamment transversale et mature pour attester effectivement du respect du RGPD par le responsable de traitement. Les recommandations de l'EDPB se réfèrent à de nombreuses reprises à la norme ISO 17065 relative à l'évaluation de la conformité par les organismes certificateurs[1482]. Toutefois, l'EDPB ne considère pas ces dispositions comme étant satisfaisantes, dans la mesure où il conseille aux organismes accréditant les organismes de certification de les compléter par ses lignes directrices de l'EDPB et les recommandations éventuelles de l'autorité de contrôle[1483]. Par exemple, l'EDPB considère que la norme

---

[1476] EDPB, *Lignes directrices 1/2018*, 4 juin 2019, *op. cit.*, pp. 17-18.
[1477] *Idem*, p. 18.
[1478] CNIL, « Certification des compétences du DPO : la CNIL adopte deux référentiels », *CNIL.fr*, 11 octobre 2018, disponible sur https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels (consulté en décembre 2021).
[1479] AEPD, « Certificación de persona Delegada de protección de datos », AEPD.es, 29 octobre 2021, disponible sur https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos/certificacion (consulté en décembre 2021).
[1480] EDPB, *Lignes directrices 1/2018*, 4 juin 2019, *op. cit.*, p. 17.
[1481] *Idem*, p. 18.
[1482] ISO/CEI, *Évaluation de la conformité — Exigences pour les organismes certifiant les produits, les procédés et les services*, ISO/CEI 17065 : 2012, septembre 2012, disponible sur https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v2:fr (consulté en décembre 2021).
[1483] EDPB, *Opinion 26/2020 on the draft decision of the competent supervisory authority of Denmark regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 7 décembre 2020, p. 3 et p. 8.

ISO 17065 ne clarifie pas suffisamment la responsabilité de l'organisme de certification quand celui-ci fait appel à des sous-traitants pour la délivrance de certifications, ce qui « pourrait entraîner une application incohérente de l'accréditation des organismes de certification »[1484].

711. Les critères que l'organisme de certification doit remplir quant au contenu du programme de certification semblent encourager l'apparition de certifications spécialisées dans un domaine de produits ou de services. Ils confirment ainsi une tendance déjà observée sur le marché des certifications qui ne présentait déjà « pas ou peu de labels généraux applicables à l'ensemble des secteurs »[1485] en 2018. Le développement des certifications a été encouragé par la complexification de la perception de la qualité des produits notamment due à la globalisation et du développement technologique. Ces facteurs ont eu pour conséquence que « le degré de connaissance requis fait effectivement obstacle à ce que [la clientèle] parvienne à cerner par elle-même l'aptitude de ce qui est offert sur le marché à répondre à ses attentes »[1486]. Dès lors, la certification sera d'autant plus utile sur des domaines difficilement évaluables par la personne concernée et qui sont perçus comme particulièrement risqués pour elle : ce sera notamment le cas pour la cybersécurité[1487] ou encore le *cloud computing*[1488]. De plus, l'identification des critères de certification n'a pas la même importance selon les secteurs concernés. Par exemple, les critères d'évaluation des services de *cloud computing* seront principalement tournés vers les questions de cybersécurité tandis que les critères d'évaluation de services de marketing apprécieront plutôt les questions de licéité, de transparence et de minimisation des données. Par conséquent, les différents secteurs ne nécessiteront pas les mêmes compétences techniques de la part des organismes de conformité. Une nuance peut être apportée à ce constat concernant les aspects de cybersécurité qui pourraient, voire devraient, concerner l'ensemble des responsables de traitement tant « l'effectivité des droits fondamentaux à la vie privée et à la

---

[1484] *Idem;* p. 8.
[1485] LEVALLOIS-BARTH Claire, CHAUVET Delphine, *op. cit.*, p. 79.
[1486] PENNEAU Anne, « La certification », *JurisClasseur Environnement et Développement Durable*, Fasc. 5300, 1er janvier 2013, mis à jour le 13 septembre 2019, §9.
[1487] La certification est notamment considérée par le législateur européen comme étant nécessaire à l'établissement de la confiance sur le marché unique numérique. Règlement (UE) 1029/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité), considérant 65.
[1488] Une consultation publique sur la question d'une certification européenne des services de *cloud* a été lancée par l'agence européenne pour la cybersécurité le 22 décembre 2020. ENISA, « Cloud Certification Scheme: Building Trusted Cloud Services Across Europe », Communiqué de presse, *Enisa.europa.eu*, 22 décembre 2020, disponible sur https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme (consulté en décembre 2021).

protection des données à caractère personnel dépend considérablement des mesures mises en place pour assurer la sécurité de celles-ci »[1489].

712. Deuxièmement, la question de l'indépendance des organismes de certification pose question dans le contexte d'une privatisation du contrôle du RGPD. Si le RGPD prévoit la possibilité pour les autorités de contrôle de procéder elles-mêmes à l'évaluation des responsables de traitement et à la délivrance de la certification, Colin J. Bennet rappelle que ces autorités ne peuvent pas effectuer directement ces contrôles par manque de ressources et de temps et doivent ainsi « s'appuyer sur des substituts, y compris un éventail complexe d'acteurs du secteur privé avec différents niveaux de compétence et d'indépendance »[1490]. De nombreux États membres ont d'ailleurs choisi de se remettre à des organismes privés pour la délivrance de certifications[1491].

713. L'indépendance des organismes de certification permet d'atténuer la menace d'une capture de l'autorité publique par des acteurs privés, dont la désignation ne résulte pas d'un processus démocratique[1492]. En effet, si certains auteurs regrettent que les standards et certifications n'aient pas le même poids juridique qu'une assurance ou une garantie[1493], ces instruments peuvent tout de même être considérés comme des instruments de *soft law* puisque malgré leur caractère volontaire et donc facultatif, les certifications créent *de facto* une présomption de conformité à certains standards[1494]. Le rôle de l'État, à travers son autorité de contrôle ou son organisme national d'accréditation, peut se révéler dès lors secondaire, mais existant tout de même à travers le contrôle des compétences et des garanties d'indépendance et

---

[1489] DUMORTIER Franck, « L'obligation de sécurité des données personnelles : vers un standard de "diligence digitale" ? », in DAVIO, Victor *et al.* (dir.), *Le RGPD dans la pratique : un exercice d'équilibre*, 1r[e] édition, Bruxelles, Larcier, 2021, p. 42

[1490] « They must rely on surrogates, including a complicated array of private-sector actors with different levels of competence and independence ». BENNET Colin J., «The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats», *in* GUAGNIN Daniel *and al.* (dir), *Managing Privacy through Accountability*, New York, Springer, 2012, pp. 45–46.

[1491] L'Allemagne, l'Autriche, la Belgique, le Danemark, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, la Norvège, les Pays-Bas, le Portugal, la République tchèque, la Roumanie et le Royaume-Uni ont tous soumis, à travers leur autorité de contrôle, une demande d'avis au Comité européen de protection des données (EDPB) quant à la validité de leur procédure d'accréditation d'un organisme certificateur. D'autres autorités de contrôle ont également mis en place des mécanismes d'accréditation d'organismes certificateurs délivrées directement par l'autorité de contrôle comme la CNIL.

[1492] LACHAUD Eric, « Accountability and Certification in the GDPR », *SSRN.com*, 22 octobre 2021, disponible sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3948093 (consulté en décembre 2021).

[1493] LACHAUD Eric, «Why the certification process defined in the General Data Protection Regulation cannot be successful», *Computer Law & Security Review*, Volume 32, Issue 6, décembre 2016, pp. 814–826.

[1494] DE HERT Paul, PAPAKONSTANTINOU Vagelis, KAMARA Ines, « The New Cloud Computing ISO/IEC 27,018 Standard Through the Lens of the EU Legislaton on Data Protection », Working Paper, *Brussels Privacy Hub*, vol. 1, n°2, novembre 2014, p. 6.

d'impartialité de l'organisme certificateur[1495]. La question de l'indépendance des organismes de certification est également centrale pour assurer la réalité de la certification. En effet, la crédibilité d'une certification dépend essentiellement de l'organisme certificateur et notamment de son indépendance au centre du processus d'audit[1496]. C'est pourquoi « le principe d'indépendance se retrouve dans toutes les références normatives de la structure organisationnelle ISO […], pour marquer l'importance que l'on y attache dans la crédibilité du processus de certification »[1497]. La dernière mise à jour de la norme ISO 17065 a d'ailleurs conduit, selon l'organisme de standardisation, à « « l'amélioration des exigences d'impartialité »[1498].

714. L'objectivité de la certification, garantie par l'indépendance et l'impartialité de l'organisme certificateur, permet à la personne concernée de se fier aux certifications délivrées sous le régime de l'article 42 du RGPD, sans crainte d'une certification factice ou relevant du pur *marketing*. L'article 43 crée en effet une exigence d'indépendance et d'impartialité de l'organisme certificateur qui devra démontrer « à la satisfaction de l'autorité compétente, leur indépendance et leur expertise au regard de l'objet de la certification »[1499] et « que leurs tâches et leurs missions n'entraînent pas de conflit d'intérêts »[1500]. Une fois que les critères d'agrément d'un organisme de certification sont dessinés par une autorité de contrôle, le Comité de protection des données émet un avis requis par l'article 64 (1) (c) du règlement. Il est intéressant de constater que l'EDPB exerce un contrôle complet des critères d'agrément, notamment sur la question de l'indépendance, de l'impartialité et de l'absence de conflit d'intérêts. Sur dix-sept projets de critères d'agrément faisant l'objet d'un avis de l'EDPB, douze contiennent une recommandation de modification des critères d'agrément afin de garantir l'indépendance et l'impartialité de l'organisme certificateur. Ces recommandations n'ont pas toutes la même ampleur, puisque certaines corrections proposées par l'EDPB concernent les critères même proposés par l'autorité de contrôle tandis que d'autres corrections sont d'ordre plutôt formel et visent à aider les organismes certificateurs à atteindre l'exigence d'indépendance et

---

[1495] PONTIER Jean-Marie, 1996, *op. cit.* p. 355.
[1496] KOUAKOU Dogui, *Indépendance des auditeurs et enjeux éthique de la certification du système de gestion environnement ISO 14001,* Thèse présentée à la Faculté des études supérieures et postdoctorales de l'Université Laval dans le cadre du programme de docteur en Sciences de l'administration pour l'obtention du grade de Philosophiae Doctor (Ph.D), 2013, p. 3.
[1497] KOUAKOU Dogui, *Indépendance des auditeurs et enjeux éthique de la certification du système de gestion environnement ISO 14001,* Thèse présentée à la Faculté des études supérieures et postdoctorales de l'Université Laval dans le cadre du programme de docteur en Sciences de l'administration pour l'obtention du grade de Philosophiae Doctor (Ph.D), 2013, p. 36.
[1498] ISO/CEI, ISO/CEI 17065 : 2012, *op. cit.*
[1499] RGPD, 27 avril 2016, article 43 (2) (a).
[1500] RGPD, 27 avril 2016, article 43 (2)(e).

d'impartialité. Les recommandations de l'EDPB concernant l'indépendance et l'impartialité de l'organisme de certification sont résumées dans le tableau suivant :

Pays	Recommandations de l'EDPB concernant l'indépendance et l'impartialité de l'organisme de certification
Allemagne[1501]	Renforcer les critères applicables aux organismes de certification appartenant ou étant contrôlés par une entité juridique distincte, de manière à prendre en considération que tout type de relation économique entre l'organisme de certification et la personne morale, selon ses caractéristiques, peut affecter l'impartialité de ses activités de certification.
Autriche[1502]	Préciser que tout type de relation économique entre l'organisme de certification et la personne morale évaluée peut, selon ses caractéristiques, affecter l'impartialité de ses activités de certification.
Belgique[1503]	Ajouter, en addition de la procédure d'identification des conflits d'intérêts, une procédure de prise en compte des conflits d'intérêts identifiés. Fournir plus d'exemples de cas où il n'y a pas de conflit d'intérêts.
Bulgarie[1504]	Ajouter, en addition de la procédure d'identification des conflits d'intérêts, une procédure de prise en compte des conflits d'intérêts identifiés.
Danemark[1505]	Requérir de l'organisme de certification d'expliquer en détail dans ses procédures comment son indépendance et sa responsabilité sont assurées au regard de ses décisions individuelles de certification.
France[1506]	Ajouter, en addition de la procédure d'identification des conflits d'intérêts, une procédure de prise en compte des conflits d'intérêts identifiés. Préciser le vocabulaire relatif à l'indépendance des organismes de certification (l'obligation de ne pas être « affilié » à l'organisme candidat n'est pas suffisamment claire).
Grèce[1507]	Procéder d'abord à l'identification des conflits d'intérêts avant de procéder à leur prise en compte. Préciser le vocabulaire relatif à l'indépendance des organismes de certification (l'obligation de ne pas être « affilié » à l'organisme candidat n'est pas suffisamment claire).

[1501] EDPB, *Opinion 15/2020 on the draft decision of the competent supervisory authority of Germany regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 25 mai 2020
[1502] EDPB, *Opinion 30/2020 on the draft decision of the competent supervisory authority of Austria regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 7 décembre 2020.
[1503] EDPB, *Opinion 35/2021 on the draft decision of the competent supervisory authority of Belgium regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 30 novembre 2021.
[1504] EDPB, *Opinion 13/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 4 juillet 2022.
[1505] EDPB, *Opinion 26/2020*, 7 décembre 2020, *op. cit.*
[1506] EDPB, *Opinion 12/2022 on the draft decision of the competent supervisory authority of France regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 4 juillet 2022.
[1507] EDPB, *Opinion 22/2020 on the draft decision of the competent supervisory authority of Greece regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 15 août 2020

Hongrie[1508]	Aucune
Irlande[1509]	Fournir plus d'exemples de cas où il n'y a pas de conflit d'intérêts.
Italie[1510]	Aucune
Lettonie[1511]	Ajouter, en addition de la procédure d'identification des conflits d'intérêts, une procédure de prise en compte des conflits d'intérêts identifiés. Fournir plus d'exemples de cas où il n'y a pas de conflit d'intérêts.
Lituanie[1512]	Clarifier les exigences en matière de conflit d'intérêts, les exemples fournis par la procédure d'accréditation étant trop larges et s'appliquant à la majorité des organismes de certification (*par exemple, remplacer le cas où l'organisme de certification est majoritairement financé par la fourniture de prestations de certification par le cas où l'organisme de certification est majoritairement financé par la fourniture de prestations de certification à l'entité évaluée*).
Luxembourg[1513]	Aucune
Norvège[1514]	Ajouter, en addition de la procédure d'identification des conflits d'intérêts, une procédure de prise en compte des conflits d'intérêts identifiés.
Pays-Bas[1515]	Aucune
Pologne[1516]	Aucune

[1508] EDPB, *Opinion 19/2021 on the draft decision of the competent supervisory authority of Hungary regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 1e juin 2021.
[1509] EDPB, *Avis 14/2020 sur le projet de décision de l'autorité de contrôle compétente irlandaise concernant l'approbation des exigences relatives à l'agrément d'un organisme de certification au titre de l'article 43, paragraphe 3*, adopté le 25 mai 2020.
[1510] EDPB, *Opinion 23/2020 on the draft decision of the competent supervisory authority of Italy regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 15 août 2020
[1511] EDPB, *Opinion 38/2021 on the draft decision of the competent supervisory authority of Latvia regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 20 juillet 2021.
[1512] EDPB, *Opinion 25/2021 on the draft decision of the competent supervisory authority of Lithuania regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 20 juillet 2021
[1513] EDPB, *Avis 5/2020 sur le projet de décision de l'autorité de contrôle compétente luxembourgeoise concernant l'approbation des exigences relatives à l'agrément d'un organisme de certification au titre de l'article 43, paragraphe 3*, adopté le 31 janvier 2020.
[1514] EDPB, *Opinion 36/2021 on the draft decision of the competent supervisory authority of Norway regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 30 novembre 2021.
[1515] EDPB, *Opinion 21/2020 on the draft decision of the competent supervisory authority of the Netherlands regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 15 août 2020
[1516] EDPB, *Opinion 12/2022 on the draft decision of the competent supervisory authority of Poland regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 4 juillet 2022.

Portugal[1517]	Ajouter, en addition de la procédure d'identification des conflits d'intérêts, une procédure de prise en compte des conflits d'intérêts identifiés.
République tchèque[1518]	Intégrer les conditions relatives à l'impartialité de l'organisme de certification de l'annexe au sein du texte des conditions d'agrément.
Roumanie[1519]	Fournir plus d'exemples de cas où il n'y a pas de conflit d'intérêts.
Royaume-Uni[1520]	Aucune

715. Enfin, l'EDPB insiste sur la question de la cohérence du contenu de la certification avec la présentation qui est faite de cette certification aux personnes concernées et affirme que "les organismes de certification qui utilisent des mécanismes de certification, des labels ou des marques destinés aux personnes concernées (en leur qualité de consommateurs ou de clients) devraient fournir des informations facilement accessibles, intelligibles et qui fassent sens sur la ou les opérations de traitement certifiées"[1521]. L'EDPB alerte aussi les organismes de certification sur la nécessité d'identifier des critères pertinents par rapport au public de la certification : les critères essentiels dans la relation entre entreprises (*B to B*) ne seront peut-être pas les mêmes que les critères permettant aux personnes concernées d'exercer un consentement éclairé dans une relation entreprise-consommateur (*B to C*)[1522]. Il s'agit ici de neutraliser « l'effet potentiellement trompeur » de la certification par rapport au référentiel d'évaluation[1523]. Ainsi, il n'est pas question qu'une certification portant sur le sérieux du processus d'analyse d'impact d'une entreprise soit présentée comme une certification de

[1517] EDPB, *Opinion 12/2021 on the draft decision of the competent supervisory authority of Portugal regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 23 mars 2021.
[1518] EDPB, *Opinion 16/2020 on the draft decision of the competent supervisory authority of the Czech Republic regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 25 mai 2020.
[1519] EDPB, *Opinion 13/2021 on the draft decision of the competent supervisory authority of Romania regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 23 mars 2021.
[1520] EDPB, *Avis 4/2020 sur le projet de décision de l'autorité de contrôle compétente du Royaume-Uni concernant l'approbation des exigences relatives à l'agrément d'un organisme de certification au titre de l'article 43, paragraphe 3*, adopté le 31 janvier 2020.
[1521] EDPB, *Lignes directrices 1/2018*, 4 juin 2019, *op. cit.*, p. 22.
[1522] *Idem*, p. 23.
[1523] LEVALLOIS-BARTH Claire, « Les labels visant à susciter la crédibilité : des pratiques existantes vers l'amélioration de la qualité », *in* LEVALLOIS-BARTH Claire (dir.), *Signes de confiance — l'impact des labels sur la gestion des données personnelles*, Institut Mines-Télécom, Chaire Valeurs et Politiques des Informations Personnelles, janvier 2018, p. 126.

conformité RGPD, dans la mesure où la certification ne mesure pas l'ensemble de la conformité aux règles contenues dans le règlement.

716. Ainsi, la certification peut se révéler être un instrument prometteur quant à la simplification de l'information pour la personne concernée. Le développement des certifications soumises au régime de l'article 42 du RGPD sera intéressant à suivre, parce qu'il s'agit d'un instrument précieux, mais fragile de co-régulation. En effet, le développement de nombreuses certifications au niveau national pourra à terme rencontrer des problèmes de cohérence et de concurrence au niveau de l'Union européenne malgré le contrôle du Comité européen pour la protection des données. Ces situations seraient problématiques à la fois quant à la crédibilité de la certification, mais également vis-à-vis de la personne concernée puisque la multiplication des labels, marques et certification entraînera sans doute une certaine confusion, à l'image de la situation actuelle dans le domaine de l'alimentaire. De plus, les certifications RGPD auront à se faire connaître du public concerné grâce à des politiques publiques de promotion de ces certifications afin que d'une part, les personnes concernées aient connaissance de cette aide à la prise de décision et d'autre part, que ces certifications restent attractives face à des certifications hors article 42 déjà proposées par des organismes de certification bien connus du public (comme les normes ISO). Peut-être que la solution d'une certification européenne commune[1524] sera en définitive une solution d'harmonisation et de crédibilité de la certification RGPD, à l'image des développements relatifs à la certification européenne en matière de cybersécurité[1525].

717. Une autre solution pour atteindre la simplification et l'harmonisation de l'information est suggérée par le RGPD à travers la normalisation, par la Commission européenne, d'informations graphiques permettant à la personne concernée de s'informer plus aisément.

B. La normalisation d'informations graphiques

718. La simplification de l'information délivrée au consommateur final est une question bien connue dans le domaine de l'alimentaire. Par exemple, dans la stratégie « *Farm to Fork* » de la Commission européenne, cette dernière propose une labellisation harmonisée et obligatoire de l'information sur les aspects nutritionnels des produits alimentaires, en plus d'un éventuel label

[1524] L'article 42 (5) du RGPD prévoit en effet que « lorsque les critères sont approuvés par le comité, cela peut donner lieu à une certification commune, le label européen de protection des données ».
[1525] Règlement (UE) 1029/881, 17 avril 2019, *op. cit.*

volontaire sur les aspects climatiques, environnementaux et sociétaux de ces produits[1526]. Les objectifs de la simplification de l'information délivrée au consommateur sont la transparence de l'information[1527] et la lutte contre les pratiques commerciales pouvant induire le consommateur en erreur[1528]. La protection des données à caractère personnel pourrait s'inspirer de l'expérience de l'étiquetage alimentaire afin de simplifier la tâche de la personne concernée souhaitant évaluer les risques attachés à un traitement de données à caractère personnel. Ainsi, le consentement pourrait être renforcé par l'existence de mentions obligatoirement visibles sur l'ensemble du site internet ou le devant de l'emballage d'un produit ou par l'existence d'un système de notation normalisée des traitements de données.

719. Dans le domaine alimentaire, certaines mentions doivent être obligatoirement mises en valeur afin, soit d'aider le consommateur à comprendre certaines valeurs nutritives (par exemple, la mention « avec édulcorants »), soit de prévenir le consommateur de certains risques à la consommation du produit (par exemple, la mention « contient de la réglisse — les personnes souffrant d'hypertension doivent éviter toute consommation excessive »)[1529]. D'autres mentions permettent au consommateur d'opérer une traçabilité de ses aliments (par exemple l'indication d'origine pour les viandes préemballées[1530]), ou encore d'attester de certaines qualités d'un produit comme le label européen « appellation d'origine protégée (AOP) »[1531].

720. Par analogie, il serait possible d'imaginer une obligation de mentions obligatoirement mises en valeur dès le premier contact de la personne concernée avec le responsable de traitement ou au niveau de l'emballage du produit concerné. Cette solution demanderait un effort d'identification des risques principaux du traitement de données à caractère personnel, des acteurs impliqués dans le traitement des données à caractère personnel et des facteurs guidant le choix des personnes concernées lorsqu'elles exercent leur consentement. Par

---

[1526] Commission européenne, *Farm to Fork Strategy. For a fair, healthy and environmentally-friendly food system*, Communication de la Commission au Parlement européen et au Conseil, Bruxelles, 20 mai 2020, COM (2020) 381 final, p. 14.

[1527] Cet objectif est annoncé clairement en France à travers le libellé de la loi. Loi n° 2020-699 du 10 juin 2020 relative à la transparence de l'information sur les produits agricoles et alimentaires.

[1528] Par exemple, l'article L.412-12 du Code de la consommation précise désormais que « le nom et l'adresse du producteur de bière sont indiqués en évidence sur l'étiquetage de manière à ne pas induire en erreur le consommateur quant à l'origine de la bière, d'une manière quelconque, y compris en raison de la présentation générale de l'étiquette ».

[1529] DGCCRF, *État des lieux de la réglementation encadrant l'information du consommateur*, Document de travail, décembre 2012, p. 9.

[1530] Ministère de l'Économie, des Finances et de la Relance, « Denrées alimentaires : quelles sont les règles d'étiquetage ? », 3 juin 2021, disponible sur https://www.economie.gouv.fr/particuliers/denrees-alimentaires-regles-etiquetage (consulté en décembre 2021).

[1531] Ministère de l'économie, des finances et de la relance, « AOP-AOC, IGP, AB… : les labels de qualité dans l'alimentation », 10 décembre 2021, disponible sur https://www.economie.gouv.fr/particuliers/aop-aoc-igp-stg-labels-certification-alimentation (consulté en décembre 2021).

exemple, dans le contexte d'un dispositif de type compteur intelligent (comme les compteurs Linky), les préoccupations de la personne concernée ont trait à la sécurité du dispositif (afin d'éviter leur utilisation illégale via un cambriolage ou du harcèlement), l'utilisation des données pour des usages commerciaux y compris la publicité ciblée et les polices d'assurance, l'utilisation des données par les forces de l'ordre ou dans le cadre d'une procédure judiciaire (garde des enfants, conflit avec le propriétaire, etc.) ou encore l'utilisation des données par une personne non autorisée (qu'elle soit intérieure au foyer ou extérieure comme un voisin)[1532]. Un nombre important de ces préoccupations relèvent de la cybersécurité, déjà bien dotée de différents labels de confiance. Cependant, certaines mentions pourraient orienter le choix de la personne concernée comme la mention de vente des données à des tiers (et éventuellement le nombre de tiers concernés), d'utilisation des données à visées commerciales, de durées de conservation de données ou encore de transferts de données vers des pays tiers. D'autres mentions informatives pourraient également être importantes dans le cadre de l'exercice du consentement de la personne concernée comme le traitement de données sensibles ou encore l'existence d'une prise de décision automatisée.

721. Le RGPD ouvre la voie à une standardisation d'éléments visuels permettant à la personne concernée d'effectuer son choix plus aisément à travers la délivrance d'informations graphiques et faciles à comprendre, à l'image de l'expérience réussie des icônes relatives aux licences de copyright *creative commons*[1533]. L'utilisation d'icônes permet également d'attirer l'attention de la personne concernée sur la protection des données à caractère personnel, alors même qu'elle est concentrée sur son objectif principal (par exemple, l'achat d'un produit ou encore l'accès à une information)[1534]. Ainsi, le RGPD offre à la Commission européenne la possibilité d'adopter des actes délégués conformément à l'article 290 du traité sur le fonctionnement de l'Union afin de déterminer « les informations à présenter sous la forme d'icônes normalisées »[1535]. L'article 12 (7) du règlement précise que ces icônes normalisées doivent « offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible du traitement prévu » et doivent « être lisibles par machine »[1536]. Dans le processus de normalisation de ces icônes, le règlement permet au Comité de protection des données de rendre

[1532] MCKENNA Eoghan, RICHARDSON Ian, THOMSON Murray, «Smart meter data: Balancing consumer privacy concerns with legitimate applications», *Energy Policy*, Volume 41, février 2012, pp. 807–814.
[1533] Weizenbaum institute, *Annual Report*, 2018–2019, p. 40.
[1534] EFRONI Zohar *et al.*, «Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing», *European Data Law Review (EDPL)*, 2019, vol. 3, p. 358.
[1535] RGPD, 27 avril 2016, considérant 166, article 12 (8).
[1536] RGPD, 27 avril 2016, considérant 60, article 12 (7).

à la Commission un avis sur les icônes proposées, de sa propre initiative ou sur demande de la Commission[1537]. Le G29, dans ses lignes directrices relatives à la transparence, alerte sur la nécessité d'une normalisation unique et claire « des symboles et images, qui doivent être utilisés de façon universelle et reconnus dans l'Union européenne comme des raccourcis indiquant ces informations »[1538]. Dès lors, le processus de normalisation demande un effort d'identification des informations à normaliser, de détermination d'icônes faciles à comprendre, mais également facilement adoptables par les responsables de traitement. Le G29 reconnaît que la normalisation d'icônes est un processus long qui nécessite en amont « de mener des recherches approfondies conjointement avec les entreprises et le grand public à l'égard de l'efficacité des icônes dans ce contexte »[1539]. En effet, le risque d'effet contre-productif de l'iconographie est substantiel, la loi étant par essence « verbocentrique »[1540] : il sera donc essentiel de délimiter précisément la signification d'une icône et le contexte dans lequel elle pourra être utilisée.

722. Une autre approche consiste en un système d'évaluation des risques, permettant à la personne concernée de se reposer sur une évaluation déjà réalisée des risques associés au traitement de données à caractère personnel. Le Weizenbaum Institute propose à cet effet la création d'un système d'icônes fondé sur l'identification de risques (violations des libertés, discriminations, etc.) et sur la mesure de ces risques par rapport aux traitements de données à caractère personnel[1541]. L'objectif est de découvrir quels aspects du traitement de données à caractère personnel entraînent des risques importants (par exemple, le traitement de données sensibles).[1542] La création d'icônes intervient dans un second temps afin d'aiguiller la personne concernée sur les aspects identifiés associés au traitement de données à caractère personnel pouvant entraîner un risque pour la personne concernée grâce à des icônes faciles à reconnaître et à mémoriser[1543].

723. L'approche fondée sur le risque n'est pas sans rappeler l'approche de la Commission quant aux systèmes d'intelligence artificielle. La notion de risque est également présente dans le texte du RGPD. Afin de déterminer s'il a l'obligation de mener une analyse d'impact pour certains traitements, le responsable de traitement doit déterminer « la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la

---

[1537] RGPD, 27 avril 2016, article 70 (1) (r).
[1538] Groupe de travail « Article 29 », WP260 rev. 01, *op. cit.*, p. 30.
[1539] *Ibidem.*
[1540] ROSSI Arianna, PALMIRANI Monica, «Can Visual Design Provide Legal Transparency? The Challenges of Icons for Data Protection», *Design Issues*, 2020, Vol. 36(3), p. 84.
[1541] Weizenbaum institute, *op. cit.*, p. 41.
[1542] EFRONI Zohar *et al.*, *op. cit.*, p. 364.
[1543] Weizenbaum institute, *op. cit.*, p. 41.

portée, du contexte et des finalités du traitement » à travers une « évaluation objective »[1544]. S'il repère la probabilité d'un risque élevé, il doit mener une analyse d'impact comportant « une évaluation des risques pour les droits et libertés des personnes concernées »[1545]. Par ailleurs, le RGPD pourrait également permettre la prise en compte de risques sociétaux, en plus des risques individuels, dans la mesure où le considérant 71 se réfère explicitement à la prévention des effets discriminatoires à l'égard des personnes physiques[1546]. Enfin, les auteurs de la proposition d'une approche fondée sur le risque remarquent que l'obligation de transparence du RGPD contient déjà une telle approche puisque le responsable de traitement doit explicitement informer la personne concernée d'un transfert de données à caractère personnel vers un pays tiers ou de l'existence d'une prise de décision automatisée, qui sont des traitements particuliers en raison du risque[1547].

724. Enfin, initialement, le Parlement européen avait proposé une nomenclature d'informations normalisées permettant à la personne concernée de repérer des pratiques évaluées par le Parlement comme étant des pratiques particulièrement protectrices des données à caractère personnel[1548]. L'article 13 bis proposait une série d'informations normalisées qui comprenaient une icône, un texte explicatif dont l'information essentielle était présentée à caractère gras et une forme graphique comportant un code couleur[1549].

[1544] RGPD, 27 avril 2016, considérant 76.
[1545] RGPD, 27 avril 2016, Article 35 (7) (c).
[1546] EFRONI Zohar *et al.*, *op. cit.*, pp. 363–364.
[1547] RGPD, 27 avril 2016, Article 13 (1) (f), Article 13 (2) (f), Article 14 (1) (f), Article 14 (2) (g) ; EFRONI Zohar *et al.*, *op. cit.*, p. 364.
[1548] Parlement européen, *Résolution législative du Parlement européen du 12 mars 2014 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) (COM [2012] 0011 – C7-0025/2012 – 2012/011 [COD]*, P7-TA [2014] 0212, Article 13bis, Annexe.
[1549] *Ibidem.*

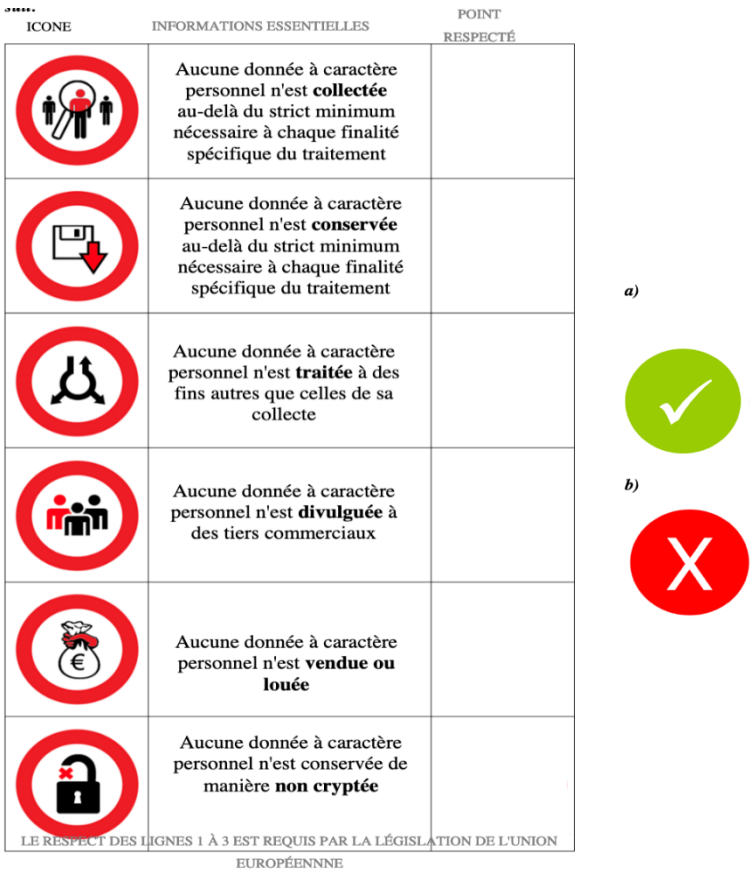

Figure 11 — Iconographie proposée par le Parlement européen

725. Plusieurs critiques peuvent être soulevées à la suite de la publication de cette nomenclature. En premier lieu, l'iconographie proposée par le Parlement européen reprend les codes graphiques de l'interdiction présents dans le Code de la route (un cercle entouré d'une bande épaisse rouge) et une formulation négative de l'information proposée (« aucune donnée à caractère personnel n'est »)[1550]. Ce choix complique inutilement l'information. Par exemple, l'apposition du graphisme négatif en troisième colonne de la sixième ligne signifie qu'il n'est pas vrai qu'aucune donnée à caractère personnel n'est conservée de manière non cryptée (triple négation)[1551]. En second lieu, il est surprenant de standardiser une information qui ne relève que du simple respect du RGPD (lignes 1 à 3), en mentionnant discrètement que « le respect des lignes 1 à 3 est requis par la législation de l'Union européenne ». En effet, le simple respect du RGPD ne peut pas constituer un élément d'information utile à la prise de décision de la personne concernée et l'information requise par le principe de transparence sera normalement

[1550] PETTERSON John Sören, « A brief evaluation of icons suggested for use in standardized information policies. Referring to the Annex in the first reading of the European Parliament on COM(2012) 0011», *in* CAMENISH J., HANSEN M. (dir.), *Privacy and Identity Management for the Future Internet in the Age of Globalisation*, Privacy and Identity 2014, IFIP Advances in Information and Communication Technology, vol. 457, Springer. pp. 125–135.
[1551] *Ibidem.*

diffusée sur l'ensemble des sites internet et produits auxquels elle a accès sur le territoire de l'Union européenne. L'objectif de ces icônes se trouve peut-être dans une dimension plus mercantile, permettant aux responsables de traitement de prouver leur respect du RGPD en dehors de l'Union européenne afin d'obtenir un avantage compétitif de perception de respect de la vie privée. L'article 13 bis proposé par le Parlement a rapidement été supprimé par le Conseil en première lecture[1552].

726. La réflexion sur l'iconographie n'avait ainsi pas atteint sa maturité au moment de la proposition du RGPD. Or, à ce jour, la Commission n'a toujours pas adopté d'acte délégué proposant une iconographie harmonisée en matière de protection des données à caractère personnel au sein de l'Union européenne. L'initiation d'une réflexion multipartite sur la définition d'icônes en matière de protection des données à caractère personnel pourrait pourtant participer à la protection de la réalité du consentement de la personne concernée, notamment du caractère éclairé de son consentement. L'autorité de contrôle italienne a en 2021 pris l'initiative d'inclure la société civile dans la conception d'icônes en créant un concours d'icônes RGPD[1553]. Quatre projets ont été sélectionnés afin d'être utilisés par tout responsable de traitement sous les termes d'une licence *open source.* Cette réflexion ne visait cependant pas à faciliter le consentement grâce à des informations visuelles les aidant dans leur vision du niveau de protection des données à caractère personnel, mais uniquement en facilitant la lecture des politiques de protection des données en proposant une série d'icônes unifiées pour chaque élément obligatoirement présent dans une politique de confidentialité.

[1552] Conseil européen, 5419/16, *op. cit.*.
[1553] GDPD, « Informative chiare i vincitori del contest lanciato dal garante privacy », *gdpd.it*, disponible sur https://www.gpdp.it/web/guest/temi/informativechiare (consulté en août 2022).

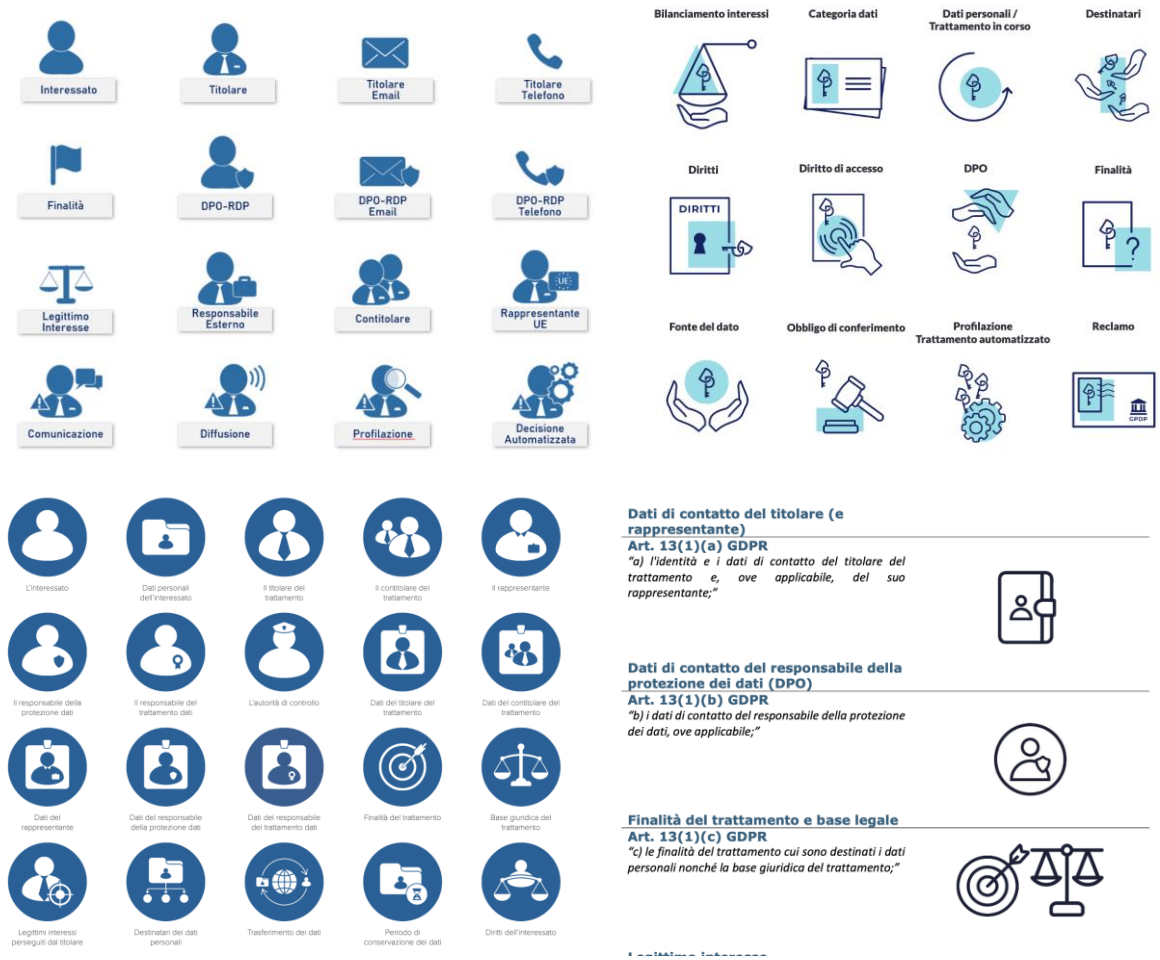

Figure 12 — Exemples d'icônes sélectionnées par la GDPD

727. Conclusion de section – L'information de la personne concernée fait l'objet de nombreuses interférences visant à influencer la personne concernée à adopter un comportement jugé bénéfique du point de vue du responsable de traitement ou de la société en général. Ces influences tendent à atténuer, réduire, voire anéantir, la liberté de consentement de la personne concernée, surtout lorsque l'information qui lui est délivrée est dessinée de telle façon que le procédé d'influence est invisible à ses yeux. La simplification de l'information apparaît essentielle dans ce cadre afin de doter la personne concernée de moyens de dépasser l'influence non désirée, ou l'exploitation d'une ignorance résiduelle, en vue d'exercer un consentement libre et éclairé. Cette simplification se concrétise à travers des éléments graphiques facilement identifiables et compréhensibles, qu'il s'agisse des résultats d'une évaluation impartiale précédente à travers le mécanisme de certification ou l'utilisation d'éléments graphiques directement destinés à faciliter la compréhension par la personne concernée des pratiques du responsable de traitement. La nécessité de simplifier l'information se complète de la nécessité de simplifier le consentement face à la multiplication des demandes de consentement.

Section 2 — La simplification nécessaire du consentement

728. Puisque le consentement de la personne concernée s'inscrit dans la logique d'*empowerement* de l'individu, la protection des données à caractère personnel dépend du comportement de l'individu face aux demandes de traitement de données à caractère personnel. Or, l'objectif annoncé par le RGPD d'une protection effective des données à caractère personnel suppose la réalité du consentement de l'individu en pratique. Ainsi, l'effort d'évaluation du RGPD est nécessaire pour en déceler les causes d'ineffectivité partielles[1554]. En l'espèce, la cause semble bien étrangère à la volonté et à l'objectif du législateur ; elle semble au contraire apparaître comme un effet contre-productif de la protection. En effet, la complexification du consentement de la personne concernée ne relève pas de la relation entre la personne concernée et le responsable de traitement, mais de la relation entre la personne concernée et les responsables de traitement. Dès lors, la difficulté ne naît pas du mécanisme de consentement, mais de la multiplication des acteurs auxquels la personne concernée devra répondre aux demandes de consentement, phénomène à l'origine de la fatigue du consentement (§1). La fatigue du consentement a ainsi montré la nécessité d'une simplification du consentement à travers une centralisation des consentements au sein du même outil (§2).

§1 — La fatigue du consentement

729. La fatigue a été définie comme un sentiment désagréable résultant de situations dans lesquelles la personne est incapable d'atteindre les buts qu'elle s'était fixés ou qu'elle attendait, ce qui a pour conséquence de provoquer chez cette personne un désillusionnement, de la frustration et un comportement relevant du cynisme[1555]. Se retrouvent dans cette définition les deux phases de la fatigue du consentement : l'hypersollicitation de la personne concernée (A) qui provoque par la suite une accoutumance auprès de la personne concernée (B).

A. L'hypersollicitation de la personne concernée

730. Dans ses lignes directrices sur le consentement, le G29 s'inquiète des effets contre-productifs qui peuvent résulter du RGPD, et des nombreuses demandes de consentement (notamment aux cookies) sur internet :

[1554] Pour saisir la signification de l'ineffectivité, v. CARBONNIER Jean, « Effectivité et ineffectivité de la règle de droit », *L'année sociologique*, Vol. 9, 1957-1958, p. 11.

[1555] CHOI Hanbyul *et al.*, «The role of privacy fatigue in online privacy behavior», *Computers in Human Behavior*, Vol. 81, avril 2018, pp. 42–51.

> « Dans le contexte numérique, de nombreux services nécessitent des données à caractère personnel afin de fonctionner. Les utilisateurs reçoivent ainsi chaque jour de nombreuses demandes de consentement auxquelles elles doivent répondre par un clic ou en balayant leur écran. Cela peut mener à une certaine lassitude : lorsque trop souvent rencontré, l'effet d'avertissement des mécanismes de consentement diminue. Il en résulte une situation où les informations de consentement cessent d'être lues. Cela constitue un grand risque pour les personnes concernées, dès lors que le consentement est généralement demandé pour des actions qui seraient illicites sans ce consentement ».[1556]

731. Cet argument appelé « fatigue du consentement » est devenu un sujet de recherche pour la doctrine, dont les travaux démontrent que les personnes concernées sont souvent « submergées » par le nombre de choix qu'elles doivent exercer, par le nombre d'options qui leur sont proposées et vont souvent « choisir l'option la plus facile, ou simplement accepter l'option par défaut »[1557]. La fatigue du consentement est le résultat de plusieurs facteurs parmi lesquelles la demande de choix excédant la capacité de choix des personnes concernées[1558], l'excès d'options disponibles[1559], ou encore les difficultés de compréhension des enjeux et de l'objet du consentement[1560]. Ces inquiétudes résonnent également du côté du législateur européen, dont la proposition de règlement e-Privacy constate que :

> « Les méthodes utilisées pour fournir des informations et obtenir le consentement de l'utilisateur final devraient être aussi conviviales que possible. Étant donné l'usage généralisé des cookies traceurs et autres techniques de suivi, il est de plus en plus souvent demandé à l'utilisateur final de consentir au stockage de tels cookies dans son équipement terminal. En conséquence, les utilisateurs finaux sont débordés par les demandes de consentement »[1561].

732. Le vocabulaire utilisé par la doctrine et le législateur traduit l'effet que la multiplication des demandes de consentement crée vis-à-vis de la personne concernée : les termes de fatigue et de lassitude, de sentiment d'être débordé, voire submergés constituent autant de termes s'inscrivant dans le champ lexical de l'émotion. Or, il a été démontré que les émotions négatives

---

[1556] Groupe de travail « Article 29 », WP259 rév.01, *op. cit.*, p. 20.
[1557] CHOI Hanbyul *et al.*, *op. cit.*
[1558] Cette surcharge de la capacité de la personne concernée à exercer des choix a donné naissance à la notion de « Consent transaction overload », SCHERMER Bart W., CUSTERS Bart, VAN DER HOF Simone, « The Crisis of Consent. How Stronger Legal Protection May Lead to Weaker Consent in Data Protection», *Ethics & Information Technology*, 2014, Vol. 15, p. 176. V. également sur le sujet VOHS Kathleen D. *and al.*, « Making Choices Impairs Subsequent Self-Control: A Limited-Resource Account of Decision Making, Self-Regulation, and Active Initiative », *Journal of Personality and Social Psychology*, 2008, Vol. 94, n° 5, p. 884.
[1559] WEITZNER Daniel J. *et al.*, «Information Accountability», *Communications of the ACM*, 2008, Vol. 51, n° 6, p. 84.
[1560] Cette surcharge d'information vis-à-vis à la capacité pour la personne concernée de la comprendre a donné naissance à la notion d'« *Information overload* ». SCHERMER Bart W., CUSTERS Bart, VAN DER HOF Simone, *op. cit.*, p. 177.
[1561] Commission européenne, 2017/0003 (COD), *op. cit.*, considérant 22.

des personnes influencent leur volonté de s'engager dans certaines actions, ce qui se traduit en termes de protection de la vie privée et de ses données à caractère personnel, en une réticence envers la gestion active et le contrôle de ses données à caractère personnel[1562]. Dès lors, une partie de la doctrine relie la fatigue du consentement au « paradoxe de la vie privée »[1563] : le partage des données à caractère personnel des personnes concernées ne se justifierait pas par leur souhait de les partager, mais par leur fatigue vis-à-vis du consentement au traitement de ses données à caractère personnel.

733. De plus, le consentement valide supposait un consentement libre, éclairé, spécifique et univoque. Puisqu'il s'agit d'un acte juridique qui lie la personne concernée tant qu'elle n'a pas retiré son consentement, il est important que la personne concernée puisse prendre conscience de la portée de cet acte. La thèse développée par Neil M. Richards et Woodrow Hartzog alerte sur le fait que le consentement est valide lorsqu'il n'est pas fréquemment (voire constamment) demandé, afin que nous puissions prendre la mesure des conséquences de notre consentement et être ainsi dans de bonnes conditions pour consentir consciencieusement et sérieusement[1564]. Dès lors, « submerger » les personnes concernées de demandes de consentement a pour conséquence de les dépouiller de leur capacité de contrôle et de rendre la protection des données à caractère personnel inefficace[1565]. La multiplication des demandes de consentement, si elle peut entraîner *a priori* un sentiment de contrôle accru chez la personne concernée, entraîne *in fine* le sentiment de surcharge de demandes. Il a pourtant été démontré que l'utilisation des outils de contrôle des données à caractère personnel n'est pas significativement influencée par la perception de contrôle, mais par la simplicité de celui-ci[1566]. De plus, une étude a démontré que la fatigue du consentement avait un effet plus important sur le comportement des personnes concernées que les préoccupations de celles-ci en matière de protection de leur vie privée[1567].

[1562] TANG Jie, AKRAM Umair, SHI Wenjing, « Why people need privacy? The role of privacy fatigue in app user's intention to disclose privacy based on personality traits», *Journal of Enterprise Information Management*, 2021, Vol. 34, n° 4, p. 1098.

[1563] V. NORBERG Patricia A., HORNE Daniel R. HORNE David A., *op. cit.*, pp. 100–126; LUTZ Christoph, HOFFMANN Christian Pieter, RANZINI Giulia, *op. cit.*, pp. 1168-1187 ; BRIGHT Laura F., LOGAN Ketly, LIM Hayoung Sally, «Social Media Fatigue and Privacy: An Exploration of Antecedents to Consumers' Concerns regarding the Security of Their Personal Information on Social Media Platforms», *Journal of Interactive Advertising*, 2022, Vol. 22, Issue 2, pp. 125–140.

[1564] RICHARDS Neil M., HARTZOG Woodrow, *op. cit.*, p. 1465.

[1565] Word Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage*, Industry Agenda, Février 2013, disponible sur http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf (consulté en mai 2021).

[1566] KEITH Mark J. *et al.*, « Privacy Fatigue: The Effect of Privacy Control Complexity on Consumer Electronic Information Disclosure », *International Conference on Information Systems (ICIS 2014)*, Auckland, Nouvelle-Zélande, 14-17 décembre 2014, disponible sur ssrn (consulté en mai 2021).

[1567] CHOI Hanbyul *et al.*, *op. cit.*, pp. 42-51.

734. Le phénomène d'hypersollicitation de la personne concernée est tellement présent sur l'environnement d'internet que la nécessité de le réguler a été reconnue par la Commission européenne[1568], le Parlement européen[1569], le Conseil de l'Union européenne[1570] et le Comité de protection des données[1571]. Le Conseil de l'Union européenne alerte notamment sur les effets d'une telle sollicitation qui peut avoir pour effet néfaste de provoquer l'accoutumance de la personne concernée aux consentements relatifs aux traitements de données à caractère personnel[1572].

B. L'accoutumance de la personne concernée

735. Selon le CNRTL, accoutumer quelqu'un à quelque chose signifie « lui faire prendre une habitude, le disposer à supporter quelque chose »[1573]. Cette définition implique que l'accoutumance s'exerce à l'égard d'une chose *a priori* désignée comme insupportable, désagréable. Appliquée au domaine de la protection des données à caractère personnel, l'accoutumance désignerait le fait de disposer la personne concernée à supporter l'exposition de ses données à caractère personnel (dans la mesure où l'on considère que la protection de ses données constitue le comportement supportable). Par exemple, la CNIL a alerté sur le fait que le développement incontrôlé des dispositifs de captation d'images « présente le risque […] de créer un phénomène d'accoutumance et de banalisation de technologie intrusives »[1574]. Le Sénat a également fait part de son inquiétude face aux applications de traçage dans le cadre de la lutte contre la pandémie de Covid-19, les sénateurs s'inquiétant « de l'accoutumance à la surveillance qui risque […] d'être instillée dans la population par la promotion étatique de ce type de dispositif numérique de traçage »[1575]. Concernant les acteurs privés, l'ancienne présidente de la CNIL, Isabelle Falque-Pierrotin mettait en exergue la limite à la tendance des

---

[1568] Commission européenne, COM/2017/010 final — 2017/03 (COD), *op. cit.*, considérant 22.
[1569] Parlement européen, *Rapport sur la proposition 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 »)*, 20 octobre 2017, Commission LIBE, 2017/003COD, amendement 24.
[1570] Conseil de l'Union européenne, 2017/0003 (COD), *op. cit.*, considérant 20a.
[1571] EDPB, *Déclaration du comité européen de la protection des données sur la révision de la directive ePrivacy et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques*, 25 mai 2018, p. 3.
[1572] Conseil de l'Union européenne, 2017/0003 (COD), *op. cit.*, considérant 20a.
[1573] CNRTL, « Accoutumer », *Lexicographie*, disponible sur https://www.cnrtl.fr/definition/accoutumer (consulté en mai 2021).
[1574] CNIL, « La CNIL appelle à la vigilance sur l'utilisation des caméras dites "intelligentes" et des caméras thermiques », 17 juin 2020, disponible sur https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras (consulté en mai 2021).
[1575] Sénat, « Mieux organiser la Nation en temps de crise », *Rapport d'information*, 8 juillet 2020, disponible sur http://www.senat.fr/rap/r19-609/r19-60935.html (consulté en mai 2021).

plateformes numériques de se présenter comme « une boussole face à l'abondance des contenus, à l'angoisse de la non-optimisation du temps »[1576], dans un modèle qui « semble "profiter" de l'individu, de sa "malléabilité", de sa tendance à s'accoutumer à la simplicité »[1577].

736. Dans le vocabulaire médical, l'accoutumance peut également être synonyme de dépendance[1578]. La dépendance sous-entend une « relation de subordination », un « manque d'autonomie »[1579]. Shoshana Zuboff, professeure émérite de Harvard, considère que « notre dépendance est au cœur du projet commercial de surveillance » et dénonce notre « engourdissement psychique qui nous rend insensibles au fait d'être géolocalisés, analysés, exploités ou modifiés »[1580]. Le phénomène d'accoutumance-dépendance va d'ailleurs provoquer des mutations profondes de nos sociétés. Par exemple, selon Pierre-Antoine Chardel et Armen Khatchatourouv, nous nous sommes tellement accoutumés à l'exposition de nos données à caractère personnel que nous avons abouti à de nouvelles formes de construction de soi à travers l'affirmation des autres[1581]. Notons que l'accoutumance-dépendance peut être volontairement créée par les responsables de traitement. Par exemple, dans son chapitre dédié au cycle de dépossession de Google Street View, Shoshana Zuboff décrit la stratégie volontairement déployée par Google pour que sa technologie déployée dépasse l'inquiétude des citoyens afin d'être « considérée comme "pratique", "utile" ou "formidable" »[1582].

737. Or, plus les citoyens sont accoutumés à l'exposition de leurs données à caractère personnel, plus les technologies intrusives seront facilement acceptées par eux et la technologie intrusive banalisée[1583]. Dans sa thèse dédiée à la surveillance diffuse, Clémence Codron constate qu'alors « qu'hier elle était une mesure d'exception visant à contrôler des populations présentées comme "à risque", la surveillance est aujourd'hui devenue banale et globale »[1584]. Une des conséquences principales de la banalisation de la technologie intrusive est l'argument consistant à affirmer « je n'ai rien à cacher » donc je n'ai rien à craindre d'une violation de ma

---

[1576] LINC, *op. cit.*, p. 1.
[1577] *Ibidem.*
[1578] OMS, « Prise en charge de l'abus de substances psychoactives », disponible sur https://www.who.int/substance_abuse/terminology/definition1/fr/ (consulté en mai 2021).
[1579] CNRTL, « Dépendance », *Lexicographie*, disponible sur https://www.cnrtl.fr/definition/d%C3%A9pendance (consulté en mai 2021).
[1580] ZUBOFF Shoshana, *op. cit.*, pp. 33–34.
[1581] CHARDEL Pierre-antoine, KHACHATOUROUV Armen, « Identité, différence et droit au secret à l'ère numérique », *Rue Descartes*, 2020/2, n° 98, pp. 103-117.
[1582] ZUBOFF Shoshana, *op. cit.*, pp. 253–263.
[1583] «Banaliser un objet. Le rendre courant, lui enlever toute originalité, le rendre vulgaire». CNRTL, « banaliser », *Lexicographie*, disponible sur https://www.cnrtl.fr/definition/banaliser (consulté en mai 2021).
[1584] CODRON Clémence, *La surveillance diffuse : entre Droit et Norme*, Thèse pour obtenir le grade de docteur en droit public, Dirigée par LAVENUE Jean-Jacques, Université de Lille, Droit et santé, 15 juin 2018, p. 49.

vie privée (principalement vis-à-vis de la surveillance étatique »). Cet argument, qui est partagé par un nombre conséquent d'Européens, implique désormais une présomption de suspicion envers la personne cherchant à couvrir ses traces numériques[1585].

738. Concernant l'exploitation des données à caractère personnel dans le cadre strictement privé, la banalisation de l'exposition des données à caractère personnel se traduit par l'inévitabilité du modèle économique construit autour de la marchandisation des données à caractère personnel. L'attractivité du modèle « cookie or cash », notamment acceptée par l'autorité de contrôle des données autrichienne[1586] et dont le développement en France résulte notamment de l'arrêt du Conseil d'État du 19 juin 2020[1587], met en exergue les mécaniques de la gratuité : soit vous acceptez de consentir aux cookies, soit vous compensez la perte financière liée à l'impossibilité d'exploiter vos données à caractère personnel en payant l'accès au contenu.

739. Enfin, l'accoutumance aux technologies intrusives crée un sentiment de résignation chez les personnes concernées. Une étude menée en 2015 sur la population américaine suggère en effet que les personnes concernées ne consentent pas à l'exploitation de leurs données à caractère personnel par ignorance ou en considérant qu'il s'agit d'une contrepartie juste au bénéfice envisagé : le consentement aux traitements de leurs données à caractère personnel proviendrait au contraire d'un sentiment de résignation, c'est-à-dire de la croyance que ces traitements sont inévitables[1588]. Cette étude est rejointe par la notion de « cynisme de la vie privée » définie par l'équipe de Christian Pieter Hoffman comme « une attitude d'incertitude, d'impuissance et de méfiance à l'égard du traitement des données à caractère personnel par les services en ligne, rendant le comportement de protection de la vie privée subjectivement futile »[1589]. La résignation ou le cynisme seraient ainsi des mécanismes d'adaptation des personnes concernées face à la perte de contrôle de leurs propres données à caractère personnel, l'inévitabilité de l'exposition de ces données, même avec la volonté de ne pas les publier[1590].

[1585] ERMOSHINA Ksenia, MUSIANI Francesca, « Hiding from Whom? Threat Models and In-The-Making Encryption Technologies», *Intermediality*, Issue 32, 2018, § 20.
[1586] FECI Nadia, « Hands up: cookies or cash? », *KU Leuven Centre for IT & IP* Law, 11 juin 2019, disponible sur https://www.law.kuleuven.be/citip/blog/hands-up-cookies-or-cash/ (consulté en mai 2021).
[1587] CE, 19 juin 2020, n° 434684, *op. cit.*.
[1588] TUROW Joseph *et al.*, *The Tradeoff Fallacy – How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation*, A Report from the Annenberg School for Communication, University of Pennsylvania, 2015, 26 p.
[1589] HOFFMANN Chritian Pieter *et al.*, « Privacy Cynism: A New Approach to the Privacy Paradox », *Cyberpsychology : Journal of Psychosocial Research on CyberSpace*, 2016, Vol. 10, n° 4, Article 7.
[1590] *Ibidem*.

740. Or, l'accoutumance aux technologies intrusives n'est pas anodine. En plus de provoquer une baisse de vigilance ou un découragement des personnes concernées dans la protection de leurs données à caractère personnel, l'accoutumance peut également avoir des conséquences en matière d'interprétation juridictionnelle des notions de vie privée et de protection des données à caractère personnel. Prenons l'exemple de la notion d'attente raisonnable en matière de protection de la vie privée et des données à caractère personnel. Le considérant 47 du RGPD propose une lecture de la compatibilité entre les intérêts légitimes du responsable de traitement et les intérêts ou libertés et droits fondamentaux de la personne concernée en se fondant sur les « attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable de traitement ». Ce critère a été notamment repris par le Conseil d'État qui, pour apprécier la licéité du traitement fondé sur l'intérêt légitime de la personne concernée, va s'intéresser, aux côtés de la nature des données traitées, des finalités et les modalités du traitement, aux « attentes que ces personnes peuvent raisonnablement avoir quant à l'absence de traitement ultérieur des données collectées »[1591]. L'attente raisonnable de la personne concernée fait également partie des critères établis par le RGPD pour déterminer si la finalité du traitement ultérieur est compatible avec les finalités pour lesquelles les données à caractère personnel ont été initialement collectées[1592]. La Cour de Justice de l'Union européenne a également utilisé le critère de l'attente raisonnable pour déterminer si un traitement de données à caractère personnel, en l'espèce un dispositif de vidéosurveillance, pouvait être autorisé[1593]. Dans sa décision du 14 mai 2020, la CNIL lie la notion d'attentes raisonnables aux principes de transparence et de loyauté résultant de l'article 5 du RGPD[1594]. Pour la Cour européenne des droits de l'homme, « l'attente raisonnable en matière de protection et de respect de la vie privée était un critère important » (« mais pas nécessairement décisif ») pour déterminer l'applicabilité de la notion de vie privée à des situations particulières[1595].

741. Or, comme le remarquent Antoinette Rouvroy et Yves Poullet, la notion volatile d'attentes raisonnables en matière de protection de la vie privée est que cette notion « n'est pas,

---

[1591] Conseil d'État, 10 décembre 2020, n° 429571, *op. cit*.
[1592] RGPD, 27 avril 2016, Considérant 50.
[1593] CJUE, 11 décembre 2019, *TK c. Asociația de Proprietari bloc M5A-ScaraA,* C-708/18, §58.
[1594] CNIL, 14 mai 2020, Délibération n° 2020-055 du 14 mai 2020 autorisant la société IMPLICITY à mettre en œuvre un traitement automatique de données à caractère personnel ayant pour finalité une étude portant sur le développement et la validation d'algorithmes de prédiction des crises de décompensation cardiaque chez les patients porteurs d'implants cardiaques connectés, intitulée « HYDRO » (Rectificatif) (Demande d'autorisation n° 920054).
[1595] CEDH, *Guide sur l'article 8, op. cit*, p. 25.

en réalité, indépendante du niveau de surveillance et de contrôle en place »[1596]. La conséquence de l'accoutumance à l'exposition des données à caractère personnel se déduit logiquement par des individus ne s'attendant pas à une protection large de leur vie privée[1597], transformant le critère de l'attente raisonnable en matière de protection de la vie privée en critère permissif. Wayne Unger considère que les attentes raisonnables en matière de protection de la vie privée présentent le défaut de ne pas être constantes dans le temps[1598]. L'universitaire démontre en effet qu'en matière de protection des données de santé, les attentes raisonnables en matière de protection de ces données se sont dégradées[1599].

742. Ainsi, il a été démontré que le consentement nécessite une protection supplémentaire afin de garantir que la personne concernée accorde son consentement sans influence inappropriée, qu'il s'agisse de l'exploitation de biais cognitifs par le design ou par l'accoutumance à des technologies particulièrement intrusives. Cependant, la domination cognitive subie par la personne concernée ne s'arrête pas au design trompeur ou à la promotion de technologies particulières. Malgré les protections du consentement par le RGPD, la personne concernée va pouvoir se trouver submergée par la demande de consentement, que ce soit du fait de sa complexité que de sa répétition.

§2 — La nécessaire centralisation du consentement au niveau de la personne concernée.

743. La centralisation du consentement est nécessaire à l'effectivité de la protection de la personne concernée : puisque la personne concernée est partie prenante de sa propre protection, le législateur doit tenir compte de ses capacités et de ses limites. Le droit étant toujours temporellement en retard sur les phénomènes économiques, il n'est pas étonnant de constater que le besoin a d'abord existé sur le marché (A) avant d'être finalement pris en compte dans les propositions législatives (B).

[1596] ROUVROY Antoinette, POULLET Yves, «The Right to Informational Self Determination and the Value of Self Development: Reassessing the Importance of Privacy for Democracy», *in* GUTWIRTH Serge *and al.* (dir.), *Reinventing Data Protection?*" Springer Netherlands, pp. 45–76.
[1597] *Ibidem.*
[1598] UNGER Wayne, « Katz and Covid-19. How a Pandemic Changed the Reasonable Expectation of Privacy», *Hastings Science and Technology Law Journal*, Volume 12, 2020, p. 78.
[1599] *Ibidem.*

A. L'existence d'un besoin sur le marché : le développement des systèmes de gestion des informations personnelles (PIMS) et autres technologies de gestion du consentement

744. Les PIMS sont des systèmes de gestion des données ayant pour vocation « de transformer le système centré sur les fournisseurs, en un système centré sur des personnes capables de gérer et de contrôler leur identité en ligne »[1600]. Les données concernant la personne concernée sont centralisées en une location, généralement grâce à un service de *cloud*[1601]. La caractéristique principale d'un système de gestion des informations personnelles (PIMS) est la gestion simplifiée du consentement de la personne concernée. Les PIMS sont donc des outils présentés sous la forme d'un tableau de bord, « permettant de visualiser l'ensemble des données détenues par un utilisateur avec la possibilité d'en moduler les différents accès »[1602]. Les PIMS ont également le potentiel de renforcer l'information de la personne concernée dans l'objectif de lui permettre de contrôler à la fois ces données, mais également ce que les données révèlent à son sujet[1603]. En effet, la perte de contrôle de la personne concernée sur ses données à caractère personnel résulte d'une dispersion de celles-ci, mais également de leur multiplication puisque les données peuvent résulter d'une collecte directe auprès de la personne concernée, d'une co-production avec d'autres personnes concernées (par exemple, les interactions sur un réseau social), de données produites par les responsables de traitement ou même de données produites automatiquement par le biais d'un logiciel, de sondes ou encore d'appareils connectés[1604].

745. L'objectif des PIMS semble séduire le législateur européen. Dans un billet de blog publié sur la plateforme Futurium de la Commission européenne, Malte Beyer-Katzenberger envisageait le futur d'internet comme un futur centré sur l'utilisateur et non plus sur les organisations, ayant opéré la transition du *B2C* au *Me2B*[1605]. La Commission européenne a, dans sa stratégie européenne des données, reconnu l'importance des outils de gestion des consentements et des PIMS qui « n'en sont encore qu'à leurs balbutiements », mais dont le « potentiel est important » et nécessite « un environnement favorable » à leur développement[1606]. En 2020, l'EDPS a dressé une liste d'exemples d'initiatives européennes

---

[1600] EDPS, *Avis 9/2016*, 20 octobre 2016, *op. cit.*, pp. 6-7.
[1601] ENISA, *Privacy and Security in Personal Data Clouds*, Final Report, novembre 2016, p.25.
[1602] ZOLYNSKI Célia, LE ROY Marylou, « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *Legicom*, 2017, p. 105.
[1603] EDPS, *Avis 9/2016*, 20 octobre 2016, *op. cit.*, p. 9.
[1604] ENISA, novembre 2016, *op. cit.*, p. 12.
[1605] BEYER-KATZENBERGER Malte, « What if the next generation of the internet was an "Internet of Me"? », *Futurium*, Commission européenne, 2 décembre 2016, disponible sur https://ec.europa.eu/futurium/en/blog/what-if-next-generation-internet-was-internet-me.html (consulté en décembre 2021).
[1606] Commission européenne, COM (2020) 66 final, *op. cit.*, pp. 12-13.

en matière de PIMS : Nextcloud, Solid, Mydex et MyData. Toutes revendiquent la possibilité de reprendre le contrôle sur ses données : Nextcloud promet la protection et le contrôle des données de l'utilisateur sans que rien ne fuît « pas même les métadonnées »[1607], Solid s'engage à permettre à la personne concernée d'avoir toutes ses données sous son contrôle[1608], Mydex a pour mission de donner aux individus le pouvoir sur leurs données[1609] et MyData a pour objectif d'améliorer l'autodétermination des individus au regard de leurs données à caractère personnel[1610]. L'intérêt de la Commission européenne et du comité européen sur la protection des données à propos des PIMS démontre bien l'existence d'un besoin sur le marché numérique. En 2016, l'EDPS invitait même la Commission à mettre en place des mécanismes incitatifs (telles que des projets pilotes ou des investissements) afin de permettre le développement de ces outils[1611].

746. Au niveau national, la philosophie gouvernant les PIMS a fait son apparition sous le nom de « Self Data ». Selon l'association FING (Fondation internet nouvelle génération), le *Self Data* se définit comme « la production, l'exploitation et le parage de données personnelles par les individus, sous leur contrôle et à leurs propres fins »[1612]. Par exemple, l'agglomération de La Rochelle est en train de tester un outil de *Self Data* permettant de calculer et réduire l'empreinte carbone et le budget de ses déplacements, à travers un outil permettant aux citoyens « de devenir maîtres de leurs données en les récupérant et exploitant sous leur contrôle et à leurs propres fins »[1613]. D'autres initiatives de *Self Data* ont été développées au sein de la Métropole de Lyon, Nantes Métropole et d'autres villes européennes (Gand, Barcelone, Amsterdam, Londres, Trento)[1614].

747. Enfin, un standard Internet dénommé « Platform for Privacy Preferences » (P3P) a été développé dans les années 1990 (et publié pour la première fois en 2002) afin de centraliser en un seul outil les gestions de consentement relatives aux cookies, à travers l'interface du

---

[1607] Next Cloud, https://nextcloud.com/fr_FR/.
[1608] Solid Project, https://solidproject.org/
[1609] MyDex, https://mydex.org/
[1610] MyData, https://mydata.org/
[1611] EDPS, *Avis 9/2016*, 20 octobre 2016, *op. cit.*, p. 17.
[1612] FING, *Self Data Territorial*, Feuille de route pour une implémentation du Self Data par les villes en France et en Europe, novembre 2021, p. 15.
[1613] AGREMOB, « Nos actions », *Agremob.com*, disponible sur https://agremob.com/nos-actions/ (consulté en décembre 2021).
[1614] Ministère de l'économie et des finances, Labo Société numérique, « Lyon, Nantes et la Rochelle jettent les bases du self data territorial », *labo.societenumerique.gouv.fr*, 18 juillet 2019, disponible sur https://labo.societenumerique.gouv.fr/2019/07/18/lyon-nantes-et-la-rochelle-jettent-les-bases-du-self-data-territorial/ (consulté en décembre 2021).

navigateur internet[1615]. Les créateurs de ce standard ont proposé aux sites internet de présenter leurs politiques de protection des données sous une forme compacte standardisée, lisible à la machine et facile à localiser[1616]. Ce protocole avait pour objectif de permettre aux personnes concernées de déterminer *a priori* ses préférences en matière de collecte des données dans leur navigateur, qui opérait ensuite automatiquement ce choix avec les sites internet présentant une politique de protection des données sous une forme compacte standardisée par le P3P[1617]. L'initiative reposait sur l'initiative privée et le volontariat de sites internet de présenter leur politique de protection des données sous forme P3P. Microsoft avait même décidé d'utiliser le P3P pour prendre des décisions relatives au blocage ou à l'acceptation de cookies à travers son navigateur Internet Explorer. Cependant, en 2010, une étude a évalué l'efficacité de l'initiative P3P sur 33 139 sites internet. L'étude a démontré que « de nombreux sites internet [adoptaient] des politiques de protection des données compactes afin d'éviter le blocage des cookies, mais ne [délivraient] pas des représentations exactes de leurs pratiques en matière de protection des données »[1618]. Parmi les cent sites les plus visités en 2010, vingt et un comportaient des erreurs parmi lesquels des sites appartenant au groupe Microsoft, mais également Facebook ou Amazon[1619]. La mauvaise évaluation des décisions relatives aux cookies était de plus aggravée par un filtre de cookies ne filtrant pas suffisamment les erreurs et manques d'information dans les politiques de protection des données compactes[1620]. De plus, une grande partie des sites internet se contentaient de copier-coller des exemples fournis sur internet permettant de contourner la protection fournie par le navigateur, l'un d'entre eux étant fourni par le site de support technique de Microsoft[1621].

748. L'absence de surveillance de l'application correcte du P3P a mené le standard à sa perte. Devant la doctrine libérale promouvant le P3P comme une alternative à une législation sur la protection des données à caractère personnel, le standard avait provoqué la méfiance des

---

[1615] W3C, « The Platform for Privacy Preferences1.1 (P3P1.1) Specification », *W3C Working Group Note*, 13 novembre 2006, Retiré le 30 août 2018, disponible sur https://www.w3.org/TR/P3P11/#P3P1.1 (consulté en janvier 2021).
[1616] *Ibidem.*
[1617] *Ibidem.*
[1618] LEON Pedro Giovanni *et al.*, « Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens », Pittsburg, Cylab, 10 septembre 2010, p. 6.
[1619] RICHMOND Riva, « A Loophole Big Enough for a Cookie to Fit Through », *The New York Times*, 17 septembre 2019, disponible sur https://bits.blogs.nytimes.com/2010/09/17/a-loophole-big-enough-for-a-cookie-to-fit-through/ (consulté en janvier 2022).
[1620] LEON Pedro Giovanni *et al.*, *op. cit.*, p. 6.
[1621] *Ibidem.*

défenseurs de la vie privée[1622]. En effet, aucun cadre technico-juridique précis ne permettait de vérifier l'application des préférences choisies par la personne concernée, de prouver leur violation et de sanctionner le responsable de traitement qui aurait volontairement contourné le système[1623]. Des initiatives, telles que le *Usable Privacy Project* tentent de combler les lacunes du P3P en créant des outils qui, grâce aux progrès du *machine learning* en matière d'analyse du langage, ont pour vocation de proposer des solutions de visualisation simplifiée des politiques de protection des données à travers l'analyse des politiques des données fournies par le responsable de traitement[1624]. Si de telles initiatives peuvent constituer une base intéressante pour le développement d'outils centralisés de gestion du consentement, elles ne permettent pour l'instant pas à la personne concernée de gérer, à travers un outil unique, l'ensemble de ses consentements.

749. Ainsi, l'expérience du P3P a dès lors démontré le besoin d'une intervention législative sur les outils de gestion du consentement, qui semble essentielle à la coopération de l'ensemble des responsables de traitement, afin de parvenir à l'objectif de doter la personne concernée d'outils de centralisation de ses consentements.

B. Le consentement centralisé et le Règlement ePrivacy

750. Le législateur européen a commencé à s'intéresser à la question du consentement centralisé lors des négociations du futur Règlement européen *e-Privacy*[1625]. La question de la fatigue du consentement est rapidement abordée par la Commission qui dès le considérant 22 de sa proposition de règlement constate que « les utilisateurs finaux dont débordés par les demandes de consentement »[1626].

751. Afin de remédier à cette problématique, la Commission propose une solution en deux parties. Premièrement, le règlement propose d'opérer une rationalisation des demandes de consentement à l'installation des cookies, en excluant une obligation de consentement « pour autoriser le stockage ou l'accès techniques dès lors qu'ils sont strictement nécessaires et proportionnés à l'objectif légitime de permettre l'utilisation d'un service spécifique expressément demandé par l'utilisateur final ». Dans ses lignes directrices relatives au

---

[1622] V. MURIS Timothy J., *Hearing before the Comitee on Commerce, Science and Transportation, United States Senate,* Second Session 25 avril 20,021, S. 2201, Online Personal Privacy Act; SCHWARTZ Ari, « Looking Back at P3P: Lessons for the Future », *Center for Democracy &* Technology, novembre 2009, p. 5.
[1623] NIGUSSE Girma, DE DECKER Bart, « Capabilities and Limitations of P3P », Katholieke Universiteit Leuven, Report CW 539, mai 2009, p. 33.
[1624] https://usableprivacy.org/learn_more
[1625] Commission européenne, COM/2017/010 final — 2017/03 (COD), *op. cit.*
[1626] *Ibidem.*

consentement, la CNIL propose une liste non exhaustive de cookies étant exemptés du recueil du consentement par l'article 82 de la loi informatique et libertés, parmi lesquels les « traceurs conservant le choix exprimé par les utilisateurs sur le dépôt des traceurs » ou encore « les traceurs destinés à garder en mémoire le contenu d'un panier d'achats sur un site marchand »[1627]. Une telle exemption de consentement permet la compatibilité du Règlement *e-Privacy* avec le RGPD dans la mesure où ces cookies sont nécessaires à l'utilisation d'un service et le consentement RGPD ne tolère pas le conditionnement de l'accès à un service au consentement de la personne concernée.

752. Deuxièmement, la Commission européenne propose d'établir la possibilité pour les personnes concernées de recourir « à des moyens techniques permettant de donner son consentement », notamment « en utilisant les paramètres appropriés d'un navigateur ou d'une autre application »[1628]. Elle semble tirer les leçons de l'expérience P3P en prévoyant au sein du règlement le fait que « 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 »[1629]. De manière intéressante, la Commission européenne lie le Règlement *E-privacy* au RGPD non seulement au niveau de la définition du consentement, mais également à l'obligation pour les navigateurs de filtrer les cookies autorisés sur le terminal de la personne concernée aux principes de protection de la vie privée dès la conception et par défaut. Définis à l'article 25 du RGPD, ces principes impliquent d'une part pour le responsable de traitement de réfléchir dès le moment de la détermination des moyens de traitements aux mesures appropriées pour garantir le respect des principes énoncés par le RGPD — et notamment la minimisation des données — et d'autre part, de garantir à la personne concernée que par défaut, seuls les traitements de données à caractère personnel nécessaires ne seront mis en œuvre. Cet effort d'harmonisation des législations est d'autant plus notable que la Commission supprime les difficultés auxquelles seraient confrontés les navigateurs dans cette démarche (à l'image du navigateur Internet Explorer de Microsoft) en forçant légalement les responsables de traitement à collaborer, dans la mesure où les choix renseignés dans le navigateur leur deviennent opposables. Ainsi, l'article 10 de la proposition de règlement dispose :

[1627] CNIL, Délibération n° 2020-01 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019, §49.

[1628] Commission européenne, COM/2017/010 final — 2017/03 (COD), *op. cit.,* § 22.

[1629] *Ibidem.*

> « Les logiciels mis sur le marché qui permettent d'effectuer des communications électroniques, y compris la récupération et la présentation d'informations sur Internet, offrent la possibilité d'empêcher les tiers de stocker des informations sur l'équipement terminal d'un utilisateur final ou de traiter des informations déjà stockées sur ledit terminal ».[1630]

En février 2021, le Conseil a approuvé un mandat de négociation du règlement e-privacy contenant les mesures proposées par la Commission pour « éviter la lassitude du consentement aux cookies ».

753. Le Comité européen de protection des données a exprimé son enthousiasme quant à la proposition de la Commission à laquelle il accorde un soutien « sans réserve »[1631]. L'EDPB, dans sa déclaration, insiste sur la nécessité d'une interface facile à utiliser et proposant un choix clair, qui soit « contraignante et exécutoire à l'égard de toutes les parties »[1632]. Le comité regrette uniquement la formulation, jugée insuffisamment neutre technologiquement (« logiciel ») qui permettrait aux responsables de traitement de contourner l'application de l'article 10 ou qui pourrait devenir obsolète à la suite de développements technologiques (à l'image de la directive 95/46/CE)[1633].

754. Des critiques ont été formulées à propos de la centralisation du consentement proposée par la Commission européenne. En effet, une telle mesure aurait un effet financier important sur l'économie de la publicité, le risque étant de voir un grand nombre d'utilisateurs refuser par défaut l'ensemble des dépôts de cookies sur leur équipement terminal[1634]. C'est ainsi qu'Étienne Drouard, Président de la Commission Enjeux réglementaires du Groupement des éditeurs des services en ligne (Geste) critique l'« inversion de la chronologie information/consentement » qui ne « permettrait plus de rechercher un équilibre entre les finalités légitimes poursuivies par l'entreprise et les droits des personnes »[1635]. Une lettre ouverte, signée par une cinquantaine d'acteurs privés européens, regrette également que le règlement

> « délègue la gestion des cookies aux interfaces de navigation, privant les internautes de décider en conscience de la relation qu'ils souhaitent entretenir avec chacun des sites. Cette évolution créerait un désavantage majeur pour les acteurs numériques européens, en réduisant leurs

---

[1630] *Idem,* Article 10 (1).
[1631] EDPB, 25 mai 2018, *op. cit.* p. 3.
[1632] *Ibidem.*
[1633] *Idem,* p. 4.
[1634] FISCHER Bogdan, MAZWSKI Milosk, « Analysis of processing electronic communication data on the basis on consent in the light of Council's e-privacy regulation proposal », *Journalism Research Review Quarterly*, 2017, n° 4, p. 97.
[1635] DROUARD Étienne, « La Proposition de Règlement ePrivacy se trompe de cible et de moyens », *Légipresse*, 2017, p. 291.

> capacités à collecter des revenus publicitaires avec des messages ciblés et pertinents. Elle diminuerait l'investissement possible dans un journalisme de qualité partout en Europe, en empêchant les éditeurs de presse et les médias d'établie une relation de confiance avec leurs lecteurs et de valoriser leurs contenus éditoriaux »[1636].

755. Ces critiques semblent cependant relever plus du lobbyisme politique que de la technique juridique. Contrairement à ce que Étienne Drouard affirme et à ce qui semble être sous-entendu dans la lettre ouverte, le Règlement *ePrivacy* ne viole pas les dispositions du règlement européen sur la protection des données en matière de consentement. L'inversion de la chronologie entre information et consentement est à relativiser dans la mesure où la personne concernée est informée des finalités du traitement avant de donner son consentement aux cookies au sein de son navigateur (par exemple, accepter ou refuser les cookies à des fins de mesure d'audience). Or, cette information brève n'est pas différente de l'information délivrée en première intention par les responsables de traitement dans leurs bannières de cookies (voir figure ci-dessous). Ainsi, la personne concernée peut continuer, si elle le souhaite, à s'informer sur la politique de protection des données si elle souhaite plus d'informations sur le traitement de ses données à caractère personnel.

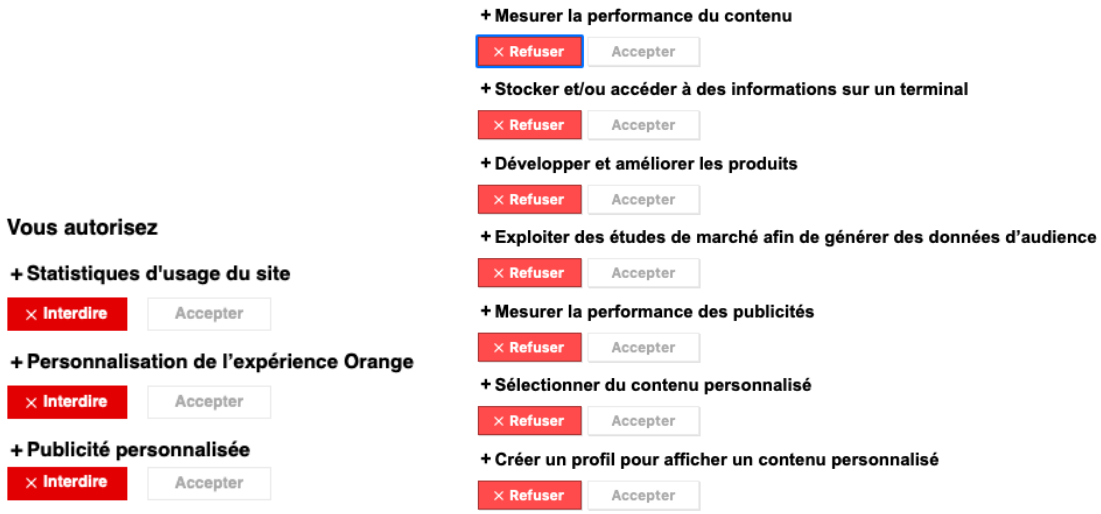

Figure 13 — Bannières de cookies d'orange.fr (à gauche) et de Geste.fr (à droite)

756. La question de l'inversion de la chronologie entre information et consentement pourrait s'avérer problématique dans la situation où la personne concernée accepterait par défaut tous les cookies, sans conscience de l'ampleur et des risques que ce consentement sans limite

[1636] Aikakausmedia *et al.*, « L'Europe ne peut pas se permettre de manquer la révolution des données », 7 mars 2018, disponible sur https://www.fftelecoms.org/nos-travaux-et-champs-dactions/reglementation-et-fiscalite/e-privacy-lettre-ouverte-europe/ (consulté en janvier 2022).

impliquerait pour la protection de ses droits fondamentaux. La Commission européenne semble être consciente de ce risque puisqu'elle précise que l'information de la personne concernée lors du paramétrage de son consentement aux cookies sur son navigateur doit « comprendre des renseignements utiles sur les risques qu'implique le consentement au stockage de cookies tiers sur l'ordinateur, parmi lesquels la conservation à long terme des historiques de navigation des personnes concernées et leur utilisation pour l'envoi de publicités ciblées »[1637]. Ainsi, la personne concernée pourra donner son consentement sur la base d'informations « pertinentes et transparentes »[1638]. Cette disposition permet notamment d'éviter les consentements de facilité de la personne concernée qui voit le refus des cookies comme un obstacle à sa navigation et lui permet de concilier son objectif premier d'accès au site internet avec la protection de ses données à caractère personnel.

757. De plus, l'argument concernant la mise en balance de la protection des données à caractère personnel avec les considérations économiques propres aux responsables de traitement relève d'une vision désormais datée de la proposition de règlement *ePrivacy*. Il est vrai que la proposition de règlement réduit la capacité pour les responsables de traitement de déposer des cookies sur le terminal de la personne concernée en limitant la possibilité de ne pas recourir au consentement et en permettant à la personne concernée de paramétrer en amont son consentement au dépôt de cookies[1639]. Cependant, le Conseil a, en février 2021, déclaré que « le fait de subordonner l'accès à un site web au consentement à l'utilisation de cookies à d'autres fins en tant que solution alternative à un verrou d'accès payant sera autorisé si l'utilisateur est en mesure de choisir entre cette offre et une offre équivalente du même fournisseur qui n'implique pas le consentement aux cookies »[1640]. La position du Conseil, similaire à la décision du Conseil d'État, est d'ailleurs vivement critiquée par le Comité de protection des données à caractère personnel qui invite le législateur européen à explicitement interdire les « cookies walls »[1641].

[1637] Commission européenne, COM/2017/010 final — 2017/03 (COD), *op. cit.*, considérant 24.
[1638] EDPS, 25 mai 2018, *op. cit.*, p. 4.
[1639] Commission européenne, COM/2017/010 final — 2017/03 (COD), *op. cit.*, considérants 22-24, Article 8 (1).
[1640] Conseil de l'Union européenne, « Confidentialité des communications électroniques : le Conseil arrête sa position sur des règles en matière de vie privée et de communications électroniques », *Communiqué de presse*, 10 février 2021.
[1641] EDPS, 25 mai 2018, *op. cit.*, p. 4.

CHAPITRE 2 – LA DIMENSION ÉCONOMIQUE DES DONNÉES À CARACTÈRE PERSONNEL

758. Le RGPD est un instrument juridique destiné à protéger les personnes concernées en leur qualité de citoyen, d'usager et surtout de consommateur[1642]. Le RGPD ne mentionne cependant jamais la personne concernée sous ces différentes formes : aucune référence n'est faite ni au citoyen, ni à l'usager, ni au consommateur. La référence au consommateur et au droit de la consommation est plus subtile. En effet, le RGPD est un instrument qui s'insère au sein du droit dérivé de l'Union européenne[1643] et dont les dispositions sont susceptibles de compléter, préciser ou se confronter aux dispositions d'autres instruments juridiques adoptés par le législateur européen. C'est ainsi que le RGPD s'applique sans préjudice de la directive 2000/31/CE sur le commerce électronique[1644], ses dispositions relatives à la déclaration sur le consentement sont complétées par la directive 93/13/CEE concernant les clauses abusives dans les contrats conclus avec les consommateurs[1645], et s'articule avec le règlement (UE) 1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale[1646].

759. Au sein du Règlement, la personne concernée voit ses droits renforcés dans le cadre de la démarche d'*empowerment*, et « le consentement est considéré par ses partisans comme la consécration suprême du "*Privacy self-management*" […] que justifie la responsabilisation

---

[1642] La dimension « consommateur » de la personne concernée n'est d'ailleurs pas ignorée de la doctrine, v. LIVENAIS Thomas, « Le règlement général sur la protection des données, outil d'émancipation des consommateurs face aux objets connectés », *Revue de l'Union européenne*, 2020, n° 634, p. 48 ; CASTETS-RENARD Céline, *Droit du marché unique numérique et intelligence artificielle*, Bruxelles, Bruylant, 2020, pp. 221-300 ; DELFORGE Antoine, GÉRARD Loïck, « Chapitre 2 — Le GDPR, source de solutions ou de blocages ? Une question de point de vue », *in* DE STREEL Alexandre, JACQUEMIN HERVÉ (dir.), *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, pp. 166-169 ; ZOLINSKY Célia, « Protection + Agentivité, la nouvelle équation pour penser les relations entre consommateurs et intelligences artificielles », *in* CANAL FORGUES ALTER Éric, HAMROUNI Maïa-Oumeïma (dir.), *Intelligence artificielle*, Bruxelles, Bruylant, 2021, p. 195.

[1643] Pour une vue d'ensemble, v. VERBRUGGEN Valérie, « Titre 1 — RGPD : cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne », *in* DE TERWANGNE Cécile, ROSIER Karen (dir.), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Paris, Larcier, 2018, 1e ed., pp. 27-31.

[1644] RGPD, 27 avril 2016, considérant 21 ; Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société d'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »). Cette directive affirme en son considérant 7 qu'elle a vocation à « garantir la sécurité juridique et la confiance du consommateur ».

[1645] RGPD, 27 avril 2016, considérant 42 ; Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs.

[1646] RGPD, 27 avril 2016, considérant 147 ; Règlement (UE) 1215/2012, 12 décembre 2012. Les articles 17, 18 et 19 régissent notamment la compétence territoriale des tribunaux judiciaires en matière de contrats conclus par les consommateurs.

d'un internaute devenu adulte »[1647]. En accordant un certain nombre de droits et en renforçant le consentement de la personne concernée, le RGPD a pour vocation la régulation des données à caractère personnel dans la relation horizontale présumée entre la personne concernée et le responsable de traitement. Or, si l'horizontalité des relations entre la personne concernée et le responsable de traitement se construit en opposition à la verticalité des relations entre le citoyen et l'État, il ne semble pas moins que la relation entre le consommateur et le responsable de traitement relève d'un rapport de force asymétrique (Section 1).

760. Ce rapport de force est à l'origine du constat selon lequel « l'état de consommateur impliquerait une certaine faiblesse qui mérite protection »[1648]. La création d'un droit de la consommation autonome du droit des contrats trouve alors toute sa justification : le droit des contrats régule la relation entre les cocontractants dans une relation d'égalité, le droit de la consommation régule la relation entre le consommateur et le professionnel « sur la considération de la faiblesse du consommateur par rapport au professionnel fournisseur de biens et de services »[1649]. Ces considérations sont d'autant préoccupantes pour le législateur que le consommateur va rencontrer des obstacles de nature financière et psychologique lorsqu'il va chercher à faire valoir ses droits[1650].

761. L'ubiquité des rapports entre consommateurs et professionnels et des rapports entretenus entre le responsable de traitement et les personnes concernées est à l'origine des phénomènes de préjudices de masse engendrés par des comportements abusifs de marché[1651]. La personne concernée est submergée par les phénomènes de masse que sont la consommation moderne et l'exploitation des données à caractère personnel[1652]. Pour se saisir des enjeux collectifs du droit de la consommation et de la protection des données à caractère personnel, l'Union européenne a ainsi accordé un intérêt grandissant aux mécanismes de recours collectifs[1653] qui ne semble pas encore suffisamment développé pour permettre une protection adaptée de la personne concernée (Section 2).

[1647] POULLET Yves, *La vie privée à l'heure de la société numérique*, Bruxelles, Larcier, 2019, p. 126.
[1648] PAYET Marie-Stéphane, *Droit de la concurrence et droit de la consommation*, Paris, Dalloz, Nouvelle Bibliothèque de Thèses, 2001, p. 44.
[1649] PELLIER Jean-Denis, *Droit de la consommation*, Paris, Dalloz, 3e édition, 2021, p. 1.
[1650] CALAIS-AULOY Jean, TEMPLE Henri, DEPINCÉ Malo, *Droit de la consommation*, Paris, Dalloz, Précis, 10e édition, 2020, p. 638 : PICOD Yves, PICOD Nathalie, *Droit de la Consommation*, Paris, Sirey, 5e édition, 2020, p. 539.
[1651] PICOD Yves, PICOD Nathalie, *Droit de la Consommation*, Paris, Sirey, 5e édition, 2020, p. 554.
[1652] CHAZAL Jean-Pascal, « Vulnérabilité et droit de la consommation », *Colloque sur la vulnérabilité et le droit*, Grenoble, 23 mars 2000, disponible sur hal.
[1653] RENIER Grégory, « Chapter 4 – Personal data class actions three years after the application of the GDPR », *in* JACQUEMIN Hervé (dir.), *Time to Reshape the Digital Society*, Bruxelles, Larcier, 2021, p. 135.

Section 1 — Un rapport de force économique déséquilibré

762. La protection des données à caractère personnel a la caractéristique particulière d'être particulièrement liée à des considérations économiques dont elle ne peut être cloisonnée. En effet, comme le rappelle Alain Rallet, « les données personnelles, tel Janus, ont deux faces. Une face vie privée et une face vie marchande »[1654].

763. L'évolution du marché numérique a vu l'émergence de plateformes numériques quasi monopolistiques, appelées « géants » d'internet ou du numérique, souvent désignées sous l'acronyme GAFAM (*Google, Apple, Facebook, Amazon, Microsoft*). D'autres géants ont ensuite émergé : les BATX (*Baidu, Alibaba, Tencent, Xiaomi*), surnommés les « GAFAM chinois » tant ils dominent l'espace internet chinois[1655] ou encore les NATU (*Netflix, Airbnb, Tesla, Uber*), dont la stratégie de disruption des modèles économiques leur permet d'afficher des taux de croissance impressionnants[1656]. Or, la position ultra-dominante de certaines de ces plateformes est problématique du point de vue du droit de la concurrence, ce qui se répercute ensuite sur la qualité de la protection des données à caractère personnel sur le marché (§1).

764. De plus, aujourd'hui, la valorisation des données à caractère personnel sur le marché a des effets directs qui peuvent être considérés comme néfastes, ou du moins contestables, sur la protection des données à caractère personnel. Nous nous intéresserons à la contestation de deux modèles économiques particuliers dont la généralisation nous semble rendre difficile la possibilité pour la personne concernée de consentir valablement (§2).

§1 — Le constat d'un déséquilibre inédit dans les rapports de force économiques sur le marché numérique

765. Si le déséquilibre du marché a des conséquences en matière de protection des données à caractère personnel, c'est parce que le droit de la concurrence a pour vocation de concilier à la fois les différents intérêts privés, les intérêts publics et privés, mais également les intérêts de la collectivité dans son ensemble. L'importance sociétale accordée au maintien d'une concurrence saine est telle qu'elle a conduit le Conseil d'État à qualifier la concurrence de

---

[1654] RALLET Alain, « Valoriser ses données personnelles ? 3 scénarios », disponible sur hal-archives ouvertes : https://hal.archives-ouvertes.fr/hal-01909650 (consulté en avril 2021).

[1655] France Culture, « L'expansion des BATX, les GAFAM chinois », *franceculture.fr*, 16 septembre 2019, disponible sur https://www.franceculture.fr/numerique/lexpansion-des-batx-les-gafam-chinois (consulté en mai 2021).

[1656] Forbes, « Les NATU vont-elles rejoindre les GAFAM ? », *Forbes.fr*, 12 février 2020, disponible sur https://www.forbes.fr/technologie/les-natu-vont-elles-rejoindre-les-gafam/ (consulté en mai 2021).

« composante de l'intérêt général »[1657]. L'autorité de la concurrence perçoit également en la concurrence une protection à la fois de l'entreprise, du consommateur et de la collectivité :

> « Comme dans le sport, la concurrence est un stimulant qui incite les entreprises à se dépasser, favorisant ainsi l'innovation, la diversité de l'offre et des prix attractifs pour les consommateurs comme pour les entreprises. La concurrence stimule ainsi la croissance et génère des gains substantiels pour la collectivité ! »[1658].

766. Parmi les intérêts à protéger se trouve la protection des données à caractère personnel, dont les acteurs européens appellent à la prise en compte dans les décisions concernant la concurrence[1659]. Cependant, la régulation décloisonnée du droit de la concurrence et de la protection des données à caractère personnel est rendue difficile par l'ampleur inédite de la distorsion de la concurrence sur le marché numérique (A).

767. De plus, si désormais le droit de la concurrence peut prendre en compte des éléments de protection des données à caractère personnel dans son analyse, il faudrait également prendre en compte les éléments de droit de la concurrence dans l'analyse de la protection des données à caractère personnel. En effet, l'autonomie de la volonté de la personne concernée n'est pas sans relation avec sa liberté de choix quant au responsable de traitement, liberté de choix désormais restreinte par l'absence de diversité des acteurs numériques (B).

A. Une distorsion de la concurrence difficile à réguler

768. La position dominante des grandes plateformes numériques ne fait plus aucun doute. En 2013, la ministre chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique concédait devant l'Assemblée nationale qu'à « l'évidence, le droit de la concurrence est peu efficace actuellement »[1660]. Depuis, les déclarations politiques appelant à une régulation du pouvoir économique et politique des géants du numérique se multiplient au niveau

---

[1657] SAUVÉ Jean-Marc, « À quoi sert la concurrence ? », *Allocation d'ouverture du colloque organisé par la revue Concurrences à l'Assemblée nationale le 4 décembre 2014*, disponible sur https://www.conseil-etat.fr/actualites/discours-et-interventions/a-quoi-sert-la-concurrence (consulté en mai 2021).

[1658] Autorité de la concurrence, « Les vertus de la concurrence », disponible sur https://www.autoritedelaconcurrence.fr/fr/les-vertus-de-la-concurrence (consulté en mai 2021).

[1659] DIXON Helen, « L'antitrust doit prendre en compte la protection des données personnelles », déclare la présidente de la CNIL irlandaise », *Les Echos*, 29 novembre 2019, disponible sur https://www.lesechos.fr/tech-medias/hightech/lantitrust-doit-prendre-en-compte-la-protection-des-donnees-personnelles-declare-la-presidente-de-la-cnil-irlandaise-1152341 (consulté en mai 2021).

[1660] Assemblée nationale, *Audition de Mme Fleur Pellerin, ministre déléguée auprès du ministre du redressement productif, chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique*, Commission des affaires européennes, 2 octobre 2013, disponible sur https://www.assemblee-nationale.fr/14/europe/c-rendus/c0084.asp#P5_269 (consulté en mai 2021).

français[1661] et européen[1662]. Dès lors, dans un contexte de déséquilibre de force entre la personne concernée et le responsable de traitement, le législateur s'est mobilisé afin de rétablir un équilibre sur le plan économique (1) et sur le plan politique (2).

1. La volonté réformatrice du législateur en matière de concurrence équitable

769. Les effets de la position dominante des grandes plateformes numériques étant un phénomène mondial, des projets de régulation des plateformes numériques sont également discutés aux États-Unis[1663] et en Chine[1664]. Le discours politique s'accompagne d'une mobilisation judiciaire autour des questions de distorsion de concurrence. En 2017, la Commission européenne a infligé à Google une amende de 2,42 milliards d'euros pour abus de position dominante « sur le marché des moteurs de recherche en conférant un avantage illégal à un autre de ses produits, son service de comparaison de prix »[1665]. En 2018, la Commission européenne inflige une nouvelle amende de 4,34 milliards d'euros à Google pour pratique anticoncurrentielle impliquant cette fois-ci son système d'exploitation Android : la Commission avait constaté que Google imposait « des restrictions illégales aux fabricants

[1661] En France, l'affaire de la fermeture du compte de Donald Trump par Twitter fait réagir les personnalités politiques françaises, parmi lesquelles Cédric O, Jean-Luc Mélenchon, François Ruffin, Xavier Bertrand, Marine Le Pen, ou encore Aurore Bergé. V. Ouest France, « Suspension du compte Twitter de Donald Trump : le pouvoir des GAFA inquiète la classe politique », *Ouest-France.fr*, 9 janvier 2021, disponible sur https://www.ouest-france.fr/monde/etats-unis/donald-trump/suspension-du-compte-twitter-de-donald-trump-le-pouvoir-des-gafa-inquiete-la-classe-politique-7112708 (consulté en mai 2021).

[1662] Les discours des commissaires européens se sont succédé et ont abouti au projet de *Digital Markets Act* (règlement sur les marchés numériques) et *Digital Service Act* (règlement sur les services numériques). Thierry Breton déclarait sur France Inter que « toutes les plateformes qui voudront venir chez nous devront respecter des règles » et que l'Europe sera « le premier continent de la planète qui va se doter de règles extrêmement claires pour protéger ce qui est important pour nous, mais aussi pour éviter les abus de position dominante ». BRETON Thierry, « Tout ce qui est interdit dans l'espace public sera aussi interdit dans l'espace online », France Inter, Le Grand entretien, 14 décembre 2020, disponible sur https://www.franceinter.fr/emissions/l-invite-de-8h20-le-grand-entretien/l-invite-de-8h20-le-grand-entretien-14-decembre-2020 (consulté en mai 2021). V. également The Guardian, « Margrethe Vestager: "We are doing this because people are angry", *TheGuardian.com*, Interview, 17 septembre 2017, disponible sur https://www.theguardian.com/world/2017/sep/17/margrethe-vestager-people-feel-angry-about-tax-avoidance-european-competition-commissioner (consulté en mai 2021) ; VON DER LAYEN Ursula, « Ce qui est interdit dans le monde réel doit être aussi interdit en ligne », *LeFigaro.fr*, 19 janvier 2021, disponible sur https://www.lefigaro.fr/vox/monde/ursula-von-der-leyen-ce-qui-est-interdit-dans-le-monde-reel-doit-etre-aussi-interdit-en-ligne-20210129 (consulté en mai 2021).

[1663] V. par exemple l'enquête menée par les législateurs européens sur les pratiques anticoncurrentielles sur le marché numérique. U.S. House of Representatives, *Investigation of Competition in Digital Markets*, Majority Staff Report and Recommendation, Subcommittee on Antitrust, Commercial and Administrative Law of the Committee of the Judiciary, 2020.

[1664] Les Echos, « La Chine se prépare à réguler ses propres géants du Web », *LesEchos.fr*, 7 janvier 2020, disponible sur https://www.lesechos.fr/tech-medias/hightech/la-chine-se-prepare-a-reguler-ses-propres-geants-du-web-1160949 (consulté en mai 2021).

[1665] Commission européenne, « Pratiques anticoncurrentielles : la Commission inflige à Google une amende de 2,42 milliards d'euros pour abus de position dominante sur le marché des moteurs de recherche en favorisant son propre service de comparaison de prix », *Communiqué de presse*, Bruxelles, 27 juin 2017, disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/IP_17_1784 (consulté en mai 2021).

d'appareils Android et aux opérateurs de réseaux mobiles, afin de consolider sa position dominante sur le marché de la recherche générale sur l'internet »[1666]. En 2019, l'Autorité de la Concurrence inflige une sanction de 150 millions d'euros à Google pour abus de position dominante[1667]. Le 20 octobre 2020, le gouvernement américain a lancé « la plus importante action judiciaire en plus de vingt ans » contre Google, pour atteinte au droit de la concurrence[1668]. Google n'est évidemment pas le seul « géant » concerné par la multiplication d'actions en justice pour pratiques anticoncurrentielles. En décembre 2020, la *Federal Trade Commission* a déposé une plainte contre Facebook pour « monopole illégal » et « conduite anti-concurrentielle », notamment à travers les acquisitions d'Instagram et de Whatsapp[1669].

770. La distorsion concurrentielle — alimentée par des pratiques anticoncurrentielles importantes et régulières — a une ampleur accrue par la nature de la concurrence numérique : les géants d'internet ne rivalisent pas pour obtenir des parts de marchés, mais des marchés entiers[1670]. Cette distorsion de la concurrence a eu la conséquence principale de créer des barrières à l'entrée aux nouveaux arrivants sur le marché. Or, si selon Emmanuel Combe, « les barrières à l'entrée ne sont jamais des montagnes insurmontables »[1671], une partie de la doctrine craint que, s'agissant des grands acteurs numériques, l'émergence de la concurrence soit rendue très difficile[1672]. La proposition de régulation du marché numérique de la Commission européenne constate elle-même « l'existence de barrières très hautes à l'entrée ou à la sortie », qui se traduit en des investissements très importants (non récupérables à la sortie) et l'accès limité voire « l'absence d'intrants clés » comme les données[1673]. La doctrine

---

[1666] *Ibidem.*

[1667] Autorité de la concurrence, « L'Autorité sanctionne Google à hauteur de 150 M€ pour abus de position dominante », 20 décembre 2019, disponible sur https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/lautorite-sanctionne-google-hauteur-de-150-meu-pour-abus-de-position (consulté en mai 2021).

[1668] Le Monde, « La justice américaine ouvre une procédure contre Google pour abus de position dominante », *LeMonde.fr*, 20 octobre 2020, disponible sur https://www.lemonde.fr/international/article/2020/10/20/la-justice-americaine-ouvre-une-procedure-contre-google-pour-abus-de-position-dominante_6056727_3210.html (consulté en mai 2021).

[1669] *Federal Trade Commission*, « FTC Sues Facebook for Illegal Monopolization », 9 décembre 2020, disponible sur https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization (consulté en mai 2021).

[1670] FUKUYAMA Francis *et al.*, «How to Save Democracy From Technology. Ending Big Tech's Information Monopoly », *Foreign Affairs*, janvier-février 2021, disponible sur https://www.foreignaffairs.com/articles/united-states/2020-11-24/fukuyama-how-save-democracy-technology (consulté en mai 2021).

[1671] COMBE Emmanuel, « Face aux GAFA, les autorités antitrust ont un rôle essentiel pour s'assurer que la compétition reste ouverte », *LeMonde.fr*, Tribune, 14 juin 2019, disponible sur https://www.lemonde.fr/idees/article/2019/06/14/emmanuel-combe-face-aux-gafa-les-autorites-antitrust-ont-un-role-essentiel-pour-s-assurer-que-la-competition-reste-ouverte_5476264_3232.html?xtmc=&xtcr=1 (consulté en mai 2021).

[1672] BOURREAU Marc, PERROT Anne, « Plateformes numériques : réguler avant qu'il ne soit trop tard », *Notes du Conseil d'analyse économique,* 2020/6, n° 60 ; FASQUELLE Daniel, « Le droit de la concurrence face au défi de l'économie numérique », *Cahiers de droit de l'entreprise*, n° 3, mai 2019, dossier 15.

[1673] Commission européenne, 2020/0374 (COD), *op. cit.*, considérant 3.

s'inquiète d'autant plus de ces barrières à l'entrée que le monopole des GAFAM entraîne une « clôture » des ressources intellectuelles et informationnelles[1674]. Dans un article d'Ugo Pagano consacré à la notion de « monopole intellectuel », les GAFAM ne sont pas critiqués uniquement en raison de leur pouvoir de marché issu de la concentration, mais également en raison du monopole légal qu'ils entretiennent sur certains éléments de la connaissance (à travers le mécanisme du brevet)[1675]. Ainsi, selon Daniel Fasquelle, l'apparition de ces acteurs « géants mondiaux » dotés de pouvoirs de marché d'une ampleur inédite entraîne l'apparition de nouveaux défis :

> « Un défi économique, en premier lieu, la crainte étant que ces "winner-take-all" préemptent leur marché et en excluent toute autre forme de concurrence. Un défi philosophique, ensuite, en raison du danger de confiscation de cet espace Internet censé être ouvert à tous par quelques-uns. Un défi politique, en troisième lieu, certains opérateurs devenant tellement puissants qu'ils en viennent à défier les États eux-mêmes. Vient se greffer sur ce dernier, un défi diplomatique, avec un bras de fer grandissant entre l'Europe, les États-Unis et bientôt la Chine. En dernier lieu, […] [un] défi juridique, le numérique posant la question de la crédibilité et de l'adaptabilité de la règle de droit face à ces phénomènes économiques nouveaux »[1676].

Dans ce cadre, les articles 101 et 102 du TFUE prohibant respectivement les ententes et les abus de position de dominante sur le marché ne suffisent plus à réguler le phénomène économique numérique. De l'aveu même de la Commission européenne, la régulation de la concurrence comme établie par les traités de l'Union européenne ne répondent « pas, ou pas efficacement, aux entraves observées sur le marché intérieur »[1677] résultant du comportement des « géants du numérique ». Pour résoudre cette impasse, la Commission européenne a notamment proposé deux « actes »[1678] législatifs, le *Digital Markets Act* et le *Digital Services Act*. Ces deux propositions visent d'une part à rétablir une concurrence loyale au sens traditionnel du terme et

---

[1674] SMYRNAIOS Nikos, « L'effet GAFAM : stratégies et logiques de l'oligopole de l'internet », *Communication & Langages*, 2016/2, n° 188, p. 61.

[1675] PAGANO Ugo, «Crisis of Intellectual Monopoly Capitalism», *Cambridge Journal of* Economics, 2014, Vol. 38, p. 1413.

[1676] FASQUELLE Daniel, *op. cit.*.

[1677] Commission européenne, 2020/0374 (COD), *op. cit.,* considérant 5 ; v. également le discours de Margrethe Vestager du 29 octobre 2020, Commission européenne, « Speech by Executive Vice-President Margrethe Vestager: Building trust in technology », 29 octobre 2020, disponible sur https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/speech-executive-vice-president-margrethe-vestager-building-trust-technology_en (consulté en août 2022).

[1678] Si elle n'a aucune valeur juridique dans l'ordre juridique européen, la reprise du terme « Act » dans le *Digital Markets Act* et le *Digital Service Act* montre la volonté de la Commission européenne de réguler l'ensemble des questions liées aux solutions numériques. En effet, le terme « *act* » semble résulter d'un glissement sémantique héritée de la *common law* dans lequel l'*Act* constitue la législation cadre tandis que la *regulation* (règlement) constitue le cadre législatif découlant du cadre législatif posé sans l'*Act.*

d'autre part, à rétablir les conditions d'une concurrence bénéfique vis-à-vis du consommateur, notamment en ce qui concerne la protection de ses données à caractère personnel.

771. Le rétablissement d'une concurrence loyale au sens traditionnel du terme a constitué le motif principal de l'établissement du *Digital Markets Act*. La proposition de règlement fait état de nombreuses pratiques des services de plateforme essentiels, et plus particulièrement les contrôleurs d'accès (*gatekeepers*), dont les effets résultent en une concurrence déloyale qu'il s'agisse de la relation de ces services de plateformes essentielles vis-à-vis des entreprises les utilisant et de leurs utilisateurs finaux[1679] ou encore vis-à-vis des opérateurs du marché existants ou nouveaux[1680]. Ce règlement s'inscrit comme un complément des articles 101 et 102 du TFUE en ce qu'il poursuit l'objectif est d'assurer la contestabilité des contrôleurs d'accès, indépendamment de leur comportement sur le marché[1681]. Ainsi, la Commission européenne a choisi de s'intéresser aux plus grands acteurs dont la contestabilité semble inatteignable plutôt que de s'intéresser au secteur numérique dans son ensemble. Dans la dernière version publiquement publiée, le *Digital Markets Act* définissait le contrôleur d'accès comme une plateforme essentielle, qui a un poids important sur le marché intérieur[1682], « assure un service de plateforme essentiel qui constitue un point d'accès majeur permettant aux entreprises

[1679] Le Commission européenne constate que les services numériques concernés par le DMA se caractérisent par « des économies d'échelle extrêmes, des effets de réseau très importants, la capacité de relier de nombreuses entreprises utilisatrices avec de nombreux utilisateurs finaux grâce au caractère multiface de ces services, des effets de verrouillage, l'absence de multihébergement ou l'intégration verticale ». De plus, leur position sur le marché comme unique ou très rare fournisseur de services les a placés dans la position de pouvoir « fixer facilement des conditions générales commerciales de manière unilatérale et préjudiciable pour leurs entreprises utilisatrices et utilisateurs finaux ». Commission européenne, 2020/0374 (COD), *op. cit.,* considérant 12.

[1680] La Commission européenne regrette que les contrôleurs d'accès soient « structurellement extrêmement difficiles à concurrencer ou à contester par des opérateurs du marché existants ou nouveaux, indépendamment de leur degré d'innovation et d'efficacité ». Commission européenne, Commission européenne, 2020/0374(COD), *op. cit.*,considérant 3.

[1681] Commission européenne, 2020/0374 (COD), *op. cit.,* 2020/0374 (COD), considérant 10.

[1682] Le seuil caractérisant le poids important d'une plateforme essentielle sur le marché intérieur a été un sujet de discussion et de négociation entre le Parlement européen et le Conseil. Initialement, la Commission européenne considérait le critère du poids important sur le marché satisfait si la plateforme essentielle réalisait un chiffre d'affaires annuel dans l'espace économique européen (EEE) supérieur ou égal à 6 500 000 000 euros au cours des trois derniers exercices ou si la capitalisation boursière moyenne ou la juste valeur marchande équivalente de l'entreprise atteint au moins 65 000 000 000 euros. L'amendement 80 proposé par le Parlement européen augmentait le seuil à un chiffre d'affaires annuel dans l'EEE supérieur ou égal à 8 000 000 000 euros au cours des trois derniers exercices ou une capitalisation boursière ou juste valeur marchande atteignant 80 000 000 000 euros. La dernière version publiée du DMA, résultat d'un accord interinstitutionnel entre le Parlement européen et le Conseil fixe les seuils à un chiffre d'affaires annuel dans l'EEE supérieur ou égal à 7 500 000 000 euros au cours des trois derniers exercices ou une capitalisation boursière ou juste valeur marchande atteignant 75 000 000 000 euros. Commission européenne, 2020/0374 (COD), *op. cit.,* article 3 (1) (a) et article 3 (2) (a) ; Parlement européen, *Rapport sur la proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques)*, Strasbourg, 30 novembre 2021, amendement 80 ; Conseil de l'Union européenne, *Proposition de Règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques) — Lettre du président du COREPER à la présidente de la Commission IMCO*, Bruxelles, 11 mai 2022, 2020/0374 (COD), article 3 (1) (a) et article 3 (2) (a).

utilisatrices d'atteindre leurs utilisateurs finaux »[1683] et détient, ou est amené à détenir selon toute probabilité, une position « solide et durable » dans ses activités[1684].

La particularité du DMA est que le règlement propose un nombre d'obligations *ex ante* qui s'appliquent aux contrôleurs d'accès non pas en raison des effets de leurs comportements, mais en raison de leur qualification en tant que contrôleurs d'accès[1685]. Cette approche présente l'avantage de permettre une plus grande célérité de l'action européenne en matière de concurrence du marché numérique européen, jusqu'alors caractérisé par une approche *ex post* demandant l'ouverture d'un long contentieux[1686]. Les obligations des contrôleurs d'accès sont diverses et comportent l'interdiction de la combinaison[1687] ou de l'utilisation croisée de données à caractère personnel[1688], l'interdiction de contrat d'exclusivité avec leur plateforme[1689] ou de contrat obligeant l'entreprise utilisatrice d'utiliser un de ses services accessoires[1690],

---

[1683] Le seuil établi pour déterminer si un service de plateforme essentiel constitue un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux a été établi à l'enregistrement de plus de 45 millions d'utilisateurs finaux actifs par mois établis ou situés dans l'Union et plus de 10 000 entreprises utilisatrices actives par an établies dans l'Union au cours du dernier exercice. La dernière version publiée du DMA adjoint à ces seuils une annexe précisant le mode de calcul de ces utilisateurs. Par exemple, l'annexe précise que le nombre d'utilisateurs actifs par mois ne doit pas prendre en compte les chiffres aberrants qui peuvent résulter d'une chute d'utilisateurs non anticipée sur le service sur un seul mois de l'année. Commission européenne, *Proposition de Règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques)*, Bruxelles, 15 décembre 2020, 2020/0374 (COD), article 3 (1) (b) et article 3 (2) (b) ; Conseil de l'Union européenne, *Proposition de Règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques) — Lettre du président du COREPER à la présidente de la Commission IMCO*, Bruxelles, 11 mai 2022, 2020/0374 (COD), article 3 (1) (b), article 3 (2) (b) et Annexe.

[1684] Le seuil établi pour déterminer si un service de plateforme essentiel détient ou est probablement amené à détenir une position stable et durable dans ses activités a été fixé à la réalisation du seuil constituant la qualification de point d'accès majeur au cours de chacun des trois derniers exercices. Commission européenne, 2020/0374 (COD), op. cit., article 3 (1) (c) et article 3 (2) (c) ; Conseil de l'Union européenne, 2020/0374 (COD), op. cit., article 3 (1) (c) et article 3 (2) (c).

[1685] KÖRBER Torsten, « Lessons from the Hare and the Tortoise: Legally Imposed Selfregulation, Proportionality and the Right to Defence Under the DMA », *NZKart*, 2021, p. 437 ; SCHWEITZER Heike, «The Art to Make Gatekeeper Positions Contestable and the Challenge to Know What is Fair: A Discussion of the Digital Markets Act Proposal, *ZEuP*, 2021, issue 3 pp. 522–523; Sénat, *Proposition de règlement relative aux marches contestables et équitables dans le secteur numérique (législation sur les marchés numériques) dite Digital Markets Act — Examen du rapport de la proposition de résolution européenne et de l'avis politique de Mmes Florence Blatrix Contat et Catherine Morin-Desailly*, Extrait du compte rendu de la réunion de la commission des affaires européennes du 7 octobre 2021, disponible sur https://www.senat.fr/ue/pac/EUR000006741.html (consulté en août 2022).

[1686] Par exemple, d'après Florence Blatrix Contat, « le droit de la concurrence permet de permet de sanctionner les comportements anti-concurrentiels, mais ses délais de mise en œuvre ne sont pas adaptés. De nombreuses amendes, parfois très élevées, ont été dispensées pour abus de position dominante. Toutefois, lorsque ces amendes sont imposées, la concurrence a déjà disparu. Ces sanctions, qui sont infligées après des enquêtes particulièrement longues, ne s'avèrent pas efficacité du point de vue de la contestabilité du marché ». Sénat, 7 octobre 2021, *op. cit.*

[1687] Commission européenne, 2020/0374 (COD), op. cit., article 5 (a).

[1688] *Idem*, article 6 (a).

[1689] *Idem*, article 5 (b).

[1690] *Idem*, article 5(e), article 5 (f). Cette disposition est complétée par l'article 6 (f) qui oblige le service de plateforme essentiel de permettre aux entreprises utilisatrices et fournisseurs de services accessoires d'accéder aux mêmes fonctionnalités que tout service accessoire proposé par le contrôleur d'accès, y compris en termes d'interopérabilité.

l'obligation de permettre aux entreprises utilisatrices de leurs services de communiquer directement avec les consommateurs[1691], ou encore l'interdiction des comportements d'autopréférence[1692]. La volonté du législateur d'établir des règles s'appliquant dès la qualification d'un service de plateforme essentiel en contrôleur d'accès peut entraîner des conséquences intéressantes en matière de protection des données à caractère personnel et plus particulièrement, garantir la correspondance entre le consentement donné par la personne concernée et la volonté de la personne concernée. S'intéresser à la captivité de la personne concernée dans un marché monopolistique permet en effet de garantir à la personne concernée la possibilité d'exercer un choix, puisque le même service sera proposé par plusieurs acteurs[1693]. De plus, prévenir de manière *ex ante* les distorsions de la concurrence par les acteurs dominants du marché permet d'anticiper les situations où l'acteur dominant sur le marché utilise le rapport de force qui lui est favorable pour imposer des conditions jugées inacceptables du point de vue de la protection des données à caractère personnel. Ces situations sont actuellement adressées *ex* post, comme le montre l'exemple de la décision du 7 février 2019 de l'autorité de la concurrence fédérale allemande. En effet, cette décision a mis en exergue la convergence entre le respect du droit de la concurrence et la protection des données à caractère personnel : en l'espèce, Facebook aurait abusé de sa position dominante sur les réseaux sociaux par l'accès à un nombre important de données à caractère personnel, en imposant aux personnes concernées des conditions non conformes au RGPD[1694]. On comprend ainsi que l'un des objectifs de la proposition de règlement est de faire du respect de la vie privée un avantage concurrentiel à travers une obligation de transparence accrue en matière de profilage, car la libre concurrence

[1691] *Idem,* article 5 (c).

[1692] *Idem,* article 6 (b) pour l'obligation de permettre à l'utilisateur final de désinstaller toute application préinstallé dans son service de plateforme essentiel, article 6 (c) pour l'obligation de permettre l'installation d'application logicielle et d'application interopérant avec ses systèmes d'exploitation, article 6 (d) pour l'interdiction d'accorder un traitement plus favorables de ses produits et services, article 6(e) pour l'interdiction de restreindre la capacité des utilisateurs finaux de s'abonner à d'autres applications et services accessibles sur la plateforme.

[1693] Le lien entre liberté du consentement et concurrence avait été mis en exergue dans les conclusions de M. Alexandre Lallet, selon qui la « clé » de la liberté du consentement « paraît résider dans la nature du besoin que l'utilisateur cherche à satisfaire et, surtout, dans l'existence, la disponibilité et l'accessibilité d'alternatives raisonnables permettant d'atteindre un résultat équivalent ». LALLET Alexandre, Conclusions, n° 434684, *op. cit.*.

[1694] Bundeskartellamt « Bundeskartellamt prohibits Facebook from combining user data from different sources », 7 février 2019, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (consulté en mai 2021) ; LINC, « Les données personnelles : un levier pour différents régulateurs », 5 juillet 2019, disponible sur https://linc.cnil.fr/en/node/114185 (consulté en mai 2021).

aurait des effets bénéfiques visant à élargir le choix des consommateurs, « ouvrant ainsi la voie à de nouvelles plateformes et à des services innovants et respectueux de la vie privée »[1695].

772. Cette nouvelle obligation de transparence est renforcée par la proposition de règlement sur les services numériques (*Digital Services Act* ou DSA) dont l'un des objectifs est de réguler la publicité en ligne en mettant à la disposition de la personne concernée des informations sur l'auteur de la publicité et les informations « relatives aux principaux paramètres utilisés pour déterminer qu'une publicité donnée a vocation à leur être présentée, accompagnées d'explications judicieuses sur la logique utilisée à cette fin, notamment lorsque celle-ci est fondée sur le profilage »[1696]. En effet, la proposition de DSA est la traduction de l'inquiétude du législateur quant aux effets du manque de transparence de la publicité comportementale. L'affaire *Cambridge analytica*[1697], la question des *deep fakes* ou encore l'utilisation de données sensibles afin de cibler les individus[1698] sont autant de questions adressées par le DSA. Dès lors, le DSA se présente comme une législation complémentaire au RGPD et autres législations européennes en matière de protection des données à caractère personnel[1699]. La logique prônée par la Commission européenne de protection des données à caractère personnel à travers le droit de la concurrence a d'ailleurs été largement accueillie par contrôleur européen de la protection des données, dont les recommandations visent principalement à renforcer le lien entre les deux propositions de règlement et les instruments de protection des données, à travers notamment l'utilisation de définitions communes[1700]. L'intérêt du DSA en ce qui concerne le consentement au traitement de ses données à caractère personnel réside particulièrement dans le fait que le

---

[1695] Commission européenne, 2020/0374 (COD), *op. cit.*, Résultats des consultations des parties intéressées et des analyses d'impact.

[1696] Commission européenne, 2020/0361 (COD), *op. cit.*, considérant 52.

[1697] Pour un aperçu des événements de l'affaire *Cambridge Analytica* qui sont adressées par la proposition de DSA v. BBC, « *Facebook fined £500,000 for Cambridge Analytica scandal* », *bbc.com*, 25 octobre 2018, disponible sur https://www.bbc.com/news/technology-45976300 (consulté en août 2022) ; BBC, « Fake Cambridge Analytica ad hits Facebook », *bbc.com*, 31 octobre 2018, disponible sur https://www.bbc.com/news/technology-46043578 (consulté en août 2022); DEBET Anne, « L'ICO, autorité de protection des données anglaise, prononce une sanction de 500 000 livres à l'encontre de Facebook dans l'affaire Cambridge Analytica », *Communication Commerce* électronique, n°12, décembre 2018, comm. 92 ; Le Monde, « Au Parlement européen, l'ombre du Brexit plane sur le débat consacré à Cambridge Analytica », *LeMonde.fr*, 23 octobre 2018, disponible sur https://www.lemonde.fr/pixels/article/2018/10/23/facebook-au-parlement-europeen-l-ombre-du-brexit-plane-sur-le-debat-consacre-a-cambridge-analytica_5373348_4408996.html (consulté en mai 2021).

[1698] GONZÁLEZ CABAÑAS José, CUEVAS Ángel, CUEVAS Rubén, « Facebook Use of Sensitive Data for Advertising in Europe », *27th USENIX Security Symposium*, 2018, pp. 479-495.

[1699] EDPS, *Avis n° 01/2021 concernant la proposition de législation sur les services numériques*, Bruxelles, 10 février 2021, p. 18.

[1700] EDPS, *Avis n° 01/2021 concernant la proposition de législation sur les services numériques*, Bruxelles, 10 février 2021, 28 p. ; EDPS, *Opinion 2/2021 on the Proposal for a Digital Markets Act*, 10 février 2021, 18 p.

législateur précise le régime applicable au profilage et à la publicité ciblée[1701]. D'habitude timide quant à la régulation de la publicité comportementale dont le caractère très lucratif constitue un modèle économique central des services numériques[1702], le législateur européen se décide à présenter une législation justifiée par la volonté de protéger les consommateurs de nouveaux risques — qu'ils soient individuels ou collectifs — créés par la généralisation de la publicité ciblée[1703]. La proposition de DSA de la Commission européenne crée des obligations de transparence renforcée à la charge des très grandes plateformes[1704] en ce qui concerne les systèmes de recommandation et la publicité en ligne. Le résultat du trilogue a abouti aux articles 24 et 24 (a) de la proposition de DSA[1705] régissant respectivement la publicité sur les plateformes en lignes et la transparence des systèmes de recommandation.

L'article 24 crée une obligation de transparence à la charge des plateformes en ligne de présenter en temps réel à chaque destinataire d'une publicité certaines informations de manière claire, concise et équivoque[1706]. Ces informations incluent le fait qu'il s'agit d'une publicité, la personne physique ou morale pour le compte de qui la publicité est diffusée, la personne physique ou morale qui a payé pour la publicité ainsi que des informations sur les paramètres principaux utilisés pour déterminer les destinataires de la publicité ainsi que, lorsque c'est applicable, les moyens de changer ces paramètres[1707]. Cette disposition a le potentiel de renforcer le consentement au traitement de ses données à caractère personnel en matière de publicité comportementale à deux égards. Premièrement, la disposition permet de renforcer le caractère éclairé du consentement en établissant une réelle prise de conscience de la personne concernée quant aux données à caractère personnel utilisées par les mécanismes de publicité comportementale. Une telle information n'est en effet pour l'instant pas requise par le RGPD, alors même que les mécanismes de publicité comportementale, à travers le système de mise aux

[1701] Si seule la question du profilage et de la publicité comportementale sera ici étudiée, le DSA contient de nombreuses dispositions complémentaires au RGPD telle que l'obligation de transparence quant à la méthode de modération des contenus (article 12) oui encore l'obligation d'établir un rapport de transparence sur les modalités de modération du contenu incluant, pour les plateformes en ligne, l'obligation de révéler les indicateurs de la précision des outils de prise de décision automatisée utilisés (articles 13 et 23).
[1702] v. *supra* n° 598-607.
[1703] MORAIS CARVALHO Jorge, ARGA E LIMA Francisco, FARINHA Martim, « Introduction to the Digital Services Act, Content Moderation and Consumer Protection », *Revista de Direito e Tecnologia*, Vol. 3, 2021, n°1, p. 74.
[1704] La proposition de DSA définit les très grandes plateformes comme des « plateformes en ligne fournissant leurs services à un nombre mensuel moyen de bénéficiaires actifs du service au sein de l'Union égal ou supérieur à 45 millions ». Commission européenne, COM (2020) 825 final, *op. cit.*, article 25 (1).
[1705] Originellement articles 29 et 30 de la proposition de règlement de la Commission européenne.
[1706] Conseil de l'Union européenne, 2020/0361 (COD), op. cit., article 24 (1).
[1707] Conseil de l'Union européenne, 2020/0374 (COD), op. cit., articles 24 (1) (a), 24 (1) (b), 24 (1) (ba), 24 (1) (c).

enchères et la multitude d'acteurs impliqués, constituent un traitement de données à caractère personnel particulièrement complexe à comprendre[1708]. Cependant, si la mise en place d'un tel mécanisme peut avoir des effets fortifiant le caractère éclairé du consentement, il sera essentiel d'observer la manière dont l'obligation de transparence est appliquée. En effet, il ne doit pas s'agir d'une obligation résultant en une sollicitation encore plus accrue de la personne concernée dans la mise en œuvre de sa protection en ligne[1709]. Deuxièmement, la disposition permet de renforcer le caractère libre du consentement en étayant l'accessibilité du retrait du consentement. En permettant à la personne concernée de changer à tout moment les paramètres utilisés pour la rendre destinataire d'une publicité comportementale, le législateur européen offre à celle-ci un moyen supplémentaire de contrôler l'usage de ses données à caractère personnel après leur collecte.

L'article 24a crée quant à lui une obligation de transparence à la charge des fournisseurs de plateformes en ligne de dévoiler, au sein de leurs conditions générales, les principaux paramètres utilisés dans leurs systèmes de recommandation, ainsi que les options offertes aux utilisateurs du service de modifier ou influencer ces paramètres, dans un langage simple et compréhensible[1710]. Cette obligation s'accompagne de celle de rendre les options permettant de modifier ou influencer les paramètres du système de recommandation accessibles à l'utilisateur à tout moment[1711]. À ce titre, l'article 24a est intéressant en ce qu'il crée un consentement hybride entre le consentement contractuel et le consentement au traitement des données à caractère personnel au sens du RGPD[1712]. Le consentement au traitement de données à caractère personnel ayant comme finalité d'offrir un système de recommandation au sein du service fourni relève de la base légale contractuelle. En effet, dans ce cadre, le système de recommandation est considéré comme faisant partie des éléments fondamentaux du contrat dans la mesure où il constitue l'élément différenciant d'un contrat de service déterminé par rapport à un autre contrat offrant le même service[1713]. Or, si les informations à fournir au sein

[1708] L'absence de connaissance du grand public du système de publicité comportementale constitue un obstacle substantiel au caractère éclairé du consentement des personnes concernées à un traitement de données à caractère personnel en vue de diffuser de la publicité ciblée. Par exemple, la Chambre contentieuse de l'APD a souligné que « le grand nombre de tiers, à savoir les fournisseurs adtech qui recevront et traiteront le cas échéant les données à caractère personnel des utilisateurs issues de la *bid request*, en fonction des préférences qu'ils ont saisies, n'est pas compatible avec la condition d'un consentement suffisamment éclairé, ni avec l'obligation de transparence plus large prévue par le RGPD ». APD, 2 février 2022, *op. cit.,* §472.
[1709] V. *supra* n° 730-743.
[1710] Conseil de l'Union européenne, 2020/0374 (COD), *op. cit.*, article 24a (1).
[1711] Conseil de l'Union européenne, 2020/0374 (COD), *op. cit.*, article 24a (3).
[1712] Pour comprendre la différence entre le consentement contractuel et le consentement RGPD, v. *supra* n° 307-323.
[1713] DPC, 6 octobre 2021, Draft Decision, *op. cit.*

des conditions générales de service relèvent du caractère éclairé du consentement contractuel, la possibilité de modifier ou influencer les paramètres du système de recommandation relève plutôt du caractère libre du consentement RGPD puisqu'il équivaut à un retrait — partiel ou total — de consentement de ses données à caractère personnel. Si l'analogie n'est pas parfaite, l'influence de la philosophie parcourant le consentement RGPD dans le champ d'application du consentement contractuel démontre la volonté du législateur européen de garantir aux personnes concernées le contrôle effectif de leurs données à caractère personnel.

773. Ainsi, si le paquet relatif aux activités numériques présente des dispositions prometteuses en matière de protection des données à caractère personnel, le DMA et le DSA présentent des limites importantes. Premièrement, aucun de ces règlements ne permet de régler le problème épineux du consentement en matière de publicité comportementale, alors même que l'adoption du Règlement *e-Privacy* semble au point mort. Or, si la philosophie du consentement RGPD a influencé le DSA au point de s'entremêler au consentement contractuel, les deux bases légales n'offrent pas le même degré de contrôle de ses données à caractère personnel. Deuxièmement, « l'abus de pouvoir algorithmique […] n'est pas traité de manière adéquate »[1714] par le paquet législatif, dont l'angle mort ne semble pas plus compensé par la proposition de règlement sur l'IA. Limiter le contrôle du pouvoir algorithmique à des questions de transparence ou de supervision humaine ne suffit pas à protéger la personne concernée, puisque celle-ci sera confrontée à la complexité des systèmes algorithmiques altérant sa compréhension des traitements concernés et au biais de confiance dans les systèmes algorithmiques, altérant l'efficacité de la supervision humaine de ces systèmes. Enfin, la puissance de la « *Big Tech* » est questionnée au-delà des questions purement économiques, dans la mesure où cette puissance est utilisée pour faire concurrence aux États. Par exemple, en octobre 2019, le Premier ministre Édouard Philippe prenait acte du contournement de la taxe sur les services numériques par Amazon et de la loi sur les droits voisins par Google, et déclarait qu'il « n'est pas acceptable qu'un acteur, aussi puissant soit-il — en l'occurrence, ces deux acteurs extrêmement puissants — puisse changer ses règles de publication de manière unilatérale pour contourner une obligation légale »[1715]. De plus, la capacité d'influence des plateformes numériques sur les personnes concernées est sérieusement questionnée. La

[1714] PONCE DEL CASTILLO Aída, « La stratégie numérique de l'Europe : centrée sur les personnes, sur les données ou sur les deux ? », *in* VANHERCKE Bart, SPASOVA Slavina (dir.), *Bilan social de l'Union européenne 2021. Les ambitions renaissantes par temps de redressement de l'Union*, Bruxelles, ETUI, 2022, p. 109.
[1715] Sénat, Question d'actualité au gouvernement n° 0934G de M. Claude Malhuret, publiée dans le JO Sénat du 3 octobre 2019, disponible sur https://www.senat.fr/questions/base/2019/qSEQ19100934G.html (consulté en mai 2021).

présidente de la Commission européenne, Ursula von der Leyen, appelait dans une lettre ouverte à « circonscrire démocratiquement ce pouvoir d'influence immense et encore largement incontrôlé dont jouissent les géants de l'internet »[1716]. L'affaire Cambridge Analytica, entreprise largement soupçonnée d'avoir influencé le résultat du vote sur le Brexit, a montré la capacité de certaines plateformes à modeler l'information de telle sorte qu'elles sont désormais capables de déformer le débat démocratique[1717]. Dans ce cadre, la régulation purement économique des activités numériques semble insuffisante à garantir la préservation des libertés démocratiques.

2. L'émergence du concept de souveraineté numérique

774. L'émergence du concept de souveraineté numérique — c'est-à-dire « la manière dont l'État affirme sa puissance dans un univers virtuel et dématérialisé » — dans le débat juridico-politique est la conséquence de la puissance inédite de ces plateformes devenues incontournables. La Commission nationale consultative des droits de l'homme (CNCDH) tire les leçons de l'affaire *Cambridge Analytica* en appelant à « une plus grande souveraineté numérique de l'Union européenne », permettant notamment d'imposer le respect des droits et libertés fondamentaux et de l'ordre public numérique[1718]. Le Conseil de l'Union européenne souligne l'importance de « renforcer la souveraineté numérique de l'UE et de veiller que celle-ci joue un rôle moteur dans les chaînes de valeurs numériques internationales stratégiques »[1719]. Les promoteurs de la souveraineté numérique s'opposent également à la remise en cause des monopoles régaliens tels que la monnaie, les activités de renseignement ou encore l'authentification de l'identité des personnes[1720]. L'exemple de la volonté de Facebook d'exercer des fonctions régaliennes est emblématique à travers l'authentification d'identité avec Facebook Connect[1721], l'institution d'organes similijuridictionnels avec la « Cour

---

[1716] VON DER LEYEN Ursula, « Ce qui est interdit dans le monde réel doit être aussi interdit en ligne », *LeFigaro.fr*, Tribune, 29 janvier 2021, disponible sur https://www.lefigaro.fr/vox/monde/ursula-von-der-leyen-ce-qui-est-interdit-dans-le-monde-reel-doit-etre-aussi-interdit-en-ligne-20210129 (consulté en mai 2021).
[1717] DEBET Anne, décembre 2018, *op. cit.* ; Le Monde, « Au Parlement européen, l'ombre du Brexit plane sur le débat consacré à Cambridge Analytica », *LeMonde.fr*, 23 octobre 2018, disponible sur https://www.lemonde.fr/pixels/article/2018/10/23/facebook-au-parlement-europeen-l-ombre-du-brexit-plane-sur-le-debat-consacre-a-cambridge-analytica_5373348_4408996.html (consulté en mai 2021).
[1718] CNCDH, *Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique*, publié au JORF n° 0126 du 3 juin 2018.
[1719] Conseil de l'Union européenne, *Façonner l'avenir numérique de l'Europe*, Conclusions du Conseil, Bruxelles, 9 juin 2020, 8711/20, p. 4.
[1720] G'SELL Florence, « Remarques sur les aspects juridiques de la "souveraineté numérique" », *Revues des Juristes de Sciences Po*, n° 19, octobre 2020, p. 13.
[1721] *Ibidem.*

suprême » des contenus[1722] ou encore la fonction de battre monnaie avec la cryptomonnaie Libra/Diem[1723]. Ainsi, la souveraineté numérique appelle particulièrement à des actions visant à limiter la dépendance des États envers ces « géants du numérique » et notamment les GAFAM. Différents leviers d'actions sont ainsi invoqués par les défenseurs de la souveraineté numérique afin de limiter la puissance des *big techs* et préserver le marché numérique.

775. Un premier levier d'action consiste à trouver des alternatives aux GAFAM dans les secteurs considérés comme stratégiques, et dans l'ensemble de la fonction publique, au profit d'entreprises plus locales ou *open source*. Par exemple, la France soutient le moteur de recherche Qwant et l'installe par défaut sur l'ensemble des systèmes informatiques de l'administration[1724]. Des plateformes indépendantes ou des alternatives *open source* sont privilégiées dans des domaines d'importance particulière comme les établissements publics hospitaliers[1725], la Gendarmerie nationale[1726] ou la recherche stratégique comme pour le CERN[1727]. Cependant, cette action est encore jugée insuffisante, la cohérence de la démarche ne s'étendant pas à l'ensemble des domaines importants[1728]. L'affaire de l'hébergement de la plateforme des données de santé (*Health Data Hub*) par la solution Azure de Microsoft a récemment relancé le débat sur la souveraineté numérique. En raison du volume important et de la sensibilité particulières des données ayant vocation à être hébergées dans le cadre du Health Data Hub (les données de santé relevant de l'article 9 du RGPD), « la CNIL a fait part de son souhait que son hébergement et les services liés à sa gestion puissent être réservés à des entités relevant exclusivement des juridictions de l'Union européenne »[1729]. Se fondant sur

---

[1722] Le Monde, « La "cour suprême" de Facebook va commencer à recevoir des réclamations d'utilisateurs », *LeMonde.fr*, 22 octobre 2020, disponible sur https://www.lemonde.fr/pixels/article/2020/10/22/la-cour-supreme-de-facebook-va-commencer-a-recevoir-des-reclamations-des-utilisateurs_6057009_4408996.html (consulté en avril 2021).

[1723] Les Echos, « Facebook recentre son projet de monnaie numérique sur le dollar », *Lesechos.fr*, disponible sur https://www.lesechos.fr/finance-marches/marches-financiers/facebook-recentre-son-projet-de-monnaie-numerique-sur-le-dollar-1315154 (consulté en mai 2021).

[1724] BÉVIÈRE-BOYER Bénédicte, « Faire face au risque de souveraineté numérique incontrôlée », *Dalloz IP/IT* 2020, p. 339.

[1725] *Ibidem.*

[1726] France Inter, « Logiciels libres et administrations : l'impossible mariage ? », *FranceInter.fr*, 15 septembre 2016, disponible sur https://www.franceinter.fr/info/la-bataille-des-logiciels-libres-reste-ca-mener-dans-l-administration (consulté en mai 2021).

[1727] BÉVIÈRE-BOYER Bénédicte, *op. cit.*, p. 339.

[1728] V. par exemple la tribune de Luc Rubellio : « On ne peut atteindre un but indéfinissable et nos dirigeants préfèrent jouer l'indépendance numérique de la France à pile (laisser-faire les GAFAM) ou face (espérer une alternative venant du marché) et ainsi gagner à tous les coups plutôt que de fixer des objectifs difficiles à quantifier et à atteindre pour sortir de cette indépendance hégémonique ». RUBELLIO Luc, « GAFAM : "L'indépendance de la France se joue à pile ou face" », *Marianne.net*, 3 mai 2021, disponible sur https://www.marianne.net/agora/tribunes-libres/gafam-lindependance-numerique-de-la-france-se-joue-a-pile-ou-face (consulté en mai 2021).

[1729] CNIL, « La Plateforme des données de santé (Health Data Hub) », *CNIL.fr*, 9 février 2021, disponible sur https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub (consulté en mai 2021).

l'arrêt de la CJUE invalidant le *Privacy Shield*[1730], le Conseil d'État avait considéré que le risque que Microsoft soit amené à transférer les données hébergées sur ses serveurs aux autorités américaines ne pouvait pas être « totalement exclu »[1731]. L'hébergement des données par Microsoft avait également été critiqué par le conseil d'administration de la Caisse nationale d'Assurance maladie (CNAM), pour qui « seul un dispositif souverain et uniquement soumis au RGPD permettra de gagner la confiance des assurés »[1732]. Les inquiétudes face à la dépendance de l'État vis-à-vis des *big techs* ont été résumées dans l'intervention de la sénatrice Anne-Catherine Loisier :

> « Alors que l'exécutif soutient l'impérieuse reconquête de notre souveraineté numérique, comment expliquer […] les choix faits ces derniers mois de confier des données stratégiques sensibles à des entreprises américaines ? »[1733]

La Sénatrice illustre ensuite ses propos non seulement par l'hébergement du *Health Data Hub* par Microsoft, mais également par les contrats d'aérospatial et de renseignement français confiés à l'entreprise américaine Palantir ou encore les prêts garantis par l'État confiés à Amazon Website[1734]. Ces contrats montrent la complexité de la mise en place de la souveraineté numérique puisque, selon Agrès Pannier-Runacher, ministre déléguée chargée de l'industrie, ces contrats révèlent une situation de nécessité et de dépendance : « d'un côté, des plateformes numériques étrangères qui proposent un haut niveau de service ; de l'autre, des briques technologiques françaises et européennes qui n'ont pas la capacité, à ce jour, d'offrir une solution complète de cloud souverain »[1735].

776. Un deuxième levier d'action est la construction « d'un tissu économique et entrepreneurial dynamique qui doit être protégé des abus de position dominante ou des situations monopolistiques suscitées par les grands groupes étrangers »[1736]. Plusieurs solutions sont alors envisagées. Premièrement, le démantèlement est régulièrement envisagé dans les réflexions sur l'économie numérique. Les parlementaires démocrates ont publié un rapport au

---

[1730] CJUE, 16 juillet 2020, C-311/18, *op. cit.*.
[1731] CE, ord. 13 octobre 2020, *Association Le Conseil national du logiciel libre et autres,* n° 444937, §17.
[1732] Next Impact, « L'assurance maladie se prononce contre Microsoft », *Nextimpact.com,* 22 février 2021, disponible sur https://www.nextinpact.com/lebrief/46167/health-data-hub-assurance-maladie-se-prononce-contre-microsoft (consulté en mai 2021).
[1733] LOISIER Anne-Catherine, *in Déclaration de Mme Agnès Pannier Runacher, ministre de l'industrie, sur la souveraineté économique de la France, au Sénat le 4 mai 2021,* Débat organisé au Sénat à la demande du groupe Les Républicains, disponible sur https://www.vie-publique.fr/discours/279908-agnes-pannier-runacher-04052021-souverainete-economique (consulté en mai 2021).
[1734] *Ibidem.*
[1735] PANNIER-RUNACHER Agnès, *in Déclaration de Mme Agnès Pannier Runacher, op. cit.*
[1736] Sénat, *Résolution européenne pour une réforme des conditions d'utilisation des mesures conservatoires prévues par le règlement (CE) n° 1/2003 du Conseil relatif à la mise en œuvre des règles de concurrence,* Session extraordinaire, 8 septembre 2017, n° 131.

Congrès américain recommandant le démantèlement de Google, Facebook, Apple et Amazon[1737]. Le démantèlement n'est cependant pas considéré comme la panacée face à l'hégémonie des GAFAM,[1738] car « nombreux sont ceux qui considèrent que, telle l'Hydre de Lerne, l'entreprise même scindée, poursuivrait le développement de sa puissance »[1739]. Le deuxième, la restriction de la possibilité pour des opérateurs dominants de se lancer sur certains marchés. Une enquête américaine sur la concurrence sur les marchés numériques conseille au gouvernement américain d'instaurer des séparations structurelles — c'est-à-dire l'interdiction pour un intermédiaire dominant d'opérer sur des marchés le plaçant en concurrence avec les entreprises dépendantes de son infrastructure — et des restrictions de secteurs d'activité — c'est-à-dire la limitation des marchés sur lesquels l'entreprise dominante peut s'engager[1740]. Notons que le *Digital Markets Act* prévoit « une mesure corrective structurelle, telle que la séparation juridique, fonctionnelle ou structurelle » en dernier recours, « s'il n'existe pas de mesure corrective comportementale qui soit aussi efficace » ou moins lourde pour l'entreprise concernée[1741].

777. Ainsi, il a été montré que le marché numérique fait face à des distorsions de la concurrence d'une ampleur inédite. Bien que les législateurs européens aient la volonté et l'ambition de réguler les plateformes numériques hégémoniques sur le marché, une telle régulation est à ce jour lacunaire et manque encore d'effectivité sur le marché malgré les différentes sanctions prononcées ces dernières années. Cette distorsion de la concurrence a pourtant des conséquences sur le consommateur, qui se confond souvent avec la personne concernée par les traitements de données à caractère personnel.

B. Les conséquences de la distorsion concurrentielle sur le consentement

778. Il faut dès à présent rappeler que « la concurrence ne trouve pas sa fin en elle-même, qu'elle n'est pas une fin en soi »[1742]. Les fins de la régulation des plateformes numériques ont

---

[1737] The Guardian, «The US government wants to break up Facebook. Good – it's long overdue », *TheGuardian.com*, 11 décembre 2020, disponible sur https://www.theguardian.com/commentisfree/2020/dec/11/us-government-break-up-facebook-long-overdue (consulté en mai 2021).

[1738] Les Echos, « Le droit à la vie privée rempart ultime contre l'hégémonie des GAFAM », *LesEchos.fr*, 9 décembre 2019, disponible sur https://www.lesechos.fr/idees-debats/editos-analyses/le-droit-a-la-vie-privee-rempart-ultime-contre-lhegemonie-des-gafam-1154706 (consulté en mai 2021) ;

[1739] Sénat, « Le devoir de souveraineté numérique », *Rapport n° 7 (2019-2020) de M. Gérard Longuet, fait au nom de la commission d'enquête, déposé le 1er octobre 2019*.

[1740] U.S. House of Representatives, *Investigation of Competition in Digital Markets, op. cit.*, p. 379.

[1741] Commission européenne, 2020/0361 (COD), *op. cit.*, Considérant 64.

[1742] MATHEY Nicolas, « Les finalités du droit de la concurrence. Essai de téléologie du droit », *Contrats Concurrence Consommation*, n° 12, décembre 2020, dossier 13.

été susénoncées : préservation de la souveraineté et du processus démocratique, intérêts du consommateur, soutien de l'innovation et enfin protection de la vie privée et des données à caractère personnel[1743].

779. En 2014, la CNIL appelait à prendre en compte la protection des données à caractère personnel dans « l'analyse de la concurrence sur les marchés numériques »[1744], démarche désormais entamée par les autorités de régulation de la concurrence. Cette analyse prend en compte le fait que la valorisation des données constitue aujourd'hui un avantage économique substantiel sur les marchés numériques. Cependant, les autorités espèrent voir le jour d'un autre lien entre la concurrence et la protection des données : faire de la protection des données à caractère personnel un objet de concurrence[1745]. Les acteurs économiques commencent désormais à intégrer ce type de logique dans leur stratégie commerciale. Par exemple, le grand cabinet d'audit et de conseil PricewaterhouseCooper (PwC) prédit qu'à l'horizon 2030, « une part croissante des consommateurs sera prête à quitter les entreprises auxquelles ils sont fidèles s'ils trouvent un concurrent capable de leur offrir de meilleures commodités, mais avec un contrôle et une valeur plus fiable de leurs données »[1746].

780. Cette tendance est accompagnée par les régulateurs, à l'égard de la CNIL qui propose aux *startups* de les accompagner à « faire de la protection de la vie privée un avantage concurrentiel » pour leur activité[1747]. En effet, une concurrence saine intégrant dans son analyse le paramètre de la vie privée peut avoir deux avantages importants pour l'effectivité de la protection des données à caractère personnel. Le premier est l'incidence directe de la concurrence : l'amélioration de l'offre[1748]. Appliqué aux marchés numériques, l'amélioration de l'offre signifie que le jeu de la concurrence puisse inciter les acteurs du marché numérique à proposer des solutions innovantes de plus en plus protectrices des données à caractère personnel[1749]. Le second, l'incidence indirecte est celui qui nous intéresse ici : le choix ouvert

---

[1743] La remise en cause de l'autonomie du droit de la concurrence n'est pas encore parfaitement achevée. Pour une vue d'ensemble sur cette problématique, v. MALAURIE-VIGNAL Marie *et al.*, « Comment appréhender les abus et l'utilisation des données dans la relation d'une plateforme avec ses partenaires contractuels », *Contrats Concurrence Consommation*, n° 12, décembre 2020, dossier 16.

[1744] CNIL, *Rapport* d*'activité*, 2014, p. 29.

[1745] *Ibidem.*

[1746] Next Inpact, « La vie privée, ça va payer », *Nextinpact.com*, 3 février 2021, disponible sur https://www.nextinpact.com/article/45876/la-vie-privee-ca-va-payer (consulté en mai 2021).

[1747] CNIL, « Startup : comment faire de votre conformité RGPD un avantage concurrentiel ? », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/startup-comment-faire-de-votre-conformite-rgpd-un-avantage-concurrentiel (consulté en mai 2021).

[1748] NIHOUL Paul, *La concurrence et le* droit, EMS Éditions, 2001, p. 26.

[1749] CNIL, *Rapport* d*'activité*, 2014, p. 29.

par la concurrence[1750]. Puisque le jeu de la concurrence implique une multiplicité d'acteurs rivaux, le consommateur en choisissant une entreprise écarte les autres, ce qui a pour conséquence que chaque entreprise chercherait à améliorer sa protection des données à caractère personnel afin de ne pas être écartée par la personne concernée. Ainsi, dans l'analyse stratégique externe des entreprises du marché numérique, le pouvoir de négociation du client sera augmenté du fait de l'augmentation du nombre de fournisseurs sur le marché[1751].

781. Le législateur européen a aussi fourni des efforts dans ce domaine en créant au sein du RGPD le droit à la portabilité des données. L'article 20 du RGPD dispose en effet que les personnes concernées ont le droit de recevoir « dans un format structuré, couramment utilisé et lisible par machine » leurs données à caractère personnel et de les transmettre à un autre responsable de traitement, ou d'exiger du responsable de traitement de transmettre directement à un autre responsable de traitement ses données à caractère personnel selon les mêmes modalités. Si ce droit ne s'applique *a priori* que lorsque les données ont été fournies par la personne concernée, l'interprétation du G29 a permis d'élargir le champ d'application des données concernées par la portabilité aux données « observées dans le cadre des activités des utilisateurs »[1752]. Ce droit s'inscrit dans la logique irriguant le RGPD de contrôle par les individus de leurs données à caractère personnel : non seulement l'utilisateur peut récupérer facilement l'ensemble de ses données, mais en plus il peut changer d'opérateur en cas d'insatisfaction[1753]. Le G29 le met lui-même en exergue : le droit à la portabilité est « une occasion de "rééquilibrer" la relation entre les personnes concernées et les responsables du traitement »[1754], autrement dit, d'augmenter le pouvoir de négociation de la personne concernée par rapport au responsable de traitement. De plus, en permettant aux utilisateurs de changer plus facilement d'opérateur, le droit à la portabilité des données « permet de dépasser le verrouillage des marchés pour les nouveaux entrants »[1755]. Le droit à la portabilité du RGPD a vocation à être renforcé par le règlement sur les marchés numériques. Dans le projet proposé par la Commission européenne en décembre 2020, le champ d'application du droit à la portabilité est élargi à « toutes les autres données, à différents niveaux d'agrégation, qui peuvent

---

[1750] NIHOUL Paul, *op. cit.* p. 26.
[1751] Pour comprendre la théorie des cinq forces de porter et leurs effets en termes d'avantages concurrentiels, v. CADIAT Anne-Christine, MICHAUX Stéphanie, *Les 5 forces de Porter. Comprendre les sources des avantages concurrentiels,* 50 minutes, 2015, 58 p.
[1752] Groupe de travail « Article 29 », *Lignes directrices relatives au droit à la portabilité des données,* adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, WP 242 rev.01, p. 12.
[1753] ZOLYNSKI Célia, LE ROY Marylou, 2017, *op. cit.,* p. 105**.**
[1754] Groupe de travail « Article 29 » WP 242 rev.01, *op. cit.,* p. 4.
[1755] BERTRAND Brunessen, « Chronique Droit européen du numérique — Perfectibilité de la protection des données personnelles », *RTD Eur.* 2021, p. 143.

être requises pour permettre effectivement cette portabilité »[1756]. De plus, l'article 6 crée une obligation à la charge des contrôleurs d'accès d'assurer « la portabilité effective des données générées par l'activité d'une entreprise utilisatrice ou d'un utilisateur final » et de fournir « aux utilisateurs finaux les outils facilitant l'exercice de cette portabilité, conformément au règlement (UE) 2016/679, dont la fourniture d'un accès continu et en temps réel »[1757]. Notamment, le DMA a pour objectif de garantir le droit à la portabilité, droit dont l'effectivité est dépendante de l'interopérabilité des systèmes et de l'homogénéité des formats[1758].

782. Or, si les initiatives de rééquilibrage du jeu concurrentiel semblent prometteuses, nous ne sommes pas convaincus que le jeu de la concurrence actuel confère actuellement à la personne concernée un pouvoir de négociation important sur plusieurs domaines gourmands en données à caractère personnel.

783. En effet, le marché numérique souffre toujours de la « tendance naturelle à la concentration des marchés autour de plateformes bénéficiant d'un pouvoir structurant et difficilement contestables »[1759]. Cette tendance est bien expliquée par les économistes : elle résulte de plusieurs facteurs concomitants, dont les économies d'échelle et les effets de réseaux[1760]. Or, si certains économistes adeptes des théories de Joseph Schumpeter attendaient de la théorie de la « destruction créatrice » un renouvellement des acteurs par la stimulation de l'innovation (l'innovation crée un monopole qui est par la suite contesté par une nouvelle innovation la rendant obsolète), l'Assemblée nationale constate que « la prophétie schumpétérienne ne s'est pas réalisée et la concentration des marchés atteint des niveaux inquiétants, signe de dysfonctionnements concurrentiels »[1761]. Les chiffres sont en effet vertigineux : Google concentre environ 90 % des parts de marché sur les moteurs de recherche et 86 ; 7 % des parts de marché des systèmes d'exploitation mobile (avec le système Android), Facebook et Google concentrent 85 % du marché européen de la publicité en ligne[1762]. De plus, ces acteurs déploient des stratégies hégémoniques ayant pour objectif de les rendre incontournables, combinant à la fois une stratégie de concentration verticale et une stratégie de

---

[1756] Commission européenne, 2020/0374 (COD), *op. cit.*, considérant 54.
[1757] *Idem,* article 6 (1) (h).
[1758] BRUGUIÈRE Jean-Michel, « La nature du droit à la portabilité des données personnelles », *in* GLEIZE Bérangère, MAFFRE-BAUGÉ Agnès (dir.), *La propriété intellectuelle renouvelée par le numérique*, Paris, Dalloz, 2020, p. 150.
[1759] Assemblée nationale, *Rapport d'information sur les plateformes numériques déposé en application de l'article 145 du Règlement par la Commission des affaires économiques*, présenté par Mme Valérie FAURE-MUNTIAN et M. Daniel FASQUELLE, députés, 24 juin 2020, n° 3127.
[1760] BOURREAU Marc, PERROT Anne, *op. cit.*, p. 1.
[1761] Assemblée nationale, 24 juin 2020, n° 3127, *op. cit.*.
[1762] *Ibidem.*

concentration horizontale[1763]. Ainsi, non seulement l'entreprise va chercher à concentrer sous un pouvoir de décision unique l'ensemble des activités de la chaîne de production (du data center au service en passant par les infrastructures, équipements, systèmes d'exploitation, logiciels, etc.), mais l'entreprise va aussi chercher à concentrer l'ensemble des biens ou services substituables sur le marché[1764]. Par conséquent, la Commission européenne a encore beaucoup d'efforts à fournir pour rééquilibrer le marché (notons qu'en limitant le pouvoir des « contrôleurs d'accès » sur les entreprises utilisatrices de leurs services et infrastructures, le *Digital Markets Act* pourra probablement participer au rééquilibrage du marché[1765]).

784. De plus, bien que le droit à la portabilité des données soit une avancée notable dans le rééquilibrage de la concurrence sur les marchés numériques, il faut tout de même garder à l'esprit que son champ d'application est limité par plusieurs facteurs. La première limite est que le droit à la portabilité consistant à exiger d'un responsable de traitement qu'il transmette les données à caractère personnel à un autre responsable de traitement est subordonné au fait que cette transmission soit « techniquement possible ». En l'absence d'exigence d'interopérabilité des plateformes numériques, cette limite peut faire reposer l'effectivité de la portabilité des données sur la bonne foi des acteurs du marché numérique. Or, la publication du Livre blanc sur la portabilité par Facebook en 2019 pose de sérieux doutes sur la volonté des opérateurs de garantir ce droit aux personnes concernées[1766]. Encourageant la confusion du droit à la portabilité avec le partage de données avec des tiers, le Livre blanc s'attaque à la portabilité et soutient une application limitée de ce droit en mobilisant des notions telles que la sécurité des données ou encore le droit à la protection des données des tiers[1767]. En réaction, La Quadrature du Net et 75 organisations de défense des libertés, organisations professionnelles, hébergeurs et fournisseurs d'accès internet associatifs ont publié une « lettre commune pour l'interopérabilité des grandes plateformes en ligne », afin que les utilisateurs ne se trouvent pas « captif[s] d'une plateforme » et puissent « librement la quitter, sans perdre ses liens sociaux, et de continuer à communiquer avec [leurs] contacts »[1768]. Le rapport de Jacques Crémer, Yves-Alexandre de Montjoye et Heike Schweitzer publié par la Commission européenne en 2019

[1763] SMYRNAIOS Nikos, *op. cit.*, pp. 61-83.
[1764] *Idem*, pp. 74-48.
[1765] Pour une vue d'ensemble des dispositions du *Digital Markets Act*, v. Next Inpact, « Le Digital Markets Act expliqué ligne par ligne », *Nextinpact.com*, 25 janvier 2021, disponible sur https://www.nextinpact.com/article/45317/le-digital-markets-act-explique-ligne-par-ligne (consulté en mai 2021).
[1766] EGAN Erin, *Charting a Way Forward – Data Portability and Privacy*, Facebook, septembre 2019, 21 p.
[1767] *Ibidem.*
[1768] La Quadrature du Net, « Pour l'interopérabilité des géants du web : lettre commune de 75 organisations », *Laquadrature.net*, 21 mai 2019, disponible sur https://www.laquadrature.net/2019/05/21/pour-linteroperabilite-des-geants-du-web-lettre-commune-de-45-organisations/ (consulté en mai 2021).

préconisait d'instaurer en faveur des plateformes dominantes une présomption de devoir d'interopérabilité (*presumption of a duty to ensure interoperability*) : une telle présomption permettrait de toujours évaluer la possibilité d'assurer le droit à la portabilité des données par rapport aux contraintes techniques d'interopérabilité, tout en présumant l'absence de telles difficultés techniques pour les plateformes numériques dominantes[1769]. Nous rejoignons ainsi le constat de Bertrand Brunessen : le droit à la portabilité des données nécessite l'adoption de nouveaux outils, soit de gestion globale des données à caractère personnel, soit de mesures contraignantes en matière d'interopérabilité des interfaces et des formats[1770].

785. La deuxième limite est que le champ d'application des données à transmettre est limité et juridiquement nébuleux et incertain. L'article 20 du RGPD précise que le droit à la portabilité concerne les données à caractère personnelles fournies par la personne concernée et la concernant, et dont le traitement repose sur le consentement ou sur l'exécution d'un contrat. Or, selon que l'on ait une interprétation restrictive (à l'image du Livre blanc de Facebook[1771]) ou extensive de ces dispositions, la portée et l'effectivité du droit à la portabilité peuvent énormément varier[1772]. À cet égard, le G29 propose une interprétation extensive du champ d'application du droit à la portabilité. En effet, premièrement, le G29 appelle à « ne pas interpréter de manière trop restrictive » la notion de données à caractère personnel concernant la personne concernée afin de permettre l'exercice du droit à la portabilité de services pouvant inclure les données des tiers tels que les services de téléphonie, de messagerie, etc[1773]. Cette interprétation extensive s'accompagne d'une garantie d'obligation pour la plateforme importatrice des données de ne pas traiter ces mêmes données « pour une finalité qui porterait atteinte aux droits et libertés des tiers »[1774] (le G29 préconise notamment aux responsables de traitement importateur de garantir aux tiers l'exercice de leurs droits RGPD)[1775]. Deuxièmement, le G29 propose d'élargir la notion de données fournies par la personne concernée aux « données observées fournies par la personne concernée grâce à l'utilisation du service ou du dispositif »[1776] : la notion de données « fournies » ne suppose pas forcément une

[1769] CRÉMER Jacques *et al.*, *Competition policy for the digital era*, Commission européenne, 2019, p. 4.
[1770] BRUNESSEN Bertrand, « Chronique Droit européen du numérique — Perfectibilité de la protection des données personnelles », *RTD eur.*, 2021, p. 143.
[1771] Notamment sur la notion de données à caractère personnel concernant la personne concernée. V. EGAN Erin, *op. cit.*, 21 p.
[1772] DE HERT Paul *et al.*, «The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services», *Computer Law & Security Review*, Vol. 34, Issue 2, avril 2018, p. 194.
[1773] Groupe de travail « Article 29 », WP 242 rev. 01, *op. cit.*, p. 11.
[1774] *Ibidem.*
[1775] *Idem*, p. 15.
[1776] *Idem*, pp. 11-12.

action volontaire de la personne concernée. Dans un souci de ne pas interférer dans les intérêts économiques et de propriété intellectuelle découlant de la façon dont les données sont déduites (ce que l'ancien article L424-42-3 du Code de la consommation qualifiait de données faisant « l'objet d'un enrichissement significatif par le fournisseur »)[1777]. À ce jour, il y a trop peu de jurisprudences sur le droit à la portabilité des données, et aucune n'interprète la portée du droit à la portabilité en matière de champ d'application des données à caractère personnel. Il n'est pas certain que les Cours nationales suivront les recommandations du G29[1778].

786. Enfin, la dernière limite rejoint la structure du marché précédemment décrite : le droit à la portabilité des données sous-entend la possibilité pour le consommateur de changer facilement d'opérateur afin de faire jouer la concurrence et gagner en pouvoir de négociation sur le marché. Or, les stratégies de concentration horizontales menées par les plateformes numériques s'opposent à cette logique. Prenons l'exemple de l'achat par Facebook de ses concurrents Instagram (pour son activité de réseau social) et Whatsapp (pour son service de messagerie instantanée), ou encore de Amazon qui s'attaque depuis quelques années au marché des sonnettes et caméra connectées avec le rachat des start-up Blink et Ring[1779]. Ces stratégies limitent la diversification des fournisseurs ainsi que le pouvoir de substitution des consommateurs finaux, neutralisant leur pouvoir de négociation et *in fine*, l'effectivité du droit à la portabilité des données sur le rééquilibrage du marché numérique.

787. Ces constats ne sont pas sans conséquences sur le consentement. La liberté du consentement suppose que la personne dispose d'une « véritable liberté de choix »[1780]. Or, si le RGPD n'envisage que cette liberté de choix dans la relation individuelle entre la personne concernée et le responsable de traitement, il nous semble indispensable de décloisonner l'analyse de la liberté de choix pour y intégrer également certains aspects de droit de la concurrence. L'exposé des motifs de la proposition de loi visant à garantir le libre choix du consommateur dans le cyberespace s'inquiète ainsi des limitations de la liberté de choisir du consommateur :

> « Si la taille acquise par les plus grandes entreprises leur permet de rendre des services toujours plus performants, elle les incite également à "enfermer" l'utilisateur dans leur écosystème. Sur

[1777] Article L224-42-3 du Code de la Consommation, créé par l'article 48 de la loi n° 2016-1321 du 7 octobre 2016 (Loi pour une République Numérique) et abrogé par l'article 33 loi n° 2018-493 du 20 juin 2018.
[1778] V. *supra* n° 341-351.
[1779] Le Figaro, « Pourquoi Amazon achète la start-up Ring pour un milliard de dollars », *LeFigaro.fr*, 1er mars 2018, disponible sur https://www.lefigaro.fr/secteur/high-tech/2018/03/01/32001-20180301ARTFIG00305-pourquoi-amazon-achete-la-start-up-ring-pour-un-milliard-de-dollars.php (consulté en mai 2021).
[1780] RGPD, 27 avril 2016, considérant 32.

> les plateformes d'achats, nos choix sont conditionnés par toute une série de dispositifs que maîtrisent les géants du numérique. Sur les réseaux sociaux, notre rapport au monde se rétrécit à mesure que nous embrassons la hiérarchisation des contenus proposée par l'algorithme de notre fil d'actualité. "Le monde à portée de clic" que l'on nous promettait s'est progressivement réduit à celui que les GAFAM nous présentent, nous proposent, voire parfois nous imposent. »[1781]

788. Ainsi, dans de nombreux cas, la protection de la personne concernée se confond avec la protection du consommateur sur le marché numérique. Le droit de la concurrence se décloisonne petit à petit pour prendre en compte des aspects de protection des données à caractère personnel dans son analyse. Cependant, à ce jour, il ne semble pas que dans l'analyse de la liberté du consentement, la protection des données à caractère personnel prenne en compte les conditions du marché et se contente plutôt d'analyser les options offertes par un responsable de traitement à une personne concernée. Or, il nous semble que la structure du marché numérique rend presque incontournable le recours à certains acteurs, limitant à notre sens la liberté du consentement de la personne concernée. Dans son rapport sur le numérique et les droits fondamentaux, le Conseil d'État reprend à cet égard la théorie développée par Helen Nissenbaum : « le recueil du consentement est une fiction, dès lors que les internautes ne peuvent pas négocier les conditions d'utilisation de leurs données et que la plupart des grands services de la société numérique, qu'il est difficile de ne pas utiliser, appliquent tous peu ou prou les mêmes procédés ; il n'existe dès lors pas de réelle liberté de choix »[1782]. Dès lors, ce qui était présenté comme le paradoxe de la vie privée — le fait que les personnes concernées consentent à la collecte massive de leurs données à caractère personnel tout en souhaitant plus de protection des données à caractère personnel — devient une attitude rationnelle sur le marché, qui ne propose aucune alternative satisfaisante[1783]. La prise en compte l'offre réellement présente sur le marché dans l'analyse de la liberté du consentement nous semble d'autant plus nécessaire que le RGPD ne s'intéresse pas au fait que la collecte des données à caractère personnel se situe au cœur du modèle économique sur le marché numérique.

§2 — La personne concernée captive de l'économie numérique

789. Le consentement requiert la liberté de la personne concernée, aussi bien en sa qualité de sujet de droit que d'agent économique. Nous venons de voir qu'il existe à ce sens des

---

[1781] Sénat, *Proposition de loi visant à garantir le libre choix du consommateur dans le cyberespace*, proposée par la sénatrice Sophie Primas et plusieurs de ses collègues, Texte n° 48 (2019-2020), déposé au Sénat le 10 octobre 2019.
[1782] Conseil d'État, *Le numérique et les droits fondamentaux, op. cit.* p. 170.
[1783] *Ibidem.*

interactions, encore limitées, entre le droit de la concurrence, le droit de la consommation et la protection des données à caractère personnel. Cependant, la place de la personne concernée en tant qu'agent économique sur le marché numérique n'est pas suffisamment prise en compte par la protection des données à caractère personnel. Cette situation est problématique, car la personne concernée — agent économique — est retenue captive du marché de l'attention et du capitalisme de surveillance (A), ce qui a des conséquences qui ne peuvent pas être ignorées en matière de consentement au traitement de ses données à caractère personnel (B).

A. La captivité de l'agent économique : marché de l'attention et capitalisme de surveillance

790. Si l'économie de l'attention ne concerne pas uniquement le numérique, elle interroge fortement sur les pratiques sur le marché numérique entre autres. La question n'est pourtant pas propre à l'univers numérique. Par exemple, en France, les propos du PDG de TF1 Patrick Le Lay affirmant en 2014 que la télévision vendait aux publicitaires « du temps de cerveau humain disponible »[1784] avaient suscité ses réactions d'indignation, à l'image du député Alain Riou qui avait répondu que « déclarer que le but ultime de la télévision, c'est de mettre au repos le cerveau des téléspectateurs pour mieux leur imposer la publicité est absolument honteux »[1785]. La réaction s'était également traduite dans un projet législatif, à travers la proposition d'amendement n° 146 (rejeté) à la loi relative à la lutte contre la manipulation de l'information proposant de permettre au Conseil supérieur de l'audiovisuel de refuser une convention en cas de « désinformation, manipulation du public pour des intérêts commerciaux », dont l'exposé sommaire vise expressément la pratique présentée par Patrick Le Lay[1786].

791. Le concept de l'économie de l'attention est d'autant plus visible sur le marché numérique. Le pionnier de cette théorie, Herbert Simon, démontre que dans le monde numérique, l'étude du ratio ressource-allocation de la ressource s'effectue en termes d'information et d'attention : « l'abondance d'information crée une pauvreté de l'attention et un besoin d'allouer cette attention efficacement parmi la surabondance de sources

---

[1784] LE LAY Patrick, *in* Les associés d'EIM (dir.), *Les dirigeants face au changement*, Paris, Huitième Jour, 2004, 140 p.

[1785] L'Obs, « Le Lay : "nous vendons du temps de cerveau" », *Nouvelobs.com*, 11 juillet 2004, disponible sur https://www.nouvelobs.com/culture/20040710.OBS2633/le-lay-nous-vendons-du-temps-de-cerveau.html (consulté en avril 2021).

[1786] Assemblée nationale, Amendement n° 146 présenté par Mme Mme Rubin, Mme Autain, M. Bernalicis, M. Coquerel, M. Corbière, Mme Fiat, M. Lachaud, M. Larive, M. Mélenchon, Mme Obono, Mme Panot, M. Prud'homme, M. Quatennens, M. Ratenon, Mme Ressiguier, M. Ruffin et Mme Taurine, visant à modifier l'article 4 de la loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

d'information qui pourraient la consommer »[1787]. Désormais, comme le théorise justement Yves Citton, « le principe de rareté paraît s'être radicalement déplacé, depuis le pôle de la production vers le pôle de la réception »[1788]. L'économie actuelle ne souffre pas, comme elle a pu souffrir auparavant, de manques d'investissement, de forces de travail ou encore d'information et de connaissance : il n'a jamais été aussi facile de lancer un commerce, de recourir à la publicité ou encore de créer un site internet[1789]. Aujourd'hui, on ne manque plus, selon la formule de Thomas Davenport et John Beck, de bande passante pour nos télécommunications, mais de bande passante humaine, autrement dit, l'attention[1790]. Le concept n'est pas nouveau, mais le phénomène se trouve amplifié par différentes tendances actuelles, qui sont la multiplication des objets connectés, le modèle économique de la publicité sur internet et la croissance des volumes d'informations disponibles[1791].

792. Ainsi, les acteurs privés sont dépendants de l'attention, qu'ils cherchent à mieux ou plus captiver que leurs concurrents, à tel point que Thomas Davenport et John Beck font de la capture de l'attention le facteur principal de succès des organisations[1792]. Selon les employés de Google, le temps d'attention disponible d'un *millenial* serait de neuf secondes, au-delà duquel le cerveau décroche : les plateformes numériques ne disposeraient que de ce très court laps de temps pour retenir notre attention[1793]. Si le marketing de la captation d'attention a dans un premier temps des effets bénéfiques sur le marché, le passage d'une information disponible à une saturation d'informations peut, selon l'hypothèse de Josef Falkinger, avoir des effets néfastes sur le marché[1794]. En effet, comme le résume Emmanuel Kessous,

> « Cette augmentation est dans un premier temps bénéfique pour le consommateur — conformément aux conclusions classiques de l'économie de l'information — car elle lui permet de choisir dans une gamme plus diversifiée de biens. Mais cette profusion d'information sature son attention et nécessite en retour que les firmes intensifient et multiplient leurs signaux, les

[1787] « A wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it ». SIMON Herbert A., «Designing Organizations for an Information-Rich World», *in* GREENBERGER Martin (dir.), *Computers, Communications, and the Public Interest*, Baltimore, The Johns Hopkins Press, 1971, pp. 40–41.
[1788] CITTON Yves, *L'économie de l'attention : nouvel horizon du capitalisme ?*, La découverte, 2014, p. 2.
[1789] DAVENPORT Thomas H., BECK John C., *The Attention Economy*, Harvard Business School Press, 2001, disponible sur acm.org (consulté en mai 2021)
[1790] *Ibidem.*
[1791] KESSOUS Emmanuel *et al.*, « L'économie de l'attention : entre protection des ressources cognitives et extraction de la valeur », *Sociologie du travail*, 2010, vol. 52, n° 3, disponible sur sciencespo.fr (consulté en mai 2021).
[1792] DAVENPORT Thomas H., BECK John C., *op. cit.*
[1793] PATINO Bruno, *La civilisation du poisson rouge. Petit traité sur le marché de l'attention*, Paris, Grasset et Fasquelle, 2019, p. 14.
[1794] FALKINGER Josef, «Limited Attention as a Scarce Resource in Information-Rich Economies», *The Economic Journal*, volume 118, issue 532, pp. 1596–1620.

consommateurs orientant, en effet, leur attention vers les signaux les plus forts. La quantité de signaux émis peut s'avérer au final non-optimal et justifier une action normative. »[1795]

793. La multiplication des signaux se traduit désormais en une concurrence importante autour du marketing des traces, dont la traduction principale est la publicité comportementale. Par exemple, selon David S. Evans, en 2019, les adultes américains passaient 514 millions d'heures devant du contenu publicitaire alors même qu'il passait 325 millions d'heures au travail[1796]. Or, les « attention market place » sont dominés par Google et Facebook qui détenaient respectivement 28,6 % et 23,7 % du marché publicitaire numérique mondial en 2021[1797]. En réaction, Brave a créé une nouvelle attention de l'économie fondée sur la blockchain, en créant un système de mesure de l'attention (*Basic Attention Metrics*) et une monnaie fondée sur cette ressource, appelée *Basic Attention Token*[1798] comme moyen d'échange de la ressource de l'attention. Face à la transformation de l'économie classique à l'économie de l'attention, dont la forme évoluée constitue aujourd'hui l'économie du marketing des traces[1799], le législateur peine à proposer une solution législative satisfaisante, faisant de l'économie de l'attention un « angle mort »[1800] de la régulation. En effet, Tim Wu suggère au législateur de prendre en compte le modèle économique des marchés de l'attention en déconstruisant le caractère gratuit des services dont le but est la captation de l'attention en vue de sa revente[1801]. Si cette démarche a été initiée au niveau de la protection des données à caractère personnel et du droit de la

---

[1795] KESSOUS Emmanuel, *op. cit.*, p. 71.

[1796] EVANS David S., « The Economics of Attention Markets », 15 avril 2020, disponible sur SSRN : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3044858 (consulté en aoput 2022).

[1797] La domination économique des deux acteurs s'est d'autant plus aggravée par un comportement anticoncurrentiel de Google à travers des effets de verrouillages en direction de ses éditeurs et la conclusion d'un accord illégal avec Facebook appelé « Jedi Blue » visant à réduire la concurrence de Facebook sur les parts de marchés de la publicité comportementale en échange d'avantages en faveur de la plateforme sur son service d'échange de publicité. v. Le Monde, « Publicité en ligne : Bruxelles soupçonne Google et Facebook d'avoir faussé la concurrence », *Le Monde.fr*, 11 mars 2022, disponible sur https://www.lemonde.fr/economie/article/2022/03/11/publicite-en-ligne-bruxelles-soupconne-google-et-facebook-d-avoir-fausse-la-concurrence_6117107_3234.html (consulté en août 2022) ; Next Impact, « La Commission enquête sur les mystères de Jedi Blue, l'accord publicitaire entre Google et Facebook », 14 mars 2022, disponible sur https://www.nextinpact.com/lebrief/68607/la-commission-enquete-sur-mysteres-jedi-blue-laccord-publicitaire-entre-google-et-facebook (consulté en août 2022) ; United States District Court, Southern District Court of New-York, *Google LLC*, Second amended Complaint, Civil Action No : 1 :21-md-03010-PKC.

[1798] Brave Software, « Basic Attention Token (BAT). Blockchain Based Digital Advertising », 10 février 2021, pp. 12-13, disponible sur https://basicattentiontoken.org/static-assets/documents/BasicAttentionTokenWhitePaper-4.pdf (consulté en août 2022).

[1799] KESSOUS Emmanuel, « L'économie de l'attention et le marketing des traces », *op. cit.* p. 79.

[1800] WU Tim, « Blind Spot ; Attention Economy and the Law », *Antitrust Law Journal*, 2019, vol. 82, n°3, pp. 771-806.

[1801] *Idem*, pp. 772-774.

consommation[1802], l'arsenal législatif peine cependant à prendre en compte de manière globale l'architecture de l'économie de l'attention.

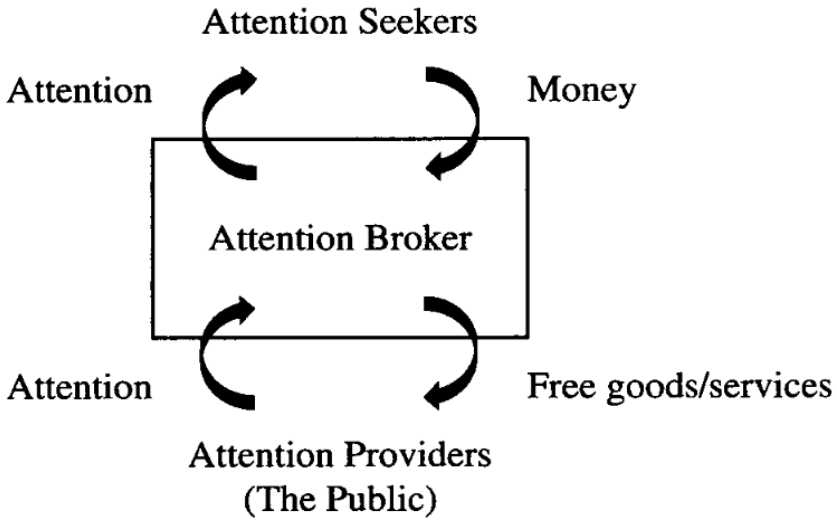

Figure 14 — Modèle de l'économie de l'attention[1803]

794. Au-delà de l'économie de l'attention, la personne concernée est également considérée par la doctrine comme captive du capitalisme de surveillance. La théorie du capitalisme de surveillance s'inscrit dans une analyse plus large de l'économie que l'analyse de l'économie de l'attention : elle replace les stratégies déployées par les acteurs privés dans une stratégie globale de surveillance. Par exemple, l'affaire PRISM révélée par Edward Snowden montre la porosité des activités de surveillance entre les activités de renseignement (la surveillance étatique) et les activités commerciales comme la publicité ciblée (la surveillance commerciale)[1804]. Le capitalisme de surveillance est une notion définie par Shoshana Zuboff comme une « nouvelle forme de capitalisme qui traduit l'expérience humaine en données comportementales afin de produite des prédictions qui sont ensuite revendues sur le marché des comportements futurs »[1805]. Selon David Lyon, la surveillance est désormais devenue une clé intrinsèque du fonctionnement d'internet tant elle irrigue l'ensemble des activités sur cet espace : non seulement les personnes concernées vont rencontrer, expérimenter et être sujets de la

[1802] V. *supra* n°318-323 pour une discussion sur la requalification des contrats présentés comme des contrats à titre gratuit en des contrats à titre pécuniaire.
[1803] WU Tim, *op. cit.*, p. 788.
[1804] KUMAR Priya, « Corporate Privacy Policy Changes during PRISM and the Rise of Surveillance Capitalism », *Media and Communication*, 2017, Volume 5, Issue 1, p. 68.
[1805] ZUBOFF Shoshana, « Le capitalisme de la surveillance. Un nouveau clergé », *Esprit*, 2019, n°5, p. 63.

surveillance, mais elles vont également en être acteurs[1806]. Le capitalisme de surveillance s'inscrit dans la monétisation de l'expérience humaine — envisagée comme « matière première gratuite —, une recherche de modification des comportements inscrite dans la logique économique et une concentration du savoir, du pouvoir et de la richesse[1807]. Ainsi, on entend principalement comme capitalisme de surveillance le fait pour une plateforme numérique de transformer ses interactions avec les utilisateurs en « surplus comportemental » (*actifs de surveillance*), grâce à des procédés complexes (et de plus en plus grâce à l'intelligence artificielle), afin de créer des « produits de prédiction », qui sont vendus sur les « marchés des comportements futurs » à des acteurs ayant pour objectif de prédire, d'influencer voire de modeler notre comportement[1808].

795. Le phénomène inquiète la doctrine, principalement anglo-saxonne[1809]. Les conséquences d'un tel phénomène ont des conséquences en matière de protection des données à caractère personnel, ce qui a été rappelé par la présidente de la Commission européenne Ursula von der Leyen dans une lettre ouverte en réponse à Mathias Döpfner :

> « C'est nous-mêmes, les utilisatrices et utilisateurs, qui sommes le produit qui intéresse les grandes plateformes. Plus elles en savent sur nous, plus nous sommes précieux pour elles. Cela leur permet de nous inonder de publicités de manière ciblée, et de facturer à leurs clients des montants toujours plus élevés »[1810] .

Dans ce cadre, la captivité de la personne concernée dans la structure actuelle de l'économie questionne la capacité pour la personne concernée de détenir le contrôle sur la protection de ses données à caractère personnel, et plus précisément, d'émettre un consentement libre et éclairé au traitement de ses données à caractère personnel par un acteur intégré dans le marché numérique.

B. Les conséquences problématiques de la structure de l'économie numérique sur le consentement

796. Ramenée à la question du consentement, une telle structure de l'économie est problématique à plusieurs titres. Premièrement, la diminution de notre capacité d'attention

---

[1806] LYON David, « Surveillance Capitalism, Surveillance Culture and Data Politics », *in* BIGO Didier *and al.* (dir.), *Data Politics. Worlds, Subjects, Rights*, Londres, Routledge, 2019, p. 65.
[1807] ZUBOFF Shoshana, *op. cit.*, p. 14.
[1808] *Idem*, pp. 163-169.
[1809] Dans la doctrine française, le capitalisme de surveillance est surtout envisagé comme le modèle économique américain. V. BRUNESSEN Bertrand,2021, *op. cit.*, p. 139.
[1810] VON DER LEYEN Ursula, « Ce qui est interdit dans le monde réel doit être aussi interdit en ligne », *LeFigaro.fr*, 29 janvier 2021, disponible sur https://www.lefigaro.fr/vox/monde/ursula-von-der-leyen-ce-qui-est-interdit-dans-le-monde-reel-doit-etre-aussi-interdit-en-ligne-20210129 (consulté en mai 2021).

affaiblit proportionnellement la réalité du consentement : comment obtenir un consentement éclairé de la personne concernée en neuf secondes ? Comment une personne concernée, dont la ressource du temps est de plus en plus rare[1811], peut-elle consentir devant la multiplication des choix qui s'offrent à elle à tout instant ? C'est ainsi que "de nombreux best-sellers se plaignent depuis plusieurs années d'un sentiment sous la « tyrannie du choix » : nous autres, "simples mortels" dont les ressources attentionnelles sont limitées, ne parvenons plus à faire face à toute la myriade de choix que nous offrent à tout instant nos modes de vie et de consommation"[1812]. À cet égard, c'est la nature même de la structure de l'économie qui pose la question de l'adéquation du consentement de la personne concernée.

797. Deuxièmement, l'économie de l'attention est aussi problématique quant à ses conséquences. Dans son ouvrage dédié au marché de l'attention, Bruno Patino s'intéresse aux pathologies nées des efforts de capture d'attention des plateformes numériques : il y cite l'addiction, la nomophobie (*no mobile phone phobia* –, la peur de se retrouver éloigné de son téléphone), le *phnubbing* (*phone snubbing* – le fait pour une personne d'être si attirée par son téléphone qu'elle le consulte ostensiblement alors même qu'une personne lui adresse la parole) ou encore l'anxiété[1813]. Selon lui, "le vertige que provoque la séparation d'avec les outils connectés et de leurs applications est un produit de laboratoire, tout comme le besoin compulsif de répondre aux sollicitations numériques qui envahissent nos écrans[1814]. Soshana Zuboff attire également l'attention sur les effets de l'hyperconnexion, créateurs d'une « variété de troubles émotionnels que l'on peut rapidement classer en six catégories : l'addiction, l'incapacité à se débrancher, l'ennui, la confusion, la détresse et l'isolement »[1815]. Au-delà des pathologies, c'est le système de capture même qui pose question. Dans son ouvrage consacré à l'économie de l'attention, le chercheur Yves Citton décrit les mécanismes psychologiques utilisés par la publicité : la publicité est un « système qui a comme vocation de nous distraire, d'interrompre

[1811] Harmut Rosa explique la rareté de la ressource temps par plusieurs facteurs parmi lesquels se trouvent l'accélération technologique, l'accélération des changements sociaux, le capitalisme (notamment la maxime « le temps c'est de l'argent »), la culture (l'idéal d'une vie bien remplie, riche en expériences et en développement de compétences), ou encore la montée en complexité de disciplines irrigant nos sociétés (il cite à cet effet la politique, les sciences, l'art, l'économie et le droit). ROSA Harmut, « Social Acceleration: Ethical and Political Consequences of a Desynchronized High-Speed Society », *in* ROSA Harmut (dir.), *High-Speed Society: Social Attention, Power, and Modernity*, Penn State Press, 2010, pp. 77-112.
[1812] AIN AL-SHAMS Abad, « Le nudge. Embarras du choix & paternalisme libertarien », *Multitudes*, 2017/3, n°68, pp. 44.
[1813] PATINO Bruno, *op. cit.*, pp. 23-24.
[1814] *Idem*, p. 27.
[1815] ZUBOFF Shoshana, *op. cit.* , p. 757.

notre absorption dans nos réflexions »[1816] grâce à l'exploitation de nos cartes de saillance[1817] ou du circuit de récompense[1818]. Quelle serait alors la place du consentement face aux contraintes résultant de l'économie de l'attention ? Comment la personne concernée pourrait consentir lorsque les plateformes numériques déploient des stratégies « qui agissent comme des espèces de vents violents qui attirent ou font dévier l'attention »[1819] ?

798. La question intéresse désormais les juristes, dont certains appellent à reconnaître un droit à la protection de l'attention[1820]. Un tel droit contiendrait une obligation de transparence des plateformes numériques quant à l'utilisation de dispositifs de captation de l'attention, la mise en place d'outils de maîtrise de l'attention numérique (par exemple, la possibilité de maîtriser le système de notification), une protection des publics sensibles, de nouvelles obligations de sobriété numérique (est évoqué le *cooling by design*, ou refroidissement dès la conception), la création de nouvelles autorités de contrôle (*attention protector officer*) et la mise en place de politiques publiques de l'attention en ligne[1821]. La protection de l'attention serait un droit nécessaire à l'analyse des informations, qui aujourd'hui est menacé par l'économie de l'attention. Interrogée dans le cadre des travaux sur le rapport entre numérique et savoirs du Conseil national du numérique, la neuroscientifique Maryanne Wolf s'inquiétait de l'effet de l'exploitation de l'attention sur les jeunes publics qui « n'apprennent pas à allouer leur attention aux processus de lecture profonde » alors même que celle-ci permet le développement de l'analyse critique et de l'empathie :

[1816] CITTON Yves, *op. cit.*, pp. 85-86.

[1817] Ainsi, la publicité chercherait à créer des stimuli lui permettant de se détacher d'une masse d'information, et capturer l'attention de la personne. Par exemple, la publicité va chercher à attirer le regard de la personne à travers le clignotement, l'image, etc. v. la définition de la saillance visuelle proposée par Anass NOURI : « La saillance visuelle peut être définie comme l'information perceptuelle permettant à certains objets ou régions de la scène de ressortir fortement de leur voisinage et ainsi d'attirer l'attention visuelle de l'observateur ». NOURI Anass, *Cartes de saillance et évaluation de la qualité des maillages 3D*, Thèse pour l'obtention du grade de docteur en informatique sous la direction de LÉZORAY Olivier et CHARRIER Christophe, Université de Normandie, 2016, p. 20. Pour une explication générale de l'exploitation par les publicitaires des cartes de saillance, v. CITTON Yves, *op. cit.*, pp. 83-86.

[1818] L'exploitation du circuit de récompense va créer un désir de revenir, de réitérer l'action ayant déclenché la récompense, ce qui parfois peut également déclencher une addiction. Pour une explication physiologique du circuit de récompense, v. PESSIGLIONE Mathias, « Comment le cerveau motive le comportement : du circuit de la récompense au système des valeurs », *Bull. Acad. Natle Méd.*, 2014, 198, n°7, pp. 1283-1296.

[1819] CITTON Yves, *op. cit.*, p. 86.

[1820] ZOLYNSKI Célia *et al.*, « L'économie de l'attention saisie par le droit », *Dalloz IP/IT*, 2019, p. 614 ; Le Monde, « La liberté d'expression à l'heure du numérique ou la difficile quête de l'équilibre sur les réseaux sociaux », *LeMonde.fr*, 2 avril 2021, disponible sur https://www.lemonde.fr/idees/article/2021/04/02/reseaux-sociaux-et-liberte-d-expression-inventer-des-dispositifs-pour-proteger-nos-democraties_6075320_3232.html (consulté en mai 2021).

[1821] ZOLYNSKI Célia *et al.*, 2019, *op. cit.*, p. 614.

> « Notre culture axée sur le profit détourne notre attention pendant la lecture, avec des publicités successives. Les enfants et les jeunes seraient ainsi distraits au moins 27 fois par heure lorsqu'ils lisent »[1822].

Ces craintes sont reprises par le Conseil national du numérique, qui travaille à s'assurer que les technologies numériques « ne dépossèdent pas les citoyens de leurs capacités d'agir, de travailler, de réfléchir, de penser »[1823]. Dès lors, la protection de l'attention serait un prérequis à l'exercice d'un consentement réellement éclairé, qui requiert l'exercice des capacités de compréhension et d'analyse de la personne concernée.

799. Enfin, l'absence de contrôle des activités de prédiction du comportement peut avoir des conséquences dommageables sur la réalité du consentement, dans la mesure où « les algorithmes prédictifs observent la réalité pour mieux influer sur elle »[1824]. Dès lors, une protection de la personne concernée contre l'influence déraisonnable se justifie aussi bien au niveau de l'asymétrie informationnelle que de l'asymétrie économique :

> «En fin de compte, les capitalistes de surveillance ont découvert que les données comportementales les plus prédictives s'obtiennent en intervenant directement pour inciter (*nudge*) et influencer, ajuster (*tune*) et aiguillonner (*herd*) le comportement vers des résultats rentables […]. Dans cette phase d'évolution du capitalisme de surveillance, les moyens de production sont subordonnés à des "moyens de modification des comportements" de plus en plus complexes et globaux'[1825].

800. L'économie de l'attention et le capitalisme de surveillance ont pour conséquence de miner la validité et l'effectivité protectrice du consentement en matière de protection des données à caractère personnel.

[1822] Conseil national du numérique, « 5 questions à Maryanne Wolf : « Nous devons comprendre ce que fais chaque technologie, et être capables de choisir » », *cnnumerique.fr*, 20 mai 2021, disponible sur https://cnnumerique.fr/5-questions-maryanne-wolf-nous-devons-comprendre-ce-que-fait-chaque-technologie-et-etre-capables-de (consulté en mai 2021).

[1823] Conseil national du numérique, « Pour un numérique au service des savoirs. De l'informatisation à la capacitation », *cnnumérique.fr*, mai 2021, disponible sur https://cnnumerique.fr/files/uploads/2021/CNNum_Pour_un_numerique_au_service_des_savoirs_mai_2021.pdf

[1824] GODEFROY Lêmy, « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », *D.* 2016, p. 438.

[1825] ZUBOFF Shoshana, *op. cit.*, Zulma, 2020, pp. 30-31.

Section 2 — Le développement nécessaire de l'action de groupe comme correctif la relation asymétrique entre le responsable de traitement et la personne concernée

801. L'article 30 du code de procédure civile définit l'action en justice comme « le droit, pour l'auteur d'une prétention, d'être entendu sur le fond de celle-ci afin que le juge la dise bien ou mal fondée ». Traditionnellement, le contentieux est « de type personnel », traduction de l'influence de l'individualisme à partir du XVIIe siècle dans le droit français[1826]. La réflexion sur la réforme du droit de la consommation menée dans les 1980 a été, en France, l'élément déclencheur des discussions sur l'action de groupe[1827]. Finalement non intégrée à la réforme du droit de la consommation[1828], la question refera son apparition en 2005 à travers les propos du Président Jacques Chirac :

> « Il faut enfin donner aux consommateurs les moyens de faire respecter leurs droits : aujourd'hui, ils sont démunis parce que, pris séparément, aucun des préjudices dont ils sont victimes n'est suffisant pour couvrir les frais d'une action en justice. C'est pourquoi je demande au gouvernement de proposer une modification de la législation pour permettre à des groupes de consommateurs et à leurs associations d'intenter des actions collectives contre les pratiques abusives observées sur certains marchés »[1829]

802. En 2010, Thomas Clay prédisait que « l'introduction d'une action de groupe en France est désormais inévitable parce que c'est le sens de l'histoire et parce qu'elle est reconnue presque partout ailleurs »[1830]. La prédiction se réalisera quatre ans plus tard par l'adoption de la loi n° 2014-344 du 17 mars 2014 relative à la consommation créant un cadre juridique relatif à l'action de groupe. Le Conseil constitutionnel confirmera la constitutionnalité de l'action de groupe, la liant à l'article 16 de la Déclaration de l'homme et du citoyen de 1789, en ce que le mécanisme garantit « le droit des personnes intéressées à exercer un recours juridictionnel effectif »[1831].

803. Un bref aperçu de droit comparé montre que l'action de groupe apparaît tardivement en France, par rapport à l'introduction en 1966 de la *class action* aux États-Unis ou du recours

---

[1826] CAYROU Nicolas, *Action en justice*, Paris, Dalloz, novembre 2019, pp. 214-215.
[1827] ALLARD Baptiste, JOURDAN-MARQUES Jérémy, « Action de groupe », *Répertoire de procédure civile,* février 2021.
[1828] *Ibidem.*
[1829] Extrait des vœux du Président Jacques Chirac reproduit dans CABRILLAC Séverine, « Pour l'introduction de la class action en droit français », *Petites affiches,* 18 août 2008, n°165, p. 4.
[1830] CLAY Thomas, « *Class actions or not class actions ?* », *D.*, 2020, p. 1776.
[1831] DC, 13 mars 2014, n°2015-690, §15.

collectif québécois en 1978[1832]. La réticence française face à la création d'une action de groupe peut probablement être expliquée par le fait que « la diabolisation du modèle américain de *class action* a occupé une place déterminante dans les préoccupations du législateur, sans doute une trop grande place »[1833]. En effet, le Sénat fait part des craintes « d'une dérive à l'américaine » caractérisée par la transformation de l'action de groupe en marché particulièrement lucratif pour les avocats — par exemple, le versement de 688 millions de dollars d'honoraire lors de l'affaire Enron —, par un système de preuve à la charge uniquement de l'entreprise attaquée, par la définition des plaignants à travers un mécanisme d'*opt-out* et par le « chantage au procès » entraînant la multiplication des transactions[1834]. L'action de groupe introduite par la loi du 17 mars 2014 a été également définie dans cette optique, à l'image des propos de Pierre Moscovici, alors ministre de l'Économie et des Finances, qui se félicitait dans ces termes :

> "Nous avons cherché, et je crois trouvé […] un équilibre sur l'action de groupe. Le texte est en effet ambitieux, notamment avec l'introduction d'une procédure simplifiée, et évite de tomber dans certains travers que l'on peut trouver de l'autre côté de l'Atlantique, car nous respectons les caractéristiques de notre économie. Ce texte ne créera, je veux le dire avec force et simplicité, pas de chasseurs de primes pourchassant les entreprises"[1835].

804. Les actions de groupe supposent également une transformation importante de la nature du contentieux. L'action en justice est considérée comme une liberté, définie par le Conseil constitutionnel comme « la liberté de conduire personnellement la défense de ses intérêts et de mettre un terme à cette action »[1836]. Une telle conception individualiste a eu pour conséquence de « rompre le lien historique de l'action en justice avec l'intérêt général », en considérant que ce dernier découlera naturellement de la recherche par l'individu de la satisfaction de son intérêt personnel[1837]. La reconnaissance de l'action de groupe transforme substantiellement la nature du contentieux, d'un contentieux individuel à un contentieux collectif, voire objectif[1838]. Une telle transformation demande une réflexion rigoureuse sur l'articulation entre le contentieux

---

[1832] KOBINA GABA Harold, « La protection collective des consommateurs en droit européen : nécessité d'une action de groupe ou de recours collectifs et raisons politico-économiques et juridiques », *Revue de la Recherche Juridique*, Presses Universitaires d'Aix-Marseille, 2015, pp. 1476-1477.
[1833] LAFOND Pierre-Claude, « L'action de groupe française ou l'art de rater une belle occasion », *Revue internationale de droit comparé*, 2016, n°68, p. 339.
[1834] Sénat, « L'action de groupe à la française : parachever la protection des consommateurs », *Rapport d'information n°499 fait au nom de la commission des lois*, déposé le 26 mai 2010, pp. 29-31.
[1835] Propos de Pierre Moscovisci reproduits dans Assemblée nationale, *Rapport d'information sur le bilan et les perspectives des actions de groupe*, déposé en application de l'article 145 du Règlement par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, 11 juin 2020, n°3085.
[1836] DC, 25 juillet 1989, n°89-257, §24.
[1837] SERVERIN Évelyne, « Introduction. Une enquête juridique sur la place du collectif dans la justice contemporaine », *in* OMARJEE Ismaël, SINOPOLI Laurence (dir.), *Les actions en justice au-delà de l'intérêt personnel*, Dalloz, 2014, p. 5.
[1838] CAYROU Nicolas, *op. cit.*, p. 215.

individuel et l'action de groupe, de manière à éviter les écueils de l'encombrement de la justice et du déni de justice[1839]. Ces réflexions sont à l'origine de contentieux de type hybride, groupés quant à la reconnaissance de la responsabilité du défendeur, individuels quant aux questions de preuve et d'indemnisation.

805. Concernant la protection des données à caractère personnel, la double nature commerciale et fondamentaliste de la matière permet de considérer la personne concernée à la fois comme une personne consommatrice éligible à l'action de groupe (§1) et comme une personne concernée éligible à l'action de groupe « données personnelles » (§2).

§1 — L'efficacité mitigée de l'action de groupe dans le rééquilibrage des relations économiques en droit de la consommation

806. L'asymétrie de la relation entre le consommateur et le professionnel a comme conséquence de rendre difficile l'action en justice du consommateur, par manque de moyens, d'information ou d'aptitudes. Dans ce cadre, la reconnaissance d'un intérêt à agir dépassant les intérêts individuels a constitué l'un des moyens de dépasser voire de rééquilibrer la relation entre le consommateur et le professionnel (A). Cependant, si une telle reconnaissance est indispensable pour permettre l'action en justice contre une pratique commerciale illicite, elle ne peut pas pour autant se suffire à elle-même. L'action en justice demande en effet des ressources financières, humaines et intellectuelles afin de permettre la mise en place de recours efficaces (B).

A. La reconnaissance nécessaire d'un intérêt à agir par représentation

807. La reconnaissance d'intérêts à agir par représentation précède l'apparition des actions de groupe. La première chambre civile de la Cour de cassation avait par exemple jugé en 2000 qu'une association avait un intérêt à agir contre une publication portant atteinte aux membres qu'elle a vocation à protéger[1840]. Le droit de la consommation a été le vecteur de la reconnaissance plus avancée d'un tel intérêt à agir, permettant une représentation des intérêts extérieure à travers l'action de groupe. La nécessité d'un tel mécanisme a été justifiée par « l'idée que la situation inégale entre le consommateur et le professionnel ne peut être

[1839] GUIOMARD Frédéric, « L'obscure clarté de la succession des actions collectives et individuelles en justice », *Revue de droit du travail*, 2021, p. 597.
[1840] Cass. Civ. 1er, 14 novembre 2000, n°99-10.778 ; AUTRIC Jean-Baptiste, CHAPUIS-BREYTON Simon, « Juridique – Action en justice – Intérêt à agir, intérêts collectifs et valeurs partagées », *Juris associations*, 2015, n°529, p. 37.

compensée que par une intervention positive, extérieure aux seules parties du contrat »[1841]. L'objectif ainsi de « substituer à l'équilibre formel que le contrat établit entre les droits et les obligations des contractants un équilibre réel de nature à rétablir l'égalité entre ces derniers »[1842]. Pour le législateur européen, l'accomplissement d'un tel objectif est rendu nécessaire du fait que « la mondialisation et la numérisation de l'économie ont augmenté le risque qu'un grand nombre de consommateurs soient lésés par la même pratique illicite »[1843]. L'absence d'actions représentatives dans certains États membres a des conséquences sur le marché intérieur, parmi lesquelles l'amoindrissement de la confiance sur le marché, la distorsion de la concurrence, ou encore l'entrave à une application effective du droit de l'Union[1844]. En effet, la structure actuelle de l'économie résulte en deux principaux obstacles à l'effectivité du droit d'accès au juge du point de vue du consommateur. Tout d'abord, la particularité de la matière tient en ce que ces litiges présentent une faible rentabilité pour le consommateur rationnel. Il s'agit souvent de litiges « caractérisés par leur faible ampleur, rapportée au coût, à la complexité et à la lenteur de l'action en justice nécessaire pour en obtenir la résolution »[1845]. Ensuite, le droit de la consommation présente une difficulté parfois perçue comme insurmontable par le consommateur, qui n'envisage dès lors pas « d'agir sans le soutien ou l'initiative d'un "tiers de confiance", une association de consommateurs par exemple »[1846]. Sur le marché numérique, l'absence de conformité du professionnel avec les dispositions en matière de sécurité peut représenter un préjudice dont la réparation est jugée non rentable sur le plan individuel, mais d'une importance considérable sur le plan collectif.

808. L'action de groupe apparaît alors comme un élément essentiel à l'effectivité des droits du consommateur conférés à travers le droit de la consommation. D'après Daniel Mainguy et Malo Depincé, l'action de groupe révèle le passage vers un « nouveau droit de la consommation » qui n'est « plus perçu comme une série de proclamations ou une reconnaissance de droits laissés au final à la libre application des professionnels sous le contrôle des autorités publiques, mais comme un ensemble de règles dont le législateur entendrait s'assurer de leur effectivité, en confiant aux consommateurs eux-mêmes, *via* les associations

[1841] CJUE, 5e ch., 24 janvier 2002, *Commission / Italie*, C-372/99/
[1842] CJUE, 1er ch., 26 avril 2012, *Nemzeti Fogyasztóvédelmi Hatóság*, C-472/10, §34.
[1843] Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogreant la directive 2009/22/CE, considérant 1.
[1844] *Idem*, considérant 6.
[1845] ASCENSI Lionel, « Médiation et actions collectives », *Revue Lamy droit des affaires*, 2015, n°105.
[1846] MAINGUY Daniel, DEPINCÉ Malo, « L'action de groupe, nouvelle procédure du droit français de la consommation », *Droit et Patrimoine*, mai 2014, n°236.

de consommateurs, le soin de les faire respecter »[1847]. Elle permet également, à travers la facilitation des actions en justice, d'avoir un effet préventif, afin de constituer, selon la formule retenue par Benoît Hamon, « une arme de dissuasion massive »[1848]. Le rapport de l'Assemblée nationale sur le bilan des actions de groupe considère que l'action de groupe « a pu inciter les professionnels, dans un souci de préservation de leur image, à revoir leur stratégie de prévention du contentieux, en portant une attention particulière aux réclamations des clients et en prenant les mesures adéquates pour y remédier, ou encore en modifiant certaines des stipulations contenues dans les contrats souscrits par les consommateurs »[1849]. Le rapport s'appuie notamment sur le constat partagé de l'association CCLV et du Procureur général près la Cour de cassation d'un « nettoyage des clauses » abusives.[1850]

809. Il est vrai que les risques relatifs à la réputation des professionnels ne sont pas négligeables. La structuration de la procédure de l'action de groupe en deux phases distinctes a encouragé les initiateurs de telles actions à constituer une large couverture médiatique de leurs actions. La première phase consiste en l'examen du principe de la responsabilité de l'entreprise : l'association agréée sélectionne un panel de cas exemplaires parmi les cas qui lui sont soumis afin d'introduire devant le juge l'action de groupe[1851]. Une fois la décision du juge définitive, la seconde phase correspond à la mise en œuvre de la décision, à travers la mise en place de mesures de publicité permettant aux consommateurs concernés de se manifester auprès du professionnel ou de l'association (ou éventuellement un tiers autorisé à s'adjoindre à la procédure par l'association)[1852]. Cette phase est également celle de l'indemnisation par le professionnel aux consommateurs qui se sont manifestés[1853]. La forte couverture médiatique accompagnant les actions de groupe se justifie tout d'abord par l'intérêt des associations en matière de preuve. D'après Alexandre Biard, « pour des questions liées à la préservation de la preuve par les potentiels membres du groupe, les associations ont intérêt à faire connaître l'existence d'une action de groupe le plus tôt possible, et ne pas attendre une condamnation du

---

[1847] *Ibidem.*
[1848] Propos de Benoît Hamon reproduits dans Lextenso, « Class action française : les avocats au bord du chemin », *Gazette du Palais*, 7 mai 2013, n°127.
[1849] Assemblée nationale, n°3085, *op. cit.*.
[1850] *Ibidem*.
[1851] Sénat, 26 mai 2010, n°499, *op. cit.,* p. 9 ; ministère de l'Économie, des finances et de la relance, « Comprendre l'action de groupe en 5 questions », *Bercy Infos*, 28 juin 2017, disponible sur https://www.economie.gouv.fr/particuliers/action-de-groupe (consulté en janvier 2022).
[1852] DUMAS Anne-Gaëlle, « Zoom sur l'action de groupe en matière de consommation », *justice.gouv.fr*, 12 mars 2015, disponible sur http://www.textes.justice.gouv.fr/dossiers-thematiques-10083/loi-du-170314-sur-laction-de-groupe-12775/zoom-sur-laction-de-groupe-en-matiere-de-consommation-27936.html (consulté en janvier 2022).
[1853] *Ibidem.*

professionnel susceptible de survenir de longs mois, voire des années plus tard »[1854]. Envisagée d'abord sous un angle pragmatique, la couverture médiatique deviendra la principale arme de dissuasion avant même l'action judiciaire, puisqu'elle suffit à mettre en cause l'honneur du professionnel[1855]. Le phénomène est bien connu, la publicité des sanctions de la CNIL étant considérée comme un pouvoir de sanction de la formation restreinte à part entière[1856].

810. Malgré un bilan mitigé de l'efficacité des dispositions relatives à l'action de groupe « à la française », la représentation des consommateurs, regroupés, par un intermédiaire, semble être vectrice de l'initiation d'actions en justice, qui, bien que souvent vaines, ont le mérite d'exister.

B. La poursuite de l'action par des organisations compétentes, verrou de l'action de groupe

811. Afin de garantir aux personnes physiques leur droit d'agir en justice dans le cadre d'une action de groupe, il faut encore au législateur s'assurer que la personne lésée soit représentée par la « "juste partie" ayant qualité à agir », qui présenterait une « représentativité adéquate »[1857]. Si l'action en justice se fonde au départ sur la sélection de cas identifiés, l'absence d'identification de l'ensemble des consommateurs concernés nécessite une réflexion sur la légitimité des organisations à l'origine des actions de groupe.

812. En France, la représentation a été fortement encadrée, le législateur étant peu enclin à dépasser la maxime « nul ne plaide par procureur ». La loi du 17 mai 2014 conditionnait l'action de groupe à l'obtention d'un agrément par des associations de défense des consommateurs au niveau national[1858]. La loi de modernisation de la justice ouvre la possibilité d'introduire une action aux « régulièrement déclarées depuis cinq ans au moins dont l'objet statutaire comporte la défense d'intérêts auxquels il a été porté atteinte »[1859]. Le choix de la représentation associative a été guidé par le fait que « le statut et l'objet social des associations de consommateurs agréées, à savoir la défense de l'intérêt collectif des consommateurs, leur

---

[1854] BIARD Alexandre, « Sale temps pour l'action de groupe … La nécessaire recherche d'outils alternatifs pour résoudre les litiges de masse », *Revue Lamy Droit civil*, mars 2018, n°157.
[1855] BOURDEL Christophe, « Première bougie pour l'action de groupe : un bilan en demi-teinte », *AJ contrat*, 2015, p. 488.
[1856] CNIL, « Les pouvoirs de la formation restreinte », *CNIL.fr*, 25 octobre 2019, disponible sur https://www.cnil.fr/fr/les-pouvoirs-de-la-formation-restreinte (consulté en janvier 2022).
[1857] SINOPOLI Laurence, « Chapitre 1. La légitimité des porteurs de l'action de groupe : entre représentation et qualité », », *in* OMARJEE Ismaëk, SINOPOLI Laurence (dir.), *Les actions en justice au-delà de l'intérêt personnel*, Dalloz, 2014, p. 23.
[1858] Assemblée nationale, 11 juin 2020, n°3085, *op. cit.*.
[1859] Loi n°2016-1546 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, Article 63.

permettent de répondre aux exigences de légitimité quant à l'intérêt pour agir et leur confèrent la qualité pour représenter le groupe des consommateurs en tant que tel sans qu'il soit besoin d'identifier au préalable les victimes »[1860].

813. Ainsi, le grand absent de l'introduction de l'action de groupe est l'avocat, bien que la représentation de l'association devant les tribunaux de grande instance nécessite la représentation de celle-ci par un avocat[1861]. Si l'incompatibilité de la publicité nécessaire à la création d'un groupe de consommateur avec l'interdiction de démarchage et de sollicitation des avocats a pu être évoquée, c'est pourtant bien la méfiance du législateur envers la profession qui est à l'origine d'une telle éviction[1862]. Cette méfiance est alimentée par la menace du développement d'une activité très lucrative à l'américaine motivée plutôt par le gain que par la défense des intérêts[1863]. Pourtant, l'interdiction des pactes de *quota litis* et la possibilité pour le juge de corriger le montant des honoraires exagéré au regard du service rendu constituaient des garanties suffisantes pour prévenir ce risque de dérives[1864]. Le Conseil national des Barreaux a, en 2017, proposé au candidat Emmanuel Macron d'autoriser les avocats à engager des actions de groupe des associations lorsque ces dernières ne pouvaient pas introduire de recours par manque de compétence ou d'intérêt à agir, inaction de l'association quinze jours après la mise en demeure par les consommateurs concernés, impossibilité pour l'association d'agir ou de continuer son action de justice ou présence ou risque de conflit d'intérêts de l'association[1865]. Cette possibilité a été rapidement écartée par Emmanuel Macron, qui en 2017, reporte la réévaluation des représentants des consommateurs « quand nous aurons un certain recul sur le sort de ces actions de groupe et leurs dysfonctionnements éventuels »[1866].

814. Les craintes de détournement de l'action de groupe à des fins personnelles sont tout à fait légitimes du point de vue du législateur. De telles craintes existent outre-Atlantique, mais

---

[1860] Assemblée nationale, *Étude d'impact du projet de loi relatif à la consommation*, 30 avril 2013, NOR :EFIX1307316L/Bleue-1, disponible sur https://www.assemblee-nationale.fr/14/projets/pl1015-ei.asp#P2643_381570 (consulté en janvier 2022).

[1861] RODRIGUEZ Karine, « Étude 59 – Associations de défense des consommateurs », *in* DUTHEIL Philippe-Henri (dir.), *Droit des associations et fondations*, Paris, Dalloz, Juriscorpus, §59.132.

[1862] HILT Patrice, « L'action de groupe consacrée par la loi n°2014-344 du 17 mars 2014 relative à la consommation : peut-on s'en satisfaire ? », *Gazette du Palais*, avril 2014, n°114.

[1863] *Ibidem.*

[1864] *Ibidem.*

[1865] Conseil national des barreaux (CNB), *Dix propositions du Conseil national des barreaux au Président de la République*, CNB.avocat.fr, mai 2017, disponible sur https://cnb.avocat.fr/sites/default/files/documents/10_propositions_du_cnb.pdf (consulté en janvier 2022).

[1866] Conseil national des barreaux (CNB), *Réponses du candidat Emmanuel Macron aux questions du CNB*, CNB.avocat.fr, mai 2017, disponible sur https://cnb.avocat.fr/sites/default/files/documents/reponses_du_candidat_macron_page_a_page.pdf (consulté en janvier 2022).

le danger identifié diffère : au Québec, « le monopole des associations a été exclu par crainte que "celles-ci n'utilisent le recours collectif à des fins personnelles […] pour apparaître comme les plus actives et les plus efficaces"[1867]. Cependant, il existe des systèmes ne verrouillant pas l'initiation de l'action de groupe à un seul type d'entité. Par exemple, au Portugal, l'action populaire est ouverte à certaines personnes morales, mais surtout à toute personne physique à la seule condition qu'elle soit titulaire « des intérêts diffus, collectifs ou individuels, mais homogènes qui sont menacés ou déjà affectés »[1868].

815. Si la compétence et la légitimité sont des questions essentielles, le législateur doit, dans un même temps, faire attention de ne pas fermer de manière excessive la possibilité de recours. Le bilan jugé décevant de l'action de groupe en droit de la consommation « à la française » tient tant au faible nombre d'actions initiées que par l'absence de jugement définitif reconnaissant la responsabilité du professionnel[1869]. Reine-Claude Mader, présidente de l'association de consommateurs CLCV (Consommation, Logement et Cadre de Vie) regrette que « l'action de groupe telle qu'elle est conçue actuellement pourrait bien avoir paradoxalement pour effet de dissuader les consommateurs et les associations, au lieu de les pousser à engager des procédures judiciaires »[1870]. Le rapport d'information sur le bilan des actions de groupe conclut également à la trop grande restriction des conditions requises pour avoir la qualité à agir, constat qui, selon ses rapporteurs, fait l'objet d'un « large consensus »[1871]. Le rapport pointe du doigt les difficultés pour les associations de financer les actions de groupe, les difficultés en termes de compétences des associations sur des sujets mal maîtrisés par celles-ci, et l'attitude naturelle de celles-ci à choisir des dossiers plutôt que d'autres pour des raisons de coût, d'image, de politique ou d'aptitudes[1872]. Ce constat est à l'origine de la proposition des rapporteurs d'élargir les conditions octroyant une qualité à agir :

> « Proposition n° 2 : Donner la qualité à agir :
>
> - aux associations dont l'objet social inclut celui du litige et ayant au moins deux ans d'existence ;

[1867] SINOPOLI Laurence, *op. cit.*, p. 33.
[1868] *Idem,* p. 31.
[1869] Assemblée nationale, 11 juin 2020, n°3085, *op. cit.*.
[1870] MADER Reine-Claude, « Action de groupe à la française : premiers retours d'une association de consommateurs », *Gazette du Palais*, 27 octobre *2015, n*°300, p. 14.
[1871] Assemblée nationale, 11 juin 2020, n°3085, *op. cit.*.
[1872] *Ibidem.*

- aux associations *ad hoc* composées d'au moins cinquante personnes physiques ou d'au moins dix entreprises constituées sous la forme de personnes morales et ayant au moins deux ans d'existence »[1873]

816. L'ouverture de l'action de groupe aux associations *ad hoc* permettrait ainsi d'assurer la couverture de l'ensemble des préjudices présents en droit de la consommation. En effet, le rapport faisait part de préjudices non représentés par les associations non pas par manque d'intérêt ou de sérieux de l'action en justice envisagée, mais par manque de compétence, par exemple les appels vains du collectif de voyageurs du RER A rejetés par l'ensemble des associations[1874]. Par conséquent, une réflexion doit être menée en matière d'action en justice dans le domaine du droit de la consommation. Il a en effet été sus-démontré que la personne concernée, en qualité de consommatrice de services traitant des données à caractère personnel, se situe dans une relation particulièrement asymétrique du fait de la structure actuelle du marché numérique. Ainsi, la seule pression médiatique ne peut pas suffire à défendre les intérêts des consommateurs sur le marché numérique, et les personnes concernées doivent pouvoir se défendre efficacement contre les violations du droit par les responsables de traitement. Lorsque le préjudice découle de la conformité du responsable de traitement au RGPD, la personne concernée dispose d'une possibilité de résolution collective des conflits supplémentaires à travers l'action de groupe.

§2 — Le potentiel protecteur de l'action de groupe en matière de données à caractère personnel

817. L'article 80 du RGPD porte sur la représentation des personnes concernées. Elle contient une obligation pour les États membres d'introduire dans leur droit national la possibilité pour la personne concernée de faire représenter ses intérêts par mandat ainsi que la possibilité pour les États membres de prévoir une telle représentation sans mandat. Ces modes de résolution des litiges sont indispensables pour assurer la réparation du préjudice de la personne concernée (A).

818. L'Union européenne semble vouloir franchir un palier de plus dans la représentation de l'individu à travers la mise en place d'une sorte de contentieux objectif, fondée sur l'anticipation du préjudice (B).

[1873] *Ibidem.*
[1874] *Ibidem.*

A. L'action fondée sur la réalisation d'un préjudice

819. L'article 80 prévoit un mécanisme de représentation des personnes concernées afin qu'elles puissent exercer ses droits et obtenir réparation. L'intermédiaire représentant la personne concernée pourra exercer ses droits en vertu de l'article 77 (droit d'introduire une réclamation auprès d'une autorité), de l'article 78 (droit à un recours juridictionnel effectif contre une autorité de contrôle), de l'article 79 (droit à un recours juridictionnel effectif contre un responsable du traitement) et de l'article 82 (droit à réparation).

820. La représentation de la personne concernée est alors confiée à « un organisme, une organisation ou une association à but non lucratif 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 dans le cadre de la protection des données à caractère personnel les concernant ». La définition des acteurs susceptibles de représenter la personne concernée est ainsi substantiellement plus large que celle prévue par la législation française en matière d'action de groupe, ce qui entraîne un régime de cohabitation entre l'action de groupe et l'action de groupe « données personnelles » assez surprenant.

821. L'article 80 (1) du RGPD dispose que :

> « La personne concernée a le droit de mandater 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 dans le cadre de la protection des données à caractère personnel les concernant, pour qu'il introduise une réclamation en son nom, exerce en son nom les droits visés aux articles 77, 78 et 79 et exerce en son nom le droit d'obtenir réparation visé à l'article 82 lorsque le droit d'un État membre le prévoit ».

822. Ainsi, l'article 80 (1) crée à la charge des États membres la possibilité pour les personnes concernées de mandater un intermédiaire pour la représentation de ses intérêts dans le cadre d'une action en cessation. Les États membres peuvent également, s'ils souhaitent le prévoir dans leur ordre juridique interne, prévoir la possibilité de créer la représentation des intérêts de la personne concernée dans le cadre d'une action en réparation du préjudice. La transposition de ces dispositions en droit français a été effectuée par l'article 38 de la loi informatique et libertés. Sont dès lors éligibles à l'initiation d'une action de groupe « données personnelles » toutes les associations éligibles à l'action de groupe ainsi que les associations ou organisations « dont l'objet statutaire est en relation avec la protection des droits et libertés lorsque ceux-ci sont méconnus dans le cadre d'un traitement de données à caractère personnel » et enfin les

associations dont la personne est membre « et dont l'objet statutaire implique la défense d'intérêts en relation avec les finalités du traitement litigieux »[1875].

823. Le régime de l'action de groupe « données personnelles » se distingue donc de celui de l'action de groupe « classique », qui, en matière de protection des données à caractère personnel, est régi par l'article 80 (2) du RGPD. Ce dernier dispose :

> « Les États membres peuvent prévoir que tout organisme, organisation, ou association visés au paragraphe 1 du précédent article, indépendamment de tout mandat confié par une personne concernée, a, dans l'État membre en question, le droit d'introduire une réclamation auprès de l'autorité de contrôle qui est compétente en vertu de l'article 77, et d'exercer les droits visés aux articles 78 et 79 s'il considère que les droits d'une personne concernés prévus dans le présent règlement ont été violés du fait du traitement ».

824. La transposition de l'article 80 (2) a été effectuée, dans la loi informatique et libertés, par son article 37, qui applique le même régime que les actions de groupe en matière de consommation. Ainsi, l'exercice d'une action de groupe à la française est bien plus restreint que celui d'une action de groupe « données personnelles » puisqu'il est réservé aux associations déclarées depuis au moins cinq ayant dans leur objet statutaire la protection de la vie privée ou des données à caractère personnel, les associations de défense de consommateurs représentatives au niveau national et agréées et les organisations syndicales de salariés ou fonctionnaires représentatives au sens du Code du travail[1876].

825. La différence de régime surprenante entre action de groupe classique et action de groupe « données personnelles » a été pointée du doigt par le rapport d'information sur le bilan des actions de groupe. Si une telle différence de régime est permise par le caractère facultatif, dans le RGPD, de l'action de groupe, la CNIL considère tout de même que la législation française « créer un décalage dommageable avec l'action collective »[1877]. Les faits sont parlants : seules deux actions de groupe avaient été engagées au 11 juin 2020 quand sept actions avec mandats avaient déjà été reçues par la CNIL au même moment[1878]. L'action de groupe « données personnelles » semble dès lors vouée à un plus grand succès, mais présuppose une identification au préalable des personnes ayant subi une violation de leur droit ou un préjudice du fait d'une violation du règlement.

[1875] Loi n°78-17 du 6 janvier 1978, Article 38 tel que modifié par l'ordonnance n°2018-1125 du 12 décembre 2018.
[1876] *Ibidem.*
[1877] Assemblée nationale, 11 juin 2020, n°3085, *op. cit.*.
[1878] *Ibidem.*

826. Les contours de l'article 80 (2) vont faire l'objet d'une précision par la CJUE. Une demande de décision préjudicielle du Bundesgerichtshof vise notamment à savoir si l'action de groupe définie par l'article 80 (2) nécessite l'identification au préalable de cas concrets faisant l'objet d'une violation de leurs droits[1879]. Les conclusions de l'avocat général plaident pour une interprétation permissive des dispositions de l'article 80 (2) permettant l'objectivisation du contentieux sans mandat[1880]. Une telle interprétation découlerait de l'effet utile de la disposition, notamment de sa distinction avec l'article 80 (1)[1881]. L'objectivisation du contentieux sans mandat aurait des effets protecteurs importants en matière de protection des données à caractère personnel, puisqu'il permettrait notamment aux organismes et associations concernés d'introduire des actions en cessation pour la violation des droits des personnes concernées en raison de la violation de règles relatives à la concurrence par exemple[1882]. Une telle complémentarité permettrait en effet de prendre en compte le fait que la personne concernée est souvent placée en position de consommateur. L'action de groupe « données personnelles » présente donc un potentiel protecteur très intéressant dans la mesure où l'action est ouverte à aux associations s'intéressant à la protection des données, dont certaines sont très actives, et peut potentiellement concerner la protection des données à caractère personnel dans sa globalité, en prenant en compte le fait qu'elle est influencée par d'autres champs du droit : droit de la consommation, droit de la concurrence, etc. Cependant, l'action de groupe « données personnelles » reste limitée à l'existence d'un préjudice déjà réalisé et ne peut pas être fondée sur l'anticipation d'un préjudice possible.

B. L'ouverture des actions représentatives de protection des intérêts collectifs des consommateurs à la protection des données à caractère personnel

827. Le RGPD n'est pas la seule source européenne garantissant une modalité collective de résolution des litiges. Le 25 novembre 2020, le législateur européen adoptait en effet la directive (UE) 2020/1828 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs[1883]. Cette directive est une avancée dans l'objectivisation du contentieux collectif de la consommation, dans la mesure où elle vise à protéger les « intérêts collectifs des

[1879] CJUE, Demande de décision préjudicielle, *Facebook Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V* ,déposée le 15 juillet 2020, C-319/20.
[1880] CJUE, Conclusion de l'avocat général M. Jean Richard de la Tour, Facebook Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V, présentées le 2 décembre 2021, C-319/20.
[1881] *Idem*, §64.
[1882] *Idem*, §84.
[1883] Directive (UE) 2020/1828, 25 novembre 2020.

consommateurs », définis à son article 3 comme « l'intérêt général des consommateurs » ou en matière de réparation du préjudice, « les intérêts d'un groupe de consommateurs »[1884].

828. L'utilisation d'un vocabulaire désignant l'intérêt collectif et l'intérêt général n'est pas dénuée de portée. Traditionnellement réservée à l'autorité publique, la défense de l'intérêt général des consommateurs résulte de vingt ans de jurisprudence de la Cour de justice[1885], qui opposera à la confusion de la défense de l'intérêt général par les organismes privés avec celle de l'autorité publique, la nature privée des organismes[1886], l'absence de pouvoirs exorbitants[1887] ou encore la nature préventive des litiges justifiant le fait que puisse ne pas porter sur des cas individuels[1888]. Ainsi, la directive s'applique « aux actions relatives aux droits divisibles (intérêts individuels homogènes ou la somme des intérêts individuels) et aux intérêts indivisibles (diffus) »[1889]. La défense d'intérêts collectifs des consommateurs a été par exemple reconnue lors d'actions introduites contre Volkswagen pour la manipulation des données relatives aux rejets des gaz d'échappement de ces véhicules[1890], ou de la contestation de clauses abusives insérées dans les conditions générales de vente d'Amazon[1891].

829. La directive 2020/1828 a notamment élargi les actions représentatives visant à protéger les intérêts collectifs des consommateurs à la protection des données à caractère personnel, en prévoyant à son annexe I que ces actions seront ouvertes à la constatation ou réparation de dommage du fait de la violation du RGPD[1892] ou de la directive *e-privacy*[1893]. Un tel élargissement permet notamment d'ouvrir les actions de groupe en cessation visant, plutôt que la réparation du préjudice, la cessation d'une situation illicite. En effet, la directive « propose aux consommateurs un recours supplémentaire à l'encontre des professionnels en cas de violation du droit de l'Union européenne sans préjudice des droits qu'ils détiennent par ailleurs en application du droit européen »[1894]. Le renforcement des actions en cessation est l'une des

---

[1884] *Idem*, Article 3(3).
[1885] KINSH Patrick, « La banalisation de l'action en cessation dans l'intérêt collectif des consommateurs », *in* D'AVOUT Louis *et al.*, « Droit international privé de l'Union européenne (2020) », *Journal du droit international (Clunet)*, n°4, octobre 2021, chronique 8.
[1886] CJCE, 1er octobre 2002, *Karl Heinz Henkel*, C-167/00, §30.
[1887] *Ibidem.*
[1888] CJUE, 28 juillet 2016, *VKI c. Amazon*, C-191/15, §51.
[1889] AZAR-BAUD Maria José, « La directive européenne sur les actions représentatives : un texte mi-figue, mi-raisin », *La Semaine Juridique Entreprise et Affaires*, n°51, 13 décembre 2020, 1542.
[1890] CJUE, 9 juillet 2020, *VKI c. Volkswagen*, C-343/19.
[1891] CJUE, 28 juillet 2016, C-191/15, *op. cit.*.
[1892] Directive (UE) 2020/1828, 25 novembre 2020, Annexe 1(56).
[1893] *Idem*, Annexe 1(10).
[1894] MÉTAIS Philippe, VALETTE Élodie, « La directive actions représentatives : un nouvel élan pour les actions de groupe ? », *Dalloz actualité*, 16 décembre 2020.

motivations ayant encouragé la Commission à remplacer la directive n° 2009/22/CE[1895]. L'ouverture des actions en cessation est notamment effectuée par l'article 8 (3) de la directive qui dispose :

> « Pour qu'une entité qualifiée demande une mesure de cessation, les consommateurs individuels ne sont pas tenus d'exprimer leur volonté d'être représentés par ladite entité qualifiée. L'entité qualifiée n'est pas tenue de prouver :
>
> a) une perte ou un préjudice réels subis par les consommateurs individuels lésés par l'infraction visée à l'article 2, paragraphe 1 ; ou
>
> b) l'intention ou la négligence du professionnel ».

830. L'indépendance de l'action en cessation avait déjà été rappelée à plusieurs reprises par la CJUE, qui a affirmé la possibilité pour les actions de groupe de s'exercer sur des clauses non utilisées dans des contrats déterminés, mais uniquement recommandés par des professionnels[1896]. L'EDPS envisage d'ailleurs la complémentarité entre l'action de groupe « classique » et l'action de groupe prévues dans le RGPD et l'action de groupe prévue dans la directive comme s'articulant autour de la réalisation du préjudice[1897]. En effet, le RGPD conditionne la possibilité de recours à une action représentative à la violation d'un droit de la personne concernée et non à la violation d'une disposition du règlement. L'indépendance de l'action en cessation ne semble pas intégrée à la proposition de loi pour un nouveau régime de l'action de groupe enregistrée à la Présidence de l'Assemblée nationale le 15 septembre 2020. En effet, la proposition de loi propose l'introduction d'un nouvel article 2279 du Code civil conditionnant encore l'action de groupe à l'existence d'un dommage :

> « Lorsque plusieurs personnes physiques ou personnes morales, à l'exclusion de l'État, placées dans une situation similaire, subissent un dommage causé par une même personne, ayant pour cause commune un manquement de même nature à ses obligations légales ou contractuelles, une action de groupe peut être exercée en justice au vu des cas individuels présentés par le demandeur »[1898].

[1895] Commission européenne, *Proposition de Directive du Parlement européen et du Conseil relative aux actions représentatives dans le domaine de la protection des intérêts collectifs des consommateurs et abrogeant la directive 2009/22/*CE, Bruxelles, 11 avril 2018, COM(2018) 184 final, §I ; Directive (UE) 2020/1828, 25 novembre 2020, considérant 5.

[1896] CJCE, 27 juin 2000, *Océano Grupo Editorial SA*, C-240/98 à C-244/98, §27 ; CJCE, 24 janvier 2002, Commission/Italie, C-372/99, §14 ; CJUE, 26 avril 2012, C-472/10, *op. cit.*, §37.

[1897] EDPS, *Avis 8/2018 du CEPD sur le paquet législatif « Une nouvelle donne pour les consommateurs »*, 5 octobre 2018, §62.

[1898] Assemblée nationale, *Proposition de loi pour un nouveau de régime de l'action de groupe*, Enregistré à la Présidence de l'Assemblée nationale le 15 septembre 2020, n°3329.

La proposition de loi devra donc faire l'objet d'une redéfinition importante afin d'intégrer d'ici le 25 décembre 2002 les actions en défense de l'intérêt collectif, en plus des actions « en défense des intérêts individuels homogènes »[1899].

831. L'impact de la directive sur l'action de groupe à la française est difficile à déterminer. Par l'adoption d'une directive de « compromis »[1900], la Commission européenne a fait le choix de laisser une grande marge de manœuvre aux États membres, tout en s'assurant de l'existence de l'ensemble de la palette des actions représentatives dans l'ensemble des États membres. Ce choix se justifie par la volonté d'harmoniser les dispositions européennes en matière d'actions exercées en défense de l'intérêt collectif des consommateurs, dont l'absence dans le droit interne de neuf États membres permettait aux professionnels s'y implantant d'être immunisés contre ces actions en vertu de la loi de procédure du for du défendeur[1901].

832. Notons qu'en France, la directive 2020/1828 nécessitera une transposition en droit national, et donc un nouveau débat démocratique sur les contours de l'action de groupe. Une nouvelle discussion « est l'occasion de réformer le régime de l'ensemble des actions de groupe afin d'en faciliter l'exercice »[1902]. La directive comporte notamment des éléments novateurs en matière de production des éléments de preuve[1903]. Très attendu, le mécanisme d'*opt-out* pour l'adhésion des consommateurs à un litige les concernant n'a pas été consacré par la directive, même si la nouvelle possibilité pour le consommateur d'exprimer une telle volonté tacitement peut se révéler « être un outil aussi puissant et efficace que l'*opt-out* »[1904]. Une partie de la doctrine regrette finalement l'absence de certaines dispositions qui auraient facilité la défense des intérêts collectifs des consommateurs tels qu'une obligation de financement des litiges ou la révocation du principe « *loser pays* »[1905].

833. Conclusion de section. — Les actions représentatives sont des mécanismes permettant aux consommateurs de rééquilibrer la relation qu'ils entretiennent avec les professionnels, notamment en vertu de considérations économiques et informationnelles. En matière de

---

[1899] AZAR-BAUD Maria José, décembre 2020, *op. cit.* 1542 ; AZAR-BAUD Maria José, « *Allegro ma non troppo* (à propos de la transposition en France de la directive sur les actions représentatives en protection des intérêts collectifs des consommateurs) », *D.*, 2021, p. 232.
[1900] AZAR-BAUD Maria José, 2021, *op. cit.*, p. 232.
[1901] D'AVOUT Louis *et al.*, « Droit international privé de l'Union européenne (2020) », *Journal du droit international (Clunet)*, n°4, octobre 2021, chronique 8.
[1902] USUNIER Laurence, « L'action de groupe européenne au milieu du gué », *RTD Civ.*, 2021, p. 370.
[1903] Directive (UE) 2020/1828, 25 novembre 2020, Article 18 ; CATTALANO Garance, « Intérêts collectifs des consommateurs : adoption de la directive (UE) 2020/1828 relative aux actions représentatives », *Droit des contrats*, 2021, n°1, p. 4.
[1904] AZAR-BAUD Maria José, 2021, *op. cit.* p. 232.
[1905] AZAR-BAUD Maria José, 17 décembre 2020, *op. cit.*

protection des données à caractère personnel, ce rééquilibrage présente un intérêt substantiel pour les personnes concernées, souvent placées en position de consommatrices sur le marché numérique. L'apparition de l'action de groupe en 2014 et son extension à la protection des données à caractère personnel en 2016 ont ainsi été des avancées non négligeables dans la possibilité pour la personne concernée de faire valoir ses droits face aux responsables de traitement. Cependant, l'évolution des actions représentatives souffre encore de nombreuses lacunes quant à l'effectivité de la défense des intérêts collectifs des consommateurs et des personnes concernées. Si l'action de groupe « données personnelles » a été largement acceptée par la CNIL, l'action de groupe classique souffre encore de la réticence du législateur et du juge français. Dans cette optique, l'adoption en 2020 de la directive relative aux actions représentatives est susceptible de faire évoluer l'action de groupe *à la française* en obligeant le législateur français à la repenser[1906] et en encourageant le juge à adopter une jurisprudence moins hostile, notamment en vertu de l'effet utile de la directive[1907].

[1906] Le bilan de l'action de groupe en France fait état de très peu d'actions intentées depuis la loi de 2014 créant ce mécanisme. Ce bilan pourrait potentiellement apaiser les craintes de dérives à l'américain et permettre une ouverture plus large des actions de groupe.
[1907] USUNIER Laurence, *op. cit.* , p. 370.

Conclusion du Chapitre 2

834. La prise en compte de la relation asymétrique entre la personne concernée et le responsable de traitement est tout d'abord apparu sous l'angle du droit de la consommation, le législateur européen constatant l'existence d'acteurs du numérique comptabilisant de nombreux utilisateurs dont les dommages trop complexes ou ne présentant pas ou peu de dommages (réels ou évalués) ne permettait pas aux personnes concernées d'obtenir du responsable de traitement le respect du cadre juridique en matière de protection des données ou la compensation de leurs dommages. Par l'action de groupe, le législateur souhaite rétablir l'équilibre entre la personne concernée et le responsable de traitement, l'aspect collectif des recours devant compenser l'asymétrie de connaissances et de moyens.

835. Le bilan est cependant mitigé. Premièrement, l'action de groupe relevant du domaine régalien de la justice, les États membres ne se sont pas empressés de faciliter les recours collectifs en matière de protection des données à caractère personnel. En France, la peur des *class actions* à l'américaine a justifié la réticence du législateur à ouvrir de manière plus large les actions de groupe. Deuxièmement, l'action de groupe ne semble pas pouvoir remédier au déséquilibre de la concurrence sur le marché du numérique, les *Big Tech* ayant réussi à consolider une place quasi monopolistique de *winner-take-all*. Dès lors, la distorsion sans précédent de la concurrence et la présence d'acteur à la puissance inédite ont motivé le législateur à réguler l'économie numérique. Si ces dispositions présentent des lacunes, sont tardives et ne sont même pas encore adoptées, leur possible future entrée en vigueur aura un aspect protecteur vis-à-vis de la personne concernée.

836. En rétablissant la concurrence loyale sur le marché numérique et en permettant la réparation des dommages causés par la violation de la législation européenne en matière de protection des données à caractère personnel, le consentement de la personne concernée ne se voit que renforcé par l'offre de choix de services lui permettant de faire entrer la protection des données à caractère personnel dans son choix de prestataires de services, et par la possibilité d'obtenir la réparation de dommages liés au non-respect de son consentement.

Conclusion du Titre 2

837. La dimension économique des données à caractère personnel entrave la capacité du législateur d'aborder la question de la protection des données à caractère personnel exclusivement sous l'angle de la liberté individuelle. En effet, le rapport de force entre la personne concernée et le responsable de traitement est substantiellement asymétrique et requiert du législateur de déterminer les contours du projet numérique commun européen ainsi que de permettre aux personnes concernées de disposer d'une force juridique suffisamment importante pour faire face aux « géants du numérique » (plus généralement désignés sous l'anglicisme « *big tech* »). Or, cet enjeu entre directement en concurrence avec les libertés économiques telles que protégées par l'Union européenne, y compris au sein de la Charte, en particulier la liberté d'entreprendre. Dès lors, l'arbitrage du législateur européen et à défaut, le législateur national est essentiel.

838. L'arbitrage du législateur européen est d'abord intervenu pour protéger les données à caractère personnel au niveau individuel, avec comme objectif de redonner aux personnes concernées le contrôle de leurs données à caractère personnel. Or, si cette approche permet de réguler de manière satisfaisante la relation entre une personne concernée et un responsable de traitement, l'approche n'est pas suffisamment évolutive pour faire face à la multiplication des acteurs numériques. Ainsi, le RGPD place la personne concernée devant trop de choix, trop de connaissances à assimiler, et trop peu de temps pour repérer les anomalies dans les demandes de consentement. L'arbitrage du législateur européen est ensuite intervenu pour protéger les données à caractère personnel au niveau collectif, avec comme objectif de rétablir une concurrence loyale sur le marché européen du numérique. Dans ce cadre, les données à caractère personnel sont protégées de manière indirecte, ce qui permet au législateur de prendre en compte les besoins collectifs en matière de protection des données tout en procédant à un équilibre sectoriel de cette protection avec la protection des libertés du marché européen. Cependant, il peut être regretté que cet arbitrage n'arrive que tardivement, les acteurs du numérique s'étant déjà créé une place de *winner-take-all* et les pratiques déjà bien ancrées dans les habitudes des internautes européens. Ainsi, redonner le contrôle des données à caractère personnel à travers le consentement de la personne concernée suppose de s'intéresser au contexte dans lequel se trouve la personne concernée, afin de garantir que les garanties textuelles se traduisent en pratique en garanties réelles. Le seul instrument du RGPD ne pouvait

garantir une telle réalité du consentement en pratique dans la mesure où il ne prend en compte que la relation entre la personne concernée et le responsable de traitement, ainsi que la chaîne de sous-traitance utilisée par ce responsable. Or, le mouvement de microservices couplé à l'existence de très grandes plateformes quasiment monopolistiques ne permettait pas au Règlement de prendre en compte la fatigue du consentement et les rapports économiques déséquilibrés entre la personne concernée et le responsable de traitement.

839. Dès lors, le RGPD ne peut se suffire à lui-même et nécessite que le législateur européen continue ses efforts en matière de législation complémentaire afin que la réalité du marché ne réduise pas à néant les dispositions protectrices du règlement. L'activité législative européenne, à travers les propositions de DMA, DSA, AI Act et Règlement *e-privacy* montre la volonté des décisionnaires européens de reprendre le contrôle sur l'environnement numérique[1908].

[1908] Citons par exemple les propos du Commissaire européen Thierry Breton qui appelait, le 19 janvier 2022, à mettre fin au « Far-West dominant dans notre espace informationnel » et à rendre ce qui est interdit *offline* interdit *online*. Public Sénat, « GAFAM : le Parlement européen s'attaque au « Far-West » du numérique », 20 janvier 2022, disponible sur https://www.publicsenat.fr/article/politique/gafam-le-parlement-europeen-s-attaque-au-far-west-du-numerique-191984 (consulté en août 2022).

Conclusion de la Partie 2

840. Si le consentement RGPD a été une évolution législative permettant à la personne concernée d'obtenir plus de contrôle de ses données à caractère personnel, force est de constater que ce consentement présente tout de même des limites. Ces limites appellent à une réflexion juridique de fond afin de déterminer les situations où le consentement nécessite des garanties supplémentaires pour être valide ou des précisions supplémentaires pour s'articuler correctement avec d'autres dispositions juridiques et les situations où le consentement est à proscrire du fait de l'impossibilité pour la personne concernée d'émettre un consentement libre et éclairé.

841. À ce titre, l'étude a d'abord démontré que certaines dispositions du RGPD ne sont soit pas assez précises, soit sont contre-productives au regard des objectifs auxquels le RGPD aspire. Ainsi, la complexité des traitements impliquant une prise de décision automatisée ou un transfert de données hors de l'Union européenne entrave la capacité de la personne concernée d'exercer un consentement éclairé, la faible temporisation de l'exigence de consentement explicite ne permettant pas de compenser la quantité de connaissances nécessaires à l'exercice d'un consentement valide. Or, à l'occasion du bilan des deux ans d'application du RGPD établi en 2020, la Commission a pris acte des difficultés liées à certains défis posés par l'application du RGPD par les nouvelles technologies, mais n'a pas remis en question les mécanismes de transferts internationaux de données qui constituent pour elle une « boîte à outils modernisée » permettant de garantir que « les données continuent à bénéficier d'un niveau élevé de protection »[1909]. Ces difficultés s'ajoutent à la complexe articulation entre le consentement et les autres bases légales fondant les traitements de données à caractère personnel. Il a été démontré que le consentement ne constituait pas le choix le plus instinctif du point de vue économique dans la mesure où le simple retrait du consentement de la personne concernée peut se traduire dans certaines situations comme une perte de revenus du point de vue du responsable de traitement. Or, puisque le responsable de traitement est la personne en charge de choisir la base légale applicable au traitement de données à caractère personnel, la pratique montre une tension entre les bases légales du consentement RGPD et du consentement contractuel et entre les bases légales du consentement et de l'intérêt légitime. Si une telle tension peut être en partie résolue par une interprétation jurisprudentielle de la Cour de Justice, le législateur européen est

[1909] Commission européenne, COM(2020) 264 final, *op. cit*.

tout de même appelé à clarifier le régime applicable à la publicité comportementale, nœud cristallisant l'ensemble de ces tensions.

842. L'étude a ensuite démontré que le RGPD ne peut se suffire à lui-même dans la mesure où il ne régit que la relation entre la personne concernée et le responsable de traitement (et ses sous-traitants) dans le cadre d'un traitement déterminé. Dès lors, l'environnement numérique dans lequel évolue la personne concernée et qui implique la relation entre celle-ci et un nombre conséquent de responsables de traitements n'est pas pris en compte par le règlement. Dès lors, le RGPD entraîne une série d'« effets secondaires » contre-productifs en ce qui concerne la réalité du consentement. Sursollicitée par les demandes de consentement, dont la forme est pensée pour l'encourager à consentir, la personne concernée se voit privée de la capacité d'exercer un consentement libre de toute influence et éclairé. Pourtant, certaines difficultés avaient été repérées par le législateur, qui s'était efforcé d'ébaucher certaines solutions dans le RGPD et dans le Règlement *ePrivacy*. Or, ces solutions ne sont pas encore mises en place, soit parce qu'elles sont facultatives dans le RGPD, ou relèvent du Règlement *ePrivacy* non adopté à ce jour. De plus, l'environnement numérique implique une relation asymétrique entre le responsable de traitement et la personne concernée, dont l'asymétrie de pouvoir entrave la capacité de la personne concernée d'exercer un consentement libre. Dès lors, le RGPD ne peut pas se suffire à lui-même dans la mesure où la protection des données à caractère personnel ne peut pas s'envisager comme protection uniquement individuelle, mais doit également être garantie dans son aspect collectif. Le consentement ne saurait ainsi être libre sans la prémisse d'un droit de la concurrence et de la consommation permettant de protéger la personne concernée dans sa position de consommatrice. En effet, la liberté suppose le choix, ce que la position monopolistique des responsables de traitement et leurs décisions unilatérales envers les utilisateurs de leur service entravent.

843. Ainsi, les limites du consentement traduisent un manque de prise en compte du contexte dans lequel se trouvent le responsable de traitement, les personnes avec qui celui-ci interagit et les personnes concernées. Les prochaines évolutions jurisprudentielles et législatives seront à ce titre essentielles à suivre pour évaluer la (future) validité du consentement.

CONCLUSION

844. La double nature de la stratégie européenne de protection des données à caractère personnel entre protection des droits fondamentaux et soutien à l'un des piliers de l'économie européenne, est finalement au cœur des réflexions concernant le consentement au sein de l'Union européenne. En effet, la place accordée au consentement dans l'ordre juridique européen en matière de protection des données, ainsi que ses modalités et ses faiblesses ne peuvent pas se comprendre sans s'intéresser à la volonté du législateur d'une part, de préserver le marché intérieur européen et d'autre part, de protéger les droits fondamentaux des citoyens européens. Or, si cette double volonté a pu être regrettée tant les enjeux économiques et les enjeux de protection des droits fondamentaux sont antagonistes, le législateur européen a tout de même fait l'effort de concilier ces intérêts, cherchant à faire de la protection des données à caractère personnel un facteur concurrentiel différentiant sur le marché européen. Ainsi, la Commission européenne a procédé à l'identification d'un cercle vertueux autour de la confiance du consommateur : si le consommateur contrôle — et a le sentiment de contrôler suffisamment — ses données à caractère personnel, alors il aura confiance dans les produits et services proposés sur le marché européen.

845. Dans ce cadre, la thèse a démontré que le consentement a été un élément central de la démarche d'*empowerement* de la personne concernée. Tenant compte du bilan de la directive 95/46/CE, le législateur a adapté l'intensité du consentement aux pratiques modernes, prenant en compte les nouveaux rapports entre personnes concernées et responsables de traitement. Ainsi, parce que la complexité de la technologie ne permet pas une compréhension facile des enjeux et limites des traitements des données à caractère personnel, le principe de transparence s'est placé au centre du Règlement général sur la protection des données. Parce que la mondialisation, l'apparition des GAFAM, et la présence de services quasi monopolistiques ont profondément déséquilibré la relation entre la personne concernée et le responsable de traitement, les critères de validité du consentement de la personne concernée se sont sophistiqués. Par cette démonstration, la thèse s'est attachée à démontrer le potentiel protecteur du consentement RGPD, dont la robustesse dépend également de l'interprétation de ses dispositions par les autorités de contrôle et les juges. Le Règlement présente donc des opportunités intéressantes quant à l'adéquation du consentement avec la volonté de la personne concernée. En conditionnant ses obligations à la réalisation de leurs objectifs, le RGPD subjectivise l'obligation en encourageant les responsables de traitement à mettre en place des

mesures techniques et organisationnelles en vue de la réalisation d'un objectif. Dès lors, le consentement ne sera pas valide du fait de l'existence d'un certain nombre de mentions ni par l'utilisation d'une modalité particulière quant à la demande de consentement. Le consentement sera évalué au contraire du point de vue de la personne concernée, la validité du consentement étant obtenue si la personne concernée est libre de ses choix et éclairée dans leur exercice. Il s'agit ici du premier résultat de la thèse.

846. Le deuxième résultat de la thèse est lié à l'insertion du RGPD au sein d'une stratégie globale du numérique. La Commission a dévoilé sa stratégie pour les données[1910], envisage la protection des données à caractère personnel dans le cadre du marché unique des données[1911] et plus largement, poursuit l'objectif inscrit dans ses priorités 2019-2024 d'une « Europe adaptée à l'ère numérique »[1912]. L'insertion de la protection des données à caractère personnel au sein d'une stratégie économique est symptomatique de la place des droits fondamentaux au sein de l'Union européenne. La consécration de la Charte des droits fondamentaux de l'Union européenne au sein du droit primaire n'a par exemple pas eu les effets escomptés sur la protection des droits fondamentaux au sein de l'Union européenne, n'altérant pas — ou trop peu — l'équilibre entre protection des droits fondamentaux et les objectifs poursuivis par l'Union[1913]. En effet, la Cour de justice notamment semble « vouloir préserver le marché intérieur des effets potentiels des droits fondamentaux qui pourraient remettre en cause l'intégrité de celle-ci »[1914]. La prédominance de la logique du marché est intrinsèquement liée à l'histoire de la construction européenne, dont l'Union des États membres est d'abord une union « par le marché »[1915], et dont la citoyenneté est d'abord une citoyenneté de marché[1916].

Or, le prisme du marché dans la protection des données à caractère personnel a entraîné des limites importantes quant à la réalité du consentement de la personne concernée. Ces limites proviennent tout d'abord de l'embarras du législateur face à des éléments antagonistes, dont l'arbitrage résulte en une ingérence soit dans les libertés économiques garanties sur le marché

[1910] Commission européenne, COM (2020) 66 final, *op. cit.*
[1911] Commission européenne, COM (2015) 192 final, *op. cit*.
[1912] Commission européenne, « Une Europe adaptée à l'ère numérique », *ec.europa.eu*, disponible sur https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_fr (consulté en janvier 2022).
[1913] TINIÈRE Romain, « Propos introductifs », *in* TINIÈRE Romain, VIAL Claire (dir.), *Les dix ans de la Charte des droits fondamentaux de l'Union européenne. Bilan et perspectives*, Paris, Bruylant, 2020, p. 21.
[1914] COMBET Mathieu, « La dilution de la Charte des droits fondamentaux de l'Union européenne dans les règles relatives aux libertés de circulation du marché intérieur », *in* TINIÈRE Romain, VIAL Claire (dir.), *Les dix ans de la Charte des droits fondamentaux de l'Union européenne. Bilan et perspectives*, Paris, Bruylant, 2020, p. 59.
[1915] QUESNEL Martin, « Concurrence entre économie et droit aux racines de l'identité européenne », *in* CARPANO Éric, MARTI Gaëlle (dir.), *Démocratie et marché dans l'Union européenne en crise*, p. 57.
[1916] TUORI Kaarlo, « La Constitution économique parmi les Constitutions européennes », *Revue internationale de droit économique*, 2011/4, Tome XXV, p. 574.

intérieur, soit en une ingérence dans la protection des droits fondamentaux des personnes concernées. Ainsi, le tiraillement du législateur entre protection effective du droit à la protection des données à caractère personnel et protection du marché intérieur est particulièrement visible sur des domaines très friands d'exploitation des données à caractère personnel : la publicité ciblée, l'intelligence artificielle, les transferts de données à caractère personnel hors Union européenne, etc. Tantôt silencieux, tantôt ambigu, tantôt trop verbeux, le législateur a adopté des dispositions soit trop peu précises pour être protectrices, soit contre-productives au regard des objectifs auxquels le RGPD aspire. Le juge n'a pas non plus réussi à corriger par une interprétation jurisprudentielle harmonisée les carences législatives en matière de consentement au traitement de ses données à caractère personnel. Il est arrivé que le juge se montre particulièrement protecteur de la personne concernée. Par exemple, la Cour de Justice de l'Union européenne n'a pas hésité à parfois faire primer la protection des données à caractère personnel sur des considérations économiques importantes du marché intérieur, à l'image de l'invalidation du *Safe Harbor* puis du Bouclier de protection des données (BPD ou *Privacy Shield*) à la suite des différents recours initiés par Maximilian Schrems[1917]. Ces décisions, et notamment la décision invalidant le *Privacy Shield* avaient en effet plongé les acteurs économiques « dans un grand désarroi »[1918]. Dans d'autres situations, le juge s'est montré prudent quant aux répercussions économiques de ses décisions, comme c'est actuellement le cas en ce qui concerne la question des cookies. Cette situation est pourtant à déplorer tant l'exercice d'équilibriste auquel s'adonne le législateur complexifie inutilement la protection des données à caractère personnel. La prise de décision du législateur est pourtant essentielle, afin de ne pas transformer « ce qui devrait être un choix collectif et politique en une multitude d'arbitrages individuels totalement absurdes »[1919].

847. Ainsi, et il s'agit du troisième résultat majeur de la thèse, le RGPD nécessite d'être le sujet d'une réflexion plus globale quant aux enjeux de la protection des données à caractère personnel. Notamment, le consentement est par nature lié à son émetteur, la personne concernée. Cette dernière présente de nombreuses facettes à la fois source de données, consommatrice de services, personne raisonnable, personne capable, destinataire de droits, etc. Dans ce contexte, le RGPD ne saurait se suffire à lui-même, d'autant plus que certains enjeux essentiels restent encore ignorés du Règlement. Il a notamment été démontré que l'adoption du

[1917] CJUE, 6 octobre 2015, C-362/14, *op. cit.* ; CJUE, 16 juillet 2020, C-311/18, *op. cit.*.
[1918] DE TERWANGNE Cécile, GAYREL Claire, « Flux transfrontière de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt *Schrems* », *Cahiers droit européen*, 2017/1, p. 38.
[1919] NETTER Emmanuel, 2021, *op. cit.*, p. 226.

Règlement n'a pas permis de prendre en compte de manière suffisante la situation dans laquelle la personne concernée évolue. Par exemple, si le retrait du consentement constitue une avancée importante du RGPD, ce dernier ne prend pas en compte l'existence plus globale de barrières de sortie du service utilisé par la personne concernée, qui n'est certes plus captive légalement, mais demeure dépendante du responsable de traitement économiquement ou socialement. Le législateur n'a également pas réussi à anticiper les effets secondaires du renforcement du consentement. La personne concernée est supposée exercer librement et de manière éclairée son consentement face à des demandes de consentement toujours plus nombreuses et toujours plus sophistiquées dans l'objectif d'obtenir son consentement. La thèse a ainsi démontré que l'ouverture de la protection des données aux enjeux nés de la situation de la personne concernée par rapport au responsable de traitement nécessitait un approfondissement supplémentaire. C'est le cas notamment en matière d'accès à la justice, de prise en compte des *dark patterns*, de fatigue du consentement, d'accès à des services monopolistiques, etc. Les évolutions du cadre législatif en matière de numérique et de nouvelles technologies pourront peut-être apporter des précisions et protections supplémentaires permettant d'évaluer le consentement par rapport à la situation réelle de la personne concernée. En effet, il a été démontré que le RGPD ne saurait se suffire à lui-même tant il semble que certains enjeux plus globaux restent encore ignorés par le Règlement.

848. Enfin, la protection des données à caractère personnel doit sortir du simple antagonisme entre marché et protection des droits fondamentaux, et faire l'objet d'une prise en compte des enjeux démocratiques attachés aux traitements des données à caractère personnel par les acteurs de droit privé. Si cette acception pouvait avoir un caractère contre-intuitif il y a encore quelques années — les enjeux démocratiques relevant traditionnellement des relations entre les particuliers et l'État —, les révélations d'Edward Snowden quant à l'affaire PRISM puis l'affaire *Cambridge Analytica* sont deux exemples emblématiques de l'influence des acteurs privés sur des aspects intrinsèquement liés à la démocratie, telle que l'étendue des pouvoirs de surveillance de l'État ou les questions liées au suffrage. L'autorité britannique de protection des données a notamment mis en évidence les dérives de l'utilisation des données à caractère personnel par les partis politiques, créant une asymétrie d'information entre les groupes de votant problématique pour la tenue d'un processus électoral démocratique[1920]. Le Parlement européen a estimé que « des garde-fous électoraux traditionnels ("hors ligne") » soient mis en

[1920] ICO, *Democracy disrupted ? Personal information and political influence*, 11 janvier 2018, p. 47.

place sur l'environnement numérique[1921]. Les appels à la régulation de ces dérives se multiplient, car « au-delà de la protection des données personnelles des individus, les enjeux sont maintenant de l'ordre de l'intégrité des institutions et des processus démocratiques »[1922]. Dans ce cadre, la protection des données à caractère personnel a vocation à interdire la manipulation de l'individu, mais également de garantir sa liberté d'expression, le phénomène d'autocensure étant intrinsèquement corrélé à la sensation de surveillance[1923].

849. La présence d'enjeux relevant de la démocratie et de l'État de droit pose la question de l'opportunité de l'intégration du RGPD non pas dans une stratégie économique, mais dans l'Union de valeurs telle qu'elle pourrait être envisagée à travers l'article 2 du Traité sur l'Union européenne[1924]. La protection des données à caractère personnel étant présente dans le droit primaire — à travers l'article 8 de la Charte des droits fondamentaux et l'article 16 (1) du Traité sur le fonctionnement de l'Union européenne — et le RGPD s'inscrivant dans la recherche d'une Union de valeur présentée par l'article 2 du TUE, l'objectif annoncé par le RGPD de concevoir le traitement de données à caractère personnel « pour servir l'humanité »[1925] pourrait être le cœur de la stratégie déployée par la Commission. Une telle conception de la protection des données à caractère personnel permettrait de déployer non pas une démarche d'autonomie de la protection des données à caractère personnel par rapport à d'autres droits,[1926] mais au contraire l'inscription de la protection des données à caractère personnel dans des enjeux plus globaux comme le droit à la vie privée, la protection de la dignité humaine ou encore la lutte contre les discriminations. Le respect de la vie privée n'est mentionné qu'une seule fois dans le Règlement[1927], alors même que nous adhérons aux propos de Yves Poullet rappelant que « la

---

[1921] Parlement européen, *Résolution du Parlement européen du 25 octobre 2018 sur l'exploitation des données des utilisateurs de Facebook par Cambridge Analytica et les conséquences en matière de protection des données* (2018/2855 [RSP]).

[1922] Commission de l'éthique en science et en technologie, « Cambridge Analytica : la citoyenneté numérique et la démocratie mises à l'épreuve », *ethique.gouv.qc.ca*, 23 mars 2018, disponible sur https://www.ethique.gouv.qc.ca/fr/actualites/ethique-hebdo/eh-23-mars-2018/ (consulté en janvier 2022).

[1923] V. par exemple SLEEPER Manya *and al.* « The Post that Wasn't: Exploring Self-Censorship on Facebook », *Proceedings of the 2013 Conference on Comuter Supported Cooperative Work – CSCW'13*, pp. 793–802.

[1924] L'article 2 du Traité sur l'Union européenne dispose : « L'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, d'État de droit, ainsi que de respect des droits de l'homme, y compris du droit des personnes appartenant à des minorités. Ces valeurs sont communes aux États membres dans une société caractérisée par le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité et l'égalité entre les femmes et les hommes ».

[1925] RGPD, 27 avril 2016, considérant 4.

[1926] V. TAMBOU Olivia, *Manuel de droit européen de la protection des données à caractère personnel*, 1re édition, Bruxelles, Bruylant, 2020, pp. 21-29 ; ROBUSTELLI Ludovica, « La distinction entre les articles et 8 de la Charte dans la jurisprudence de la Cour de Justice de l'Union européenne », *in* TINIÈRE Romain, VIAL Claire (dir.), *Les dix ans de la Charte des droits fondamentaux de l'Union européenne. Bilan et perspectives*, Paris, Bruylant, 2020, pp. 29-40.

[1927] RGPD, 27 avril 2016, considérant 4.

protection des données n'est jamais qu'au service » de la protection de la vie privée[1928]. La démarche, timidement entamée par la CJUE[1929], signifierait de dépasser le paradigme de contrôle qui traverse la protection des données à caractère personnel[1930], privilégiant une réflexion de ses contours au niveau de la société au détriment d'une protection individuelle qui transforme la protection des données à caractère personnel en « un pur débat de technique juridique sans âme »[1931].

[1928] POULLET Yves, 2018, *op. cit.*, p. 21. V. également DEGRAVE Élise, *L'e-gouvernement et la protection de la vie privée*, 1re édition, Bruxelles, Larcier, 2014, p. 105.
[1929] Les articles 7 et 8 de la Charte sont souvent conjointement analysés v. pour des exemples récents CJUE, 15 juin 2021, C-645/19, *op. cit.* ; CJUE, 5e ch., 17 juin 2021, *MICM*, C-597/19, §99 ; CJUE, Gde Ch., 22 juin 2021, *Randstad Italia SpA*, C-439/19, §41.
[1930] Le rejet du contrôle des données à caractère personnel comme solution à la protection des données à caractère personnel a rapidement été plaidé par la doctrine américaine. SCHWARTZ Paul M., «Internet Privacy and the State», *Connecticut Law Review*, 2000, Vol. 32, pp. 815–859; ALLEN Anita L., «Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm», *Connecticut Law Review*, 2000, Vol. 32, pp. 861–875.
[1931] POULLET Yves, 2018, *op. cit.*, p. 21.

BIBLIOGRAPHIE

I. OUVRAGES ET THÈSES NON JURIDIQUES

ARISTOTE, *Éthique à Nicomaque*, Paris, Le livre de poche, Les classiques de la philosophie, édition 1992, 448 pages.

AUDÉ Benoite, *De la perception sociale à la discrimination : une contribution à l'étude des déterminants précoces des comportements discriminatoires*, Thèse de Psychologie sous la direction de RIC François, Université de Bordeaux, 2015, 237 pages.

BASTART Jennifer, *La détection de la discrimination par un observateur : Le rôle de la catégorisation sociale du discriminateur et de la légitimité du comportement du discriminateur*, Thèse pour l'obtention du grade de docteur en sciences cognitives, psychologie et neurocognition sous la direction de DELMAS Florian et MULLER Dominique, Université de Grenoble, 2006, 372 pages.

BECK Ulrich, *La société du risque. Sur la voie d'une autre modernité,* Paris, Aubier, 2001, 528 pages.

BERLIN Isahia, *Éloge de la liberté,* Paris, Calmann-Lévy, 1994, 288 pages.

BLANC Nathalie, **BROUILLET** David, *Mémoire et compréhension*, Paris, Eyrolles, 2003, 190 pages.

CADIAT Anne-Christine, **MICHAUX** Stéphanie, *Les 5 forces de Porter. Comprendre les sources des avantages concurrentiels*, Paris, 50 minutes, 2015, 58 pages.

CHIAPPERINO Luca, *From Consent to Choice: The Ethics of Empowerment-Based Reforms*, Thèse pour l'obtention du grade de docteur en Fondations et Éthique des Sciences Vivantes sous la direction de TESTA Giuseppe, MINUCCI Saviero et TENGLAND Per-Anders, European School of Molecular Medicine, 248 pages.

CICERON, *De officiis*, Livre III, traduit par Charles APPUHN, Cicéron, Des devoirs. Paris, Garnier, 1933, disponible sur https://droitromain.univ-grenoble-alpes.fr/Francogallica/deofficiis3_fran.htm

CITTON Yves, *L'économie de l'attention : nouvel horizon du capitalisme ?*, Paris, La découverte, 2014, 328 pages.

D'AQUIN Thomas, *Summa* Theologica, Tomus Octavus, 1860.

DAVENPORT Thomas H., **BECK** John C., *The Attention Economy*, Cambridge, Harvard Business School Press, 2001, 255 pages.

DEMEULANAERE Pierre, *Les normes sociales. Entre accords et désaccords*, Paris, Presses Universitaires de France, 2003, 304 pages.

Descartes, *Lettre au Père Mesland du 9 février 1945.*

Epictète, *Manuel*, XIV.

ESFELD Michaël, *La philosophie de l'esprit – Une introduction aux débats contemporains*, Paris, Armand Colin, 2020, 3e ed., 256 pages.

FORTIN Claudette, **ROUSSEAU** Robert, *Psychologie cognitive : une approche de traitement de l'information*, Québec, Presses de l'Université du Québec, 2016, 412 pages.

FRAISSE Genevève, *Du consentement*, Paris, Éditions du Seuil, édition augmentée, 2007, 160 pages.

KANT Emmanuel, *Éléments métaphysiques de la doctrine du droit (Première partie de la Métaphysique des mœurs suivis d'un essai philosophique sur la paix perpétuelle et d'autres petits écrits relatifs au droit naturel*, traduit de l'allemand par BARNI Jules, Paris, Auguste Durand, 1853, 392 pages.

KANT Emmanuel, *Critique de la raison pratique*, Paris, Edition Félix Alcan, 1888, traduit de l'allemand par François PICAVET, 334 pages.

KENNEY Martin, *Understanding Silicon Valley: The Anatomy of an Entrepreneurial Region*, Chicago, University of Chicago Press, 2000, 304 pages.

KOUAKOU Dogui, *Indépendance des auditeurs et enjeux éthique de la certification du système de gestion environnement ISO 14001*, Thèse présentée à la Faculté des études supérieures et postdoctorales de l'Université Laval dans le cadre du programme de docteur en Sciences de l'administration pour l'obtention du grade de Philosophiae Doctor (Ph.D), 2013, 275 pages.

LAURENT Éloi, *L'économie de la confiance*, Paris, La Découverte, 2019, 128 pages.

LEBRETON Olivier, *Adaptation du modèle de la Construction-Intégration de Kintsch à la compréhension des énoncés et à la résolution des problèmes arithmétiques complexes*, Thèse pour l'obtention du grade de docteur en psychologie cognitive sous la direction de HAMON Jean-François, Université de la Réunion, 2011, 410 pages.

LE BRETON David, *Sociologie du risque*, Paris, Presses Universitaires de France, Que sais-je ?, 2017, 128 pages.

Les associés d'EIM (dir.), *Les dirigeants face au changement*, Paris, Huitième Jour, 2004, 140 pages.

LUHMANN Niklas, *Risk. A Sociological Theory*, New York, Routledge, 2002, 270 pages.

MARZANO Michela, *Je consens, donc je suis …*, Paris, Presses Universitaires de France (PUF), 2006, Hors collection, Philosophie, 274 pages.

MILL John Stuart, *De la liberté*, Paris, Gallimard, 1990, traduit de l'anglais par Laurence Lenglet, 242 pages.

Montesquieu, *De l'Esprit des Lois,* Tome Premier, Paris, Gallimard, 1995, 608 pages.

MORANA Cyril, **OUDIN** Éric, *Petite Philosophie des grandes idées – La liberté*, Paris, Eyrolles, 2010, 186 pages.

MUCCHIELLI Alex, *L'art d'influencer*, Paris, 2009, 176 pages.

NOURI Anass, *Cartes de saillance et évaluation de la qualité des maillages* 3D, Thèse pour l'obtention du grade de docteur en informatique sous la direction de LÉZORAY Olivier et CHARRIER Christophe, Université de Normandie, 2016, 153 pages.

O'NEIL Cathy, *Weapons of Math Destruction*: *How Big Data Increases Inequality and Threatens Democracy*, New York, Crown, 2016, 272 pages.

Ovide, Métamorphoses, VII, 20-2, trad. Lafaye G., Paris, Gallimard, 1992, 640 pages.

PATINO Bruno, *La civilisation du poisson rouge. Petit traité sur le marché de l'attention*, Paris, Grasset et Fasquelle, 2019, 184 pages.

Platon, *Protagoras,* 358 b 3-5, trad. Trédé M. Demont P., Paris, Poche, 1993, 241 pages.

RAZ Joseph, *The Morality of Freedom,* Oxford, Oxford University Press, 1986, 448 pages.

REICH Rob, **SAHAMI** Mehran, **WEINSTEIN** Jeremy M., *System Error. Where Big Tech Went Wrong and How we Can Reboot*, Harper, 2021, 352 pages.

REMACLE Julian, *Et internet recréa Dieu : Notre libre arbitre n'existe plus*, Rinfini, 2014, 188 pages.

SMYRNAIOS Nikos, *Internet Oligopoly. The Corporate Takeover of Our Digital World*, Bingley, Emerald Publishing, 2018, 174 pages.

ZUBOFF Shoshana, *L'âge du capitalisme de surveillance*, Paris, Éditions Zulma, 2020, 864 pages.

II. MANUELS, TRAITÉS ET OUVRAGES GÉNÉRAUX

BOURGEOIS Matthieu, *Droit de la donnée*, Paris, LexisNexis, Coll. Droit & Professionnels, 2017, 544 pages.

BUFFELAN-LANORE Yvaine, **LARRIBAU-TERNEYRE** Virginie, *Droit civil. Les* obligations, Paris, Sirey, 2020, 17e éd., 1268 pages.

CABRILLAC Rémy, *Droit des obligations*, Paris, Dalloz, 2020, 14e éd., 474 pages.

CALAIS-AULOY Jean, **TEMPLE** Henri, **DEPINCÉ** Malo, *Droit de la consommation*, Paris, Dalloz, Précis, 10e édition, 2020, 780 pages.

CASTETS-RENARD Céline, *Droit du marché unique numérique et intelligence artificielle*, Bruxelles, Bruylant, 2020, 388 pages.

CAYROU Nicolas, *Action en justice*, Paris, Dalloz, novembre 2019, 258 pages.

CORNU Gérard, *Vocabulaire juridique*, Paris, Quadrige / PUF, 2016, 11e édition, 1136 pages.

DEBARD Thierry, **GUINCHARD** Serge, *Lexique des termes juridiques 2020-2021*, Dalloz, édition n°28, août 2020, 1150 pages.

DEGRAVE Élise, *L'e-gouvernement et la protection de la vie privée*, 1e édition, Bruxelles, Larcier, 2014, 764 pages.

DE TERWANGNE Cécile, **ROSIER** Karen (dir.), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Paris, Larcier, 2018, 1e ed., 901 pages.

FÉRAL-SCHUHL Christiane, *Cyberdroit. Le droit à l'épreuve de l'Internet*, Paris, Praxis Dalloz, 8e édition, 2020, 1852 pages.

KOSTA Eleni, *Consent in European Data Protection Law*, Liden, Martinus Nijhoff Pulishers, 2013, 461 pages.

LALANDE André, *Vocabulaire technique et critique de la philosophie*, Paris, Quadrige / PUF, 2010, 3e édition, 1376 pages.

NIHOUL Paul, *La concurrence et le droit*, Colombelles, EMS Éditions, 2001, 326 pages.

PELLIER Jean-Denis, *Droit de la consommation*, Paris, Dalloz, 3e édition, 2021, 458 pages.

PICOD Yves, **PICOD** Nathalie, *Droit de la Consommation*, Paris, Sirey, 5e éd., 2020, 620 pages.

PORCHY-SIMON Stéphanie, *Droit des obligations 2022*, Paris, Dalloz, 2021, 14e éd.,700 pages.

SÈVE René, *Philosophie et théorie du droit*, Paris, Dalloz, 2e ed., 2017, 544 pages.

TAMBOU Olivia, *Manuel de droit européen de la protection des données à caractère personnel*, 1e édition, Bruxelles, Bruylant, 2020, 486 pages.

TERRÉ François, **SIMLER** Philippe**, LEQUETTE** Yves, *Les obligations*, 10 éd., Paris, Dalloz, 2009, 1542 pages.

III. MONOGRAPHIES, THÈSES ET OUVRAGES SPÉCIAUX

AFDS (dir.), *Consentement et santé*, Paris, Dalloz, 2014, 386 pages.

Association Henri Capitant, *Vulnérabilité*, Bruxelles, Bruylant, 2020, 1312 pages.

BANCK Aurélie, **SCHULTIS** Catherine, *Vade-mecum de la protection des données personnelles pour le secteur bancaire et financier*, Paris, RB édition, Les essentiels de la banque et de la finance, 2018, 118 pages.

BAROCAS Solon, **HARDT** Moritz, **NARAYANAN** Arvind, *Fairness and Machine Learning. Limitations and Opportunities*, 312 pages, disponible sur https://fairmlbook.org/pdf/fairmlbook.pdf.

BARRAUD Boris, *La prospective juridique*, Paris, L'Harmattan, 2020, 316 pages.

BENNETT Colin J., **RAAB** Charles D., *The governance of privacy: Policy instruments in global perspective*. Routledge, 2019, 272 pages.

BEELEN Axel, *Guide pratique du RGPD*, 1e édition, Bruxelles, Bruylant, 2018, 370 pages.

BRUNEAU Laurent, *Contribution à l'étude des fondements de la protection du contractant,* Thèse pour l'obtention du grade de docteur en droit sous la direction de ROZÈS Louis, 2005, Université des sciences sociales de Toulouse, 532 pages.

CALLET Clovis, *Le sérieux et le manifeste en droit judiciaire privé. Contribution à une étude de la certitude en droit*, Thèse pour obtenir le grade de docteur en droit sous la direction de CHÉROT Jean-Yves et PUTMAN Emmanuel, Université d'Aix-Marseille, 2015, 402 pages (telle que réécrite après la soutenance et mise à jour au 20 février 2021).

CANAL FORGUES ALTER Éric, **HAMROUNI** Maïa-Oumeïma (dir.), *Intelligence artificielle*, Bruxelles, Bruylant, 2021, 208 pages.

CASTETS-RENARD Céline, **NDIOR** Valère, **RASS-MASSON** Lukas. (dir.), *Enjeux internationaux des activités numériques*, 1e édition, Bruxelles, Larcier, 2020, 202 pages.

CHRISTELLE Maxence, *Consentement et subjectivité juridique. Contribution à une théorie émotivo-rationnelle du droit*, Thèse pour obtenir le grade de docteur en droit sous la direction de M Étienne PICARD, Université Paris I Panthéon-Sorbonne, 2014, 959 pages.

CODRON Clémence, *La surveillance diffuse : entre Droit et Norme*, Thèse pour obtenir le grade de docteur en droit public dirigée par LAVENUE Jean-Jacques, Université de Lille, 2018,575 pages.

COLLET Clementine, **DILLON** Sarah, *AI and Gender: Four Proposals for Future Research*, Cambridge, The Leverhume Centre for the Future of Intelligence, 2019, 44 pages.

DABOSVILLE Benjamin, *L'information du salarié. Contribution à l'étude de l'obligation d'informer*, Paris, Dalloz, Nouvelle Bibliothèque de Thèses, volume 123, 2013, 601 pages.

DE STREEL Alexandre, **JACQUEMIN** Hervé (dir.), *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, 482 pages.

DE TERWANGNE Cécile *et al.* (dir.), *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde*, Liber Amicorum Yles Poullet, 1e édition, Bruxelles, Larcier, 2018, 800 pages.

DIEUX Xavier, *Droit, morale et marché*, Bruxelles, Bruylant, 2003, 828 pages.

DOCQUIR Benjamin, **DAVIO**, Victor, **DUMORTIER** Franck (dir.), *Le RGPD dans la pratique : un exercice d'équilibre*, 1e édition, Bruxelles, Larcier, 2021, 106 pages.

FABRE-MAGNANT Muriel, *L'institution de la liberté*, Paris, PUF, 2018, 352 pages.

FADEN Ruth R., **BEAUCHAMP** Tom L., *A History and Theory of Informed Consent*, New York, Oxford University Press, 1986, 408 pages.

GROSJEAN Alain, *Enjeux européens et mondiaux de la protection des données personnelles*, 1e édition, Bruxelles, Larcier, 2015, 465 pages.

LACORDAIRE Henri, *Conférences de Notre-Dame de Paris*, Tome III, années 1848-1849-1850, Paris, Ambroise Bay, 1855, 672 pages.

LAGADEC Alain, *De l'interprétation des clauses contractuelles à la qualification du* contrat, Thèse pour obtenir le grade de docteur en droit sous la direction de GUILLOTIN Alain, Université de Toulon, 2017, 228 pages.

LE GAC-PECH Sophie (dir.), *Les droits du contractant vulnérable*, Bruxelles, Larcier, 2016, 138 pages.

LE GOUES Morgan, *Le consentement du patient en droit de la santé*, Thèse pour obtenir le grade de docteur en droit sous la direction de BERNAUD Valérie, Université d'Avignon et des Pays de Vaucluse, 2015, 664 pages.

MAUME Florian, *Essai critique sur la protection du consentement de la partie faible en matière contractuelle*, Thèse pour l'obtention du grade de docteur en droit sous la direction de HOUTCIEFF Dimitri, Université d'Evry Val d'Essonne, 2015, 616 pages.

MCLEAN Sheila A. M., *Autonomy, Consent and the Law*, Routledge, 2010, 616 pages.

MILLER Arthur, *The Assault on Privacy*, Cambridge, Harvard University Press, 1971, 320 pages.

NDIOR Valère, *La participation d'entités privées aux activités des institutions économiques internationales,* Thèse pour l'obtention du grande de docteur en droit sous la direction de COSNAR Michel, Université Cergy-Pontoise, 2013, 450 pages.

OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Thèse pour le doctorat en droit sous la direction de TEITGEN-COLLY Catherine, Université Paris I – Panthéon-Sorbonne, 2014, 763 pages.

PAYET Marie-Stéphane, *Droit de la concurrence et droit de la consommation*, Dalloz, Nouvelle Bibliothèque de Thèses, 2001, volume 7, 524 pages.

POULLET Yves, *La vie privée à l'heure de la société numérique*, Bruxelles, Larcier, 2019, 190 pages.

PUYDEBOIS Grégori, *La transparence de la vie publique en France*, Thèse présentée pour obtenir le grade de docteur en droit sous la direction de MÉLIN-SOUCRAMANIEN Ferdinand, Université de Bordeaux, 2019, 517 pages.

RODRIGUES Rowena *et al.*, *EU Privacy seals project: Inventory and analysis of privacy certification schemes. Final Report*, Luxembourg, 2013, Publications Office of the European Union, 290 pages.

TINIÈRE Romain, **VIAL** Claire (dir.), *Les dix ans de la Charte des droits fondamentaux de l'Union européenne. Bilan et perspectives*, Bruxelles, Bruylant, 2020, 446 pages.

TUROW Joseph *et al.*, *The Tradeoff Fallacy – How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation*, A Report from the Annenberg School for Communication, University of Pennsylvania, 2015, 26 pages.

VERGNOLLE Suzanne, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, Thèse pour le doctorat en droit sous la direction de PASSA Jérôme, Université Paris II – Panthéon-Assas, 7 décembre 2020, 555 pages.

VERHENNEMAN Griet, *The Patient, Data Protection and Changing Healthcare Models*, 1e edition, Bruxelles, Intersentia, 2021, 405 pages.

VIDAILLET Bénédicte, **D'ESTAINTOT** Véronique, **ABECASSIS** Philippe (dir.), *La décision. Une approche pluridisciplinaire des processus de choix*, Louvain-la-Neuve, De Boeck Supérieur, Collection Méthodes & Recherches, 2015, 304 pages.

VIOLET Franck (dir.), *Personne et Patrimoine en droit. Recherche sur les marqueurs d'une connexion*, Bruxelles, Bruylant, 2015, 508 pages.

IV. ARTICLES, NOTES, ÉTUDES ET CHRONIQUES

ACQUISTI Alessandro *et al.*, « Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online », *ACM Computing Surveys*, Vol. 50, 2017, n°3, pp. 1-44.

AIN AL-SHAMS Abad, « Le nudge. Embarras du choix & paternalisme libertarien », *Multitudes*, 2017/3, n°68, pp. 44-53.

ALBRECHT Jan Philipp, « How the GDPR Will Change the World », *European Data Protection Law Review*, 2016, Volume 2, Issue 3, pp. 287-289.

ALIX Pascal, « Il est plus facile pour un chameau de passer par le chas d'une aiguille que pour les responsables de traitement d'obtenir un consentement libre et éclairé au dépôt et à la lecture de cookies tiers », *Légipresse*, octobre 2020.

ALLARD Baptiste, **JOURDAN-MARQUES** Jérémy, « Action de groupe », *Répertoire de procédure civile*, février 2021.

ALLEN Anita L., « Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm », *Connecticut Law Review*, 2000, Vol. 32, pp. 861-875.

AMBROISE-CASTÉROT Coralie, « Aveu », *Répertoire de droit pénal et de procédure pénale*, avril 2020.

AMBROISE-CASTELOT Coralie, « Les nouvelles pratiques commerciales déloyales après la loi LME du 4 août 2008 », *AJ Pénal*, 2009, n°1, p. 22.

ANCET Pierre, « L'écart entre les lois et les pratiques : le problème du statut des personnes », *in* MASSE Manon *et al.* (dir.), *Accessibilité et participation sociale. Vers une mise en œuvre de la Convention relative ax droits des personnes handicapées*, IES éditions, 2020, pp. 33-55.

ARMINGAUD Claude-Etienne, **BOURNY** Marianne, « Surveiller et punir à l'aune du RGPD : l'harmonisation à l'épreuve de la diversité européenne », *Revue Lamy Droit de l'Immatériel*, n° 163, 1e octobre 2019, pp. 49-53.

ARNESON Richard J., « Nudge and Shove », *Social Theory and Practice*, Vol. 41, N°4, 2016, pp. 668-691.

ASCENSI Lionel, « Médiation et actions collectives », *Revue Lamy droit des affaires*, 2015, n°105, pp. 76-79.

AUBRY Hélène, « L'apport du droit de la consommation » *in* LE GAC-PECH Sophie, *Les droits du contractant vulnérable*, Bruxelles, Larcier, 2016, pp. 33-48.

AUDIT Mathias *et al.*, « Pour une recherche juridique critique, engagée et ouverte », *D.* 2010, p. 1505.

AUDIT Pierre-Emmanuel, « De quelques enseignements de l'analyse comportementale du droit en matière d'information du contractant », *RTD civ.*, 2021, p. 545.

AUTRIC Jean-Baptiste, **CHAPUIS-BREYTON** Simon, « Juridique – Action en justice – Intérêt à agir, intérêts collectifs et valeurs partagées », *Juris associations*, 2015, n°529, pp. 37-41.

AYALA-RIVERA Vanessa, **PASQUALE** Liliana, « The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements », *2018 IEEE 26th International Requirements Engineering Conference (RE)*, Banff, AB, 2018, pp. 136-146.

AYNÈS Augustin, « Les fonctions du temps », *in* Association Henri Capitant, *Le temps et le droit*, Journées nationales, Tome XVIII, Dijon, pp. 77-86.

AZAR-BAUD Maria José, « La directive européenne sur les actions représentatives : un texte mi-figue, mi-raisin », *La Semaine Juridique Entreprise et Affaires*, n°51, 13 décembre 2020, 1542, pp. 32-40.

AZAR-BAUD Maria José, « *Allegro ma non troppo* (à propos de la transposition en France de la directive sur les actions représentatives en protection des intérêts collectifs des consommateurs) », *D.*, 2021, p. 232.

BACHERT-PERETTI Audrey, « La protection constitutionnelle des données personnelles : les limites de l'office du Conseil constitutionnel face à la révolution numérique », *Revue française de droit constitutionnel*, 2019/2, n°118, pp. 261-284.

BACQUÉ Marie-Hélène, **BIEWENER** Carole, « L'empowerment, un nouveau vocabulaire pour les pour parler de participation ? », *Idées économiques et sociales*, 2013/3, n°179, pp. 25-32.

BALDUCCI Alexandre, **LEBEAU MARIANNA** Denise, « Adoption des lignes directrices modificatives de la CNIL relatives aux cookies et traceurs à la suite de la décision du Conseil d'État du 19 juin 2020 : quelles conséquences en pratique ? », *Dalloz IP/IT*, 2021, pp. 41-45.

BARCELOS Renato Hübner, **GRIL** Emmanuelle, « Réseaux sociaux : quel ton adopter ? », *Gestion*, Vol. 44, 2019/4, pp. 84-87.

BARLOW John Perry, « Déclaration d'indépendance du cyberespace », *in* BLONDEAU Olivier (dir.), *Libres enfants du savoir numérique. Une anthologie du « Libre »*, Paris, Éditions de l'Éclat, 2000, pp. 47-54.

BARRAUD Boris, « L'usage du plan en deux parties dans les facultés de droit françaises », *Revue trimestrielle de droit civil*, 2015, pp. 807-825.

BARRY John Christopher, « « Si vous voyez quelque chose, dites quelques chose ». Edward Snowden et l'État de sécurité nationale », *Inflexions*, 2014, n°27, pp. 135-147.

BATIFOULIER Philippe, « Développer le marché de l'assurance pour le « bien » du patient : les dangers d'un paternalisme marchand », *RDSS*, 2019, pp. 819-828.

BEARDSLEY Elizabeth, « Privacy: Autonomy and Selective Disclosure », *in* PENNOCK J. Roland, CHAPMAN, John W. (dir.), *Nomos XIII: Privacy*, New York, Atherton Press, 1971, pp. 56-70

BEAUCHAMP Tom L., « Autonomy and Consent », *in* MILLER Franklin, WERHEIMER Alan (dir.), *The Ethics of Consent: Theory and Practice*, Oxford University Press, 2010, pp. 55-78.

BELKACEM Nacima, « Bases légales (RGPD) des traitements portant sur la conservation des numéros de cartes bancaires dans le secteur de la vente de biens ou la fourniture de services à distance », *Communication Commerce électronique*, n°3, mars 2021, comm. 24.

BELLIVIER Florence, « Guillaume-Xavier BOURIN, *Contribution à l'étude du délit de manipulation mentale préjudiciable* », *RTD civ.*, 2005, pp. 206-207.

BELLIVIER Florence, « Le droit de retrait en bioéthique sur la voie de l'émancipation », *Droits*, 2008/2, n°48, pp. 131-146.

BEN MBAREK Yosra, **KHLIF** Wafa, « La complémentarité entre le contrôle et la confiance : une étude des relations entre les contrôleurs de gestion et les responsables opérationnels », *Communication au colloque « La comptabilité, le contrôle et l'audit entre changement et stabilité » organisé par l'AFC*, mai 2008, disponible sur HAL : https://halshs.archives-ouvertes.fr/halshs-00522370.

BENNET Colin J., « The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats », *in* GUAGNIN Daniel *and al.* (dir), *Managing Privacy through Accountability*, New York, Springer, 2012, pp. 33-48.

BENBOUZIB Bilel, **MENECEUR** Yannick, **ALISA SMUHA** Nathalie, « Quatre nuances de régulation de l'intelligence artificielle », *Réseaux*, 2022, n°232-233, pp. 29-64.

BERGEL Jean-Louis, « La sécurité juridique », *Revue du Notariat*, volume 110, numéro 2, septembre 2008, pp. 271-285.

BERGERON Henri, **CASTEL** Patrick, **DUBUISSON-QUELLIER** Sophie, « Gouverner par les labels. Une comparaison des politiques de l'obésité et de la consommation durable », *Gouvernement et action publique*, 2014, vol. 3, pp. 7-31.

BERNARD Françoise, « Imaginaire, participation, engagement et *empowerment*. Des notions pour penser la relation entre riques et changements », *Communication et organisation*, 2014, n°45, pp. 87-98.

BERNHEIM-DEVAUX Sabine, « Le droit de la consommation, entre protection du consommateur et régulation du marché », *Revue Juridique de l'Ouest*, 2013, pp. 45-54.

BERTINO Elisa et al., « Redefining Data Transparency: A Multidimensional Approach », *Computer*, 2019, Volume 52, Issue 1, pp. 16-26.

BERTRAND Brunessen, **SIRINELLI** Jean, « Schrems II : on prend les mêmes et on recommence », *Dalloz IP/IT*, novembre 2020, n°11, pp. 640-644.

BERTRAND Brunessen, « Chronique Droit européen du numérique – Perfectibilité de la protection des données personnelles », *RTD Eur.* 2021, pp. 143-144.

BERTRAND Christine, « L'accès au droit de l'Union européenne », *La Revue du Centre Michel de l'Hospital*, 2017, n°12, pp. 55-64.

BESIK Saliha, **FREYTAG** Johann-Christoph, « Managing consent in Workflows under GDPR », in MANNER Johannes et al. (dir.), *12th ZEUS Workshop, ZEUS 2020*, Postdam, Germany, Février 2020, pp. 18-25.

BESSE Philippe, **BESSE-PATIN** Aurèle, **CASTETS-RENARD** Céline, « Implications juridiques et éthiques des algorithmes d'intelligence artificielle dans le domaine de la santé », *Statistique et Société*, 2020, vol. 8, n°3, pp. 21-53.

BÉVIÈRE-BOYER Bénédicte, « Faire face au risque de souveraineté numérique incontrôlée », *Dalloz IP/IT*, 2020, pp. 339-343.

BEYER-KATZENBERGER Malte, « What if the next generation of the internet was an 'Internet of Me'? », *Futurium*, Commission européenne, 2 décembre 2016, disponible sur https://ec.europa.eu/futurium/en/blog/what-if-next-generation-internet-was-internet-me.html.

BIARD Alexandre, « Sale temps pour l'action de groupe … La nécessaire recherche d'outils alternatifs pour résoudre les litiges de masse », *Revue Lamy Droit civil*, mars 2018, n°157, pp. 21-26.

BIER Christoph *et al.*, « Privacy Insight: The Next Generation Privacy Dashboard » *in* SCHIFFNER Stefan *et al.* (dir.), *Privacy Technologies and Policy*, 4th Annual Privacy Forum, AFP 2016, Frankfurt/Main, Germany, September 7-8 2016, Proccedings, Springer, pp. 135-152.

BIETTI Elterra, « Consent as a Free Pass: Platform Power and the Limits of the Informational Turn », *Pace Law Review*, 2020, Volume 40, Issue 1, pp. 310-398.

BLUME Peter, « Article 61. Mutual Assistance », *in* KURNER Christopher, BYGRAVE Lee A., DOCKSEY Laura (dir.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press, pp. 973-985.

BOARINI Serge, « Le consentement : pacte et impacts », *in* AFDS (dir.), *Consentement et santé*, Paris, Dalloz, 2014, pp. 45-54.

BÖSCH Christoph *et al.*, « Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns », *Proceedings on Privacy Enhancing Technologies*, 2016, n°4, pp. 237-254.

BOUHON Frédéric, « Le risque et la Cour européenne des droits de l'homme – Premières esquisses d'une réflexion sur le risque à l'aune des droits fondamentaux », *RDLF*, chronique n°46, disponible sur http://www.revuedlf.com/droit-fondamentaux/le-risque-et-la-cour-europeenne-des-droits-de-lhomme-premieres-esquisses-dune-reflexion-sur-le-risque-a-laune-des-droits-fondamentaux/

BOURDEL Christophe, « Première bougie pour l'action de groupe : un bilan en demi-teinte », *AJ contrat,* 2015, p. 488.

BOURREAU Marc, **PERROT** Anne, « Plateformes numériques : réguler avant qu'il ne soit trop tard », *Notes du Conseil d'analyse économique*, 2020/6, n°60, pp. 1-12.

BOY Laurence, « Labels écologiques et alimentaires : les enjeux de la réglementation européenne », *Journal de droit européen*, 2013, n°195, pp. 2-9.

BOYD Danah, **CRAWFORD** Kate, « Critical Questions for Big Data », *Information, Communication & Society*, 15(5), 2012, pp. 662-679.

BRIGHT Laura F., **LOGAN** Ketly, **LIM** Hayoung Sally, « Social Media Fatigue and Privacy: An Exploration of Antecedents to Consumers' Concerns regarding the Security of Their Personal Information on Social Media Platforms », *Journal of Interactive Advertising*, 2022, Vol. 22, Issue 2, pp. 125-140.

BROCHE Christophe, « La protection de la partie faible à l'épreuve des contrats de construction », *in* CLARET Hélène *et al.* (dir.), *Les rapports entre le droit de la protection des consommateurs et les autres branches du droit*, Presses Universitaire Savoie Mont Blanc, 2020, disponible sur hal.

BROSMAN Terenia, **PERRY** Michael, « « Informed » consent in adult patients: can we achieve a gold standard? », *British Journal of Oral and Maxillofacial Surgery,* Volume 47, Issue 3, avril 2009, pp. 186-190.

BROWER Evelien, **BORGESIUS** Frederik Zuiderveen, « Access to Personal Data and the Right to Good Governance during Asylum Procedures after the CJEU's YS. And M. and S. judgement (C-141/12 and C-372-12) », *European Journal of Migration and Law*, 17(2-3), pp 259-272.

BRUGUIÈRE Jean-Michel, « La nature du droit à la portabilité des données personnelles », *in* GLEIZE Bérangère, MAFFRE-BAUGÉ Agnès (dir.), *La propriété intellectuelle renouvelée par le numérique*, Paris, Dalloz, 2020, pp. 145-165.

BRUNET Émilie, « Les mécanismes de coopération des autorités de contrôle au sein de l'Union européenne et le Comité européen de la protection des données », *Revue de droit international d'Assas*, n°2, décembre 2019, pp. 117-128.

BRYSON Joanna J., « The Artificial Intelligence of the Ethics of AI: An Introductory Overview for Law and Regulation » *in* DUBBER Markus D., PASQUALE Frak, DAS Sunit, *The Oxford Handbook of Ethics of AI*, Oxford University Press, 2020, pp. 2-25.

BU-PASHA Shakila, « Cross-border issues under EU data protection law with regards to personal data protection », *Information & Communications Technology Law*, volume 26, issue 3, pp. 213-228.

BYK Christian, « Recherches impliquant la personne humaine : protection du consentement », *JurisClasseur Pénal Code*, Art. 223-8 et 223-9, Fasc. 20.

Cabinet Vigo, « Le règlement européen "e-privacy", bloqué depuis 2017 au Conseil de l'UE, va enfin pouvoir être débattu au Parlement européen », *Dalloz Actualité*, 18 février 2021.

CABRILLAC Séverine, « Pour l'introduction de la class action en droit français », *Petites affiches*, 18 août 2008, n°165, p. 4.

CALMAN Kenneth C. « Communication of Risk: Choice, Consent and Trust », *The Lancet*, 2002, vol. 360, Issue 9327, pp. 166-68.

CALVÈS Anne-Emmanuèle, « "Empowerment" : généalogie d'un concept clé du discours contemporain sur le développement », *Revue Tiers Monde*, 2009/4, n°200, pp. 735-749.

CAMERER Colin *et. al.*, « Regulation for Conservatives: Behavioral Economics and the Case for "Asymetric Paternalism" », *University of Pennsylvania Law Review*, 2003, Vol. 151, pp. 1211-1254.

CANNARSA Michel, « Chapitre 4 – Les consommateurs aussi ont des sentiments ! Quels effets sur leur patrimoine ? », *in* VIOLET Franck, *Personne et Patrimoine*, Bruxelles, Bruylant, 2015, pp. 107-118.

CARBONNIER Jean, « Effectivité et ineffectivité de la règle de droit », *L'année sociologique*, Vol. 9, 1957-1958, pp. 3-17.

CARBONNIER Jean, « L'amour sans la loi : Réflexions de psychologie sociale sur le droit de la filiation, en mare de l'histoire du protestantisme français », *Bulletin de la Société de l'Histoire du Protestantisme Français,* 1979, pp. 47-75.

CARCASSONNE Guy, « Le trouble de la transparence », *Pouvoirs*, 2001/2, n°97, pp. 17-23.

CAROLAN Eoin, **SPINA** Alessandro, « Behavioural Sciences and EU Data Protection Law: Challenges and Opportunities », *in* ALEMANNO Alberto, SIBONY Anne-Lise (dir.), *Nudge and the Law: A European Perspective*, Oxford, Hart Publishing, 2015, pp. 161-178.

CASSILETH, Barrie R. *et al.* « Informed Consent – Why are its Goals Imperfectly Realized ? », *New England Journal of Medecine*, 1980, 302(16), pp. 896-900.

CASTETS-RENARD Céline, « La protection des données personnelles dans les relations internes à l'Union européenne », *Répertoire de droit européen*, octobre 2018.

CATE Fred H., « Protecting Privacy in Health Research: The Limits of Individual Choice », *California Law Review*, Vol. 98, No 6, 2010, pp. 1765-1803.

CATTALANO Garance, « Intérêts collectifs des consommateurs : adoption de la directive (UE) 2020/1828 relative aux actions représentatives », *Droit des contrats*, 2021, n°1, p. 4.

CHABAS François, « L'obligation médicale d'information en danger », JCP 2000. I. 212.

CHALAZONITIS Simon M., « Expériences et approches nationales de mise en œuvre de la Convention sur la protection des données », *in* Conseil de l'Europe, *Protection des données, droits de l'Homme et valeurs démocratiques*, XIIIe Conférence des Commissaires à la protection des données, 2-4 octobre 1991, Strasbourg.

CHAMBERLIN Judi, « A Working Definition of Empowerment », *Psychiatric Rehabilitation Journal*, 1997, volume 20, n°4, pp. 43-46.

CHANDER Anupam, « Is Data Localization a Solution for *Schrems II*? », *Journal of International Economic Law*, 2020, n°23, pp. 1-14.

CHANTEPIE Gaël « Contrats : effets – rayonnement du contrat », *Répertoire de droit civil*, Janvier 2018, mis à jour en Décembre 2020.

CHARDEL Pierre-antoine, **KHACHATOUROUV** Armen, « Identité, différence et droit au secret à l'ère numérique », *Rue Descartes*, 2020/2, n°98, pp. 103-117.

CHAZAL Jean-Pascal, « Vulnérabilité et droit de la consommation », *Colloque sur la vulnérabilité et le droit*, Grenoble, 23 mars 2000, disponible sur hal.

CHOI Hanbyul *et al.*, « The role of privacy fatigue in online privacy behavior », *Computers in Human Behavior*, Volume 81, 2018, pp. 42-51.

CITOT Vincent, « Liberté et volonté. L'illusoire attestation phénoménologique d'une liberté ontologique », *Le Philosophoire*, n°18, 2002/3, pp. 81-126.

CIVANER Murat, **ALPINAR** Zümrüt, **ÖRS** Yaman, « Why Would Opt-Out System for Organ Procurement Be Fairer ? », *Synthesis Philosophica*, 2010, n°2, pp. 367-376.

CLAY Thomas, « Class actions or not class actions ? », *D.*, 2020, p. 1776.

CLIFFORD Damian, **GRAEF** Inge, **VALCKE** Peggy, « Pre-formulated Déclarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections », *German Law Journal*, Cambridge University Press, 2019, n°20, pp. 679-721.

COMBET Mathieu, « La dilution de la Charte des droits fondamentaux de l'Union européenne dans les règles relatives aux libertés de circulation du marché intérieur », *in* TINIÈRE Romain, VIAL Claire (dir.), *Les dix ans de la Charte des droits fondamentaux de l'Union européenne. Bilan et perspectives*, Paris, Bruylant, 2020, pp. 57-84.

CONERADY David, **RAMEL** Aloïs, « RGPD et consentement, un malentendu handicapant pour les acteurs publics », *Le Courrier des maires*, nos 335-336, juin-juillet 2019, p. 37.

COTON Fanny, **RUELLE** Victoria, « The end of third-party cookies: nothing but smoke and mirrors if the RTB winner takes it all? », *in* JACQUEMIN Hervé (dir.), *Time to Reshape the Digital Society*, Bruxelles, Larcier, 2021, pp. 209-233.

COSTE Florent, **COSTEY** Paul, **TANGY** Lucie, « Consentir : domination, consentement et déni », *Tracés. Revue de Sciences humaines*, n°14, 2008, disponible sur https://journals.openedition.org/traces/365#quotation

DANIS-FATÔME Anne, « Arrêt Schrems II : sauvetage de façade des « clauses contractuelles types » mais invalidation du bouclier de protection des données », *Communication Commerce électronique*, n°11, novembre 2020, comm. 83

DAVID Stéphane, **PRADO** Vincent, « Protéger les personnes vulnérables », *Rapport du 116e congère des notaires de France,* 2020, disponible sur https://rapport-congresdesnotaires.fr/2020-rapport-du-116e-congres/2020-co1-p1-t1-st1-c1/#co1-p1-t1-st1-c1-s1

D'AVOUT Louis *et al.*, « Droit international privé de l'Union européenne (2020) », *Journal du droit international (Clunet)*, n°4, octobre 2021, chronique 8, pp. 1409-1502.

DEBAETS Émilie, « À propos des dérives actuelles du consentement en matière de protection des données », *AJDA*, 2021, pp. 346-350.

DEBET Anne, « Le consentement dans le RGPD : rôle et définition », *Communication Commerce électronique*, avril 2018, n°4, dossier 9.

DEBET Anne, « L'ICO, autorité de protection des données anglaise, prononce une sanction de 500 000 livres à l'encontre de Facebook dans l'affaire Cambridge Analytica », *Communication Commerce* électronique, n°12, décembre 2018, comm. 92.

DEBET Anne, « Réseaux sociaux – Facebook condamné à une sanction pécuniaire de 150 000 euros par la CNIL », *Communication Commerce électronique*, juillet 2019, ,°7-8, comm. 67.

DEBIÈS Élise, « Big data de santé et autodétermination informationnelles : quelle articulation possible pour une innovation protectrice des données personnelles ? », *Revue française d'administration publique*, 2018, n°167, pp. 565-574.

DE COOMAN Jérôme, « Éthique et intelligence artificielle : l'exemple européen », *Revue de la Faculté de Droit de l'Université de Liège*, 2020, n°3, pp. 79-123.

DEEKS Ashley, « The Judicial Demand for Explainable Artificial Intelligence », *Columbia Law Review*, novembre 2019, vol. 119, n°7, pp. 1829-1850.

DE HERT Paul, **PAPAKONSTANTINOU** Vagelis, **KAMARA** Ines, « The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection », *Computer Law & Security Review*, 2016, vol. 32, issue 1, pp. 16-30.

DE HERT Paul *et al.*, « The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services », *Computer Law & Security Review*, Vol. 34, Issue 2, avril 2018, pp. 193-203.

DE JUGLART Michel, « L'obligation de renseignements dans les contrats », *RTD civ*. 1945.1 et s.

DE LA TOUANNE Sébastien, « Les magistrats ont-ils confondu le droit et la morale dans certaines affaires politico-financières », *Dalloz Actualité*, Administratif, Pénal, 14 avril 2021.

DELFORGE Antoine, **GÉRARD** Loïck, « Chapitre 2 – Le GDPR, source de solutions ou de blocages ? Une question de point de vue », *in* DE STREEL Alexandre, JACQUEMIN HERVÉ (dir.), *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, pp. 166-169.

DELFORGE Antoine, « Le placement de « cookies » sur un site web : la Cour de justice fait le point, l'APD commence à sanctionner », *RTDI*, 2020/1-2, pp. 101-112.

DELFORGE Antoine *et al.*, « Chronique de jurisprudence 2018-2020. Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information », *Revue de Droit des Technologies de l'Information (RTDI)*, 2021/1-2, n°82, pp. 59-107.

DELTORN Jean-Marc, « La protection des données personnelles face aux algorithmes prédictifs », *RDLF*, 2017, chron. N°12, disponible sur www.revuedlf.com/droit-ue/la-protection-des-donnees-personnelles-face-aux-algorithmes-predictifs/

DENHIÈRE Guy *et al.*, « Psychologie cognitive et compréhension de texte : une démarche théorique et expérimentale », *in* PORHIEL Sylvie, KLINGER MAESTRALI Dominique (dir.), *L'unité texte*, Pleyben : Perspective, 2004, 74-95.

DE TERWANGNE Cécile, **GAYREL** Claire, « Flux transfrontière de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt *Schrems* », *Cahiers droit européen*, 2017/1, pp. 35-81.

DHOLAKIA Utpal M., « A Motivational Process Model of Product Involvement and Consumer Risk Perception », *European Journal of Marketing*, Vol. 35 No. 11/12, pp. 1340-1362.

DIACQUENOD Cindy, **SANTI** France, « La mise en œuvre du langage facile à lire et à comprendre (FALC) : enjeux, défis et perspectives », *Revue suisse de pédagogie spécialisée,* 2018, pp. 29-35.

DIATKINE Daniel, **STEINER** Philippe, « Introduction », », *Cahiers d'économie politique,* 2005/2, n°49

DISSAUX Nicolas, « Contrat : formation – Détermination des conditions », *Répertoire de droit civil*, avril 2017, actualisé en avril 2022

DISTINGUIN Isabelle, « Discipline de marché par la dette subordonnée : Impact de l'opacité bancaire et des politiques de renflouement des banques », *Revue Économique*, vol. 70, no. 2, 2019, pp. 207-228.

DONNEDIEU DE VABRES-TRANIÉ Loraine, « L'entreprise citoyenne : vices et vertus de la compliance », *Gazette du Palais*, 2021, Hors-Série n°2, p. 33.

DORAN Derek, **SCHULZ** Sarah, **BESOLD** Tarek R., « What Does Explainable AI Really Mean? A New Conceptualization of Perspectives », 2 octobre 2017, arXiv:1810.00794v1.

DOSHI-VELEZ Finale, **KORTZ** Mason A., « Accountability of AI Under the Law – The Role of Explanation », *Berkman Klein Center Working Group on Explanation and the Law*, 2017, disponible sur http://nrs.harvard.edu/urn-3:HUL.InstRepos:34372584

DOVE Edward, **CHEN** Jiahong, « What Does it Mean for a Data Subject to Make their Personal Data "Manifestly Public"? An Analysis of GDPR Article 9(2)(e) », *Edinburgh School of Law research Paper,* 2020, vol. 18, pp. 107-124.

DPO Consulting, « Les difficultés d'application du RGPD dans les entreprises – La conservation des données, un casse-tête pour les entreprises ? », *Cahiers de droit de l'entreprise*, 2019, n°1, dossier 6.

DROUARD Étienne, « La Proposition de Règlement ePrivacy se trompe de cible et de moyens », *Légipresse*, 10 juin 2017, pp. 291-293.

DUMORTIER Franck, « L'obligation de sécurité des données personnelles : vers un standard de "diligence digitale" ? », in DAVIO, Victor *et al.* (dir.), *Le RGPD dans la pratique : un exercice d'équilibre*, 1e édition, Bruxelles, Larcier, 2021, pp. 41-89.

DUMOULIN Lisa, « Droits de la personnalité et droit à la vie privée des personnes morales », *Revue des sociétés*, 2016, n°10, pp. 594-597.

DUPIE Agnès, « Rubrique de jurisprudence Risques naturels et technologies », *BDEI,* 2013, n°44, pp. 41-52.

DUPICHOT Philippe, **GRIMALDI** Cyril, **VERNIÈRES** Christophe, « Avant-propos », *in* Association Henri Capitant, *La vulnérabilité*, Bruxelles, Bruylant, 2020.

EDENBERG Elizabeth, **JONES** Meg Leta, « Analyzing the legal roots and moral core of digital consent », *New Media & Society*, 2019, Vol. 21, Issue 8, pp. 1804-1823.

EDO Anthony, **JACQUEMET** Nicolas, « Discrimination à l'embauche selon l'origine et le genre : défiance indifférenciée ou ciblée sur certains groupes ? », *Économie et Statistique*, n°464-465-466, 2013, pp. 155-172.

EDWARDS Lilia, **VEALE** Michael, « Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For », *Duke Law and Technology Review*, 2017, Vol. 16, n°1, pp. 18-84.

EFRONI Zohar *et al.*, « Privacy Icons : A Risk-Based Approach to Visualisation of Data Processing », *European Data Law Review (EDPL)*, 2019, vol. 3, pp. 352-366.

EOM Kyong Shik *et al.*, « Pre-Trade Transparency and Market Quality », *Journal of Financial Markets*, 2007, vol 10, pp. 319-341.

ERMOSHINA Ksenia, **MUSIANI** Francesca, « Hiding from Whom? Threat Models and In-The-Making Encryption Technologies », *Intermediality*, 2018, Issue 32.

ETZIONI Amitai, **ETZIONI** Oren, « Incorporating Ethics into Artificial Intelligence », *The Journal of Ethics*, 2017, Vol. 21, n°4, pp. 4.3-418.

EUDIER Frédérique, « Adoption – Adoption plénière », *Répertoire de droit civil*, octobre 2008

EVANS David S., « The Economics of Attention Markets », 15 avril 2020, disponible sur SSRN : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3044858.

EYNARD Jessica, « RGPD « empouvoirement » individuel : promesse tenue ou espoir déçu ? », *Revue des affaires européennes*, 2021/1, pp. 15-25.

EYRAUD Benoît, **VIDAL-NAQUET** Pierre A., « Consentir sous tutelle. La place du consentement chez les majeurs placés sous mesure de protection », *Tracés. Revue de Sciences humaines*, 2008, n°14, disponible sur http://journals.openedition.org/traces/378

FABRE Marie, « Réflexions sur la sanction des engagements perpétuels après la réforme du 10 février 2016 », *D.*, 2020, pp. 1189-1194.

FABRE-MAGNAN Muriel *et al.*, « Controverse sur l'autonomie personnelle et la liberté du consentement », *Droits*, 2008/2, n°48, pp. 3-58.

FABRE-MAGNAN Muriel, « Le domaine de l'autonomie personnelle. Indisponibilité du corps humain et justice sociale », *D.*, 2008, pp. 31-39.

FALKINGER Josef, « Limited Attention as a Scarce Resource in Information-Rich Economies », *The Economic Journal*, volume 118, issue 532, pp. 1596-1620.

FASQUELLE Daniel, « Le droit de la concurrence face au défi de l'économie numérique », *Cahiers de droit de l'entreprise*, n°3, mai 2019, dossier 15.

FAUVET Jacques, « La protection des données personnelles », *Revue internationale de droit comparé,* 1987, n°3, pp. 551-556.

FECI Nadia, « Hands up : cookies or cash ? », 11 juin 2019, *Ku Leuven CiTip*, Ku Leuven center for IT & IP law, disponible sur https://www.law.kuleuven.be/citip/blog/hands-up-cookies-or-cash/

FENNETEAU Hervé, **NARO** Gérald, « Contrôle et confiance dans l'entreprise virtuelle. Illustrations logiques », *Revue française de gestion*, 2005, n°156, pp. 203-219.

FENOUILLET Dominique, « Avant-propos », *in* FENOUILLET Dominique, *L'argument sociologique en droit. Pluriel et singularité*, Dalloz, 2015, pp. 1-14.

FÉRAL-SCHUHL Christiane, « Chapitre 714 – Atteintes à l'ordre public », *in* FÉRAL-SCHUHL Christiane (dir.), *Cyberdroit : le droit à l'épreuve de l'Internet*, Dalloz, Collection Praxis, 2020-2021, pp. 1590-1620.

FERRAND-BECHMANN Dan, « Une clé pour davantage de démocratie et de participation : l'empowerment ou le pouvoir d'agir », *Juris Associations*, 2008, n°383, pp. 22-25.

FERREIRA Anthony, « Addiction et faiblesse de la volonté », 2019, Institut de Recherches Philosophiques, Université Paris Nanterre, disponible sur https://chaire-philo.fr/wp-content/uploads/2019/11/Addiction-et-faiblesse-de-la-volont%C3%A9.pdf

FERRER Morte *et al.*, « Personal Autonomy in Elderly and Disabled: How assistive technologies impact on it », *in* HALTAUFDERHEIDE Joschka *et al.* (dir.), *Aging Between Participation and Simulation: Ethical Dimensions of Social Assistive Technologies in Elderly Care*, Walter de Guyter GmbH & Co KG, 2020.

FÉVRIER Jean-Marc, « Vaccination obligatoire, consentement et expérimentation », *AJDA*, n°29, 2021, p. 1677.

FISCHER Bogdan, **MAZWSKI** Milosk, « Analysis of processing electronic communication data on the basis on consent in the light of Council's e-privacy regulation proposal », *Journalism Research Review Quarterly*, 2017, n°4

FLESCH Rudolf, « How to Write Plain English. Chapter 2: Let's Start With the Formula », disponible sur https://web.archive.org/web/20160712094308/http://www.mang.canterbury.ac.nz/writing_guide/writing/flesch.shtml

FOURQUET-COURBET Marie-Pierre, « Influence attendue et influence effective de la publicité sur l'internet. Des représentations sociales des producteurs aux modèles scientifiques », *Question de communication*, 2005, n°5, pp. 31-53.

FRIED Charles, « Privacy: A Rational Context », *in* ERMANN David *et al.* (dir.), *Computers, Ethics and Society,* New York, Oxford University Press, 1990, pp. 50-63

FRISON-ROCHE Marie-Anne, « L'aventure de la *compliance* », *D.*, 2020, p. 1805.

FRISON-ROCHE Marie-Anne, « Le droit de la régulation », *D.*, 2001, pp. 610-616.

FRISON-ROCHE Marie-Anne, « Remarques sur la distinction de la volonté et du consentement en droit des contrats », *Revue trimestrielle de droit civil*, 1995, pp. 573-574.

FROOMKIN A. Michael, « The Death of Privacy ? », *Stanford Law Review,* n°52, 2000, pp. 1461-1548.

FUKUYAMA Francis *et al.*, « How to Save Democracy From Technology. Ending Big Tech's Information Monopoly », *Foreign Affairs*, janvier-février 2021, disponible sur https://www.foreignaffairs.com/articles/united-states/2020-11-24/fukuyama-how-save-democracy-technology

GALUSTIAN Gohar, « La protection des données personnelles à l'épreuve du numérique », *Revue du droit public*, n°5, p. 1389.

GAURIGAN Jean-Louis, « La transparence pour susciter la confiance », *Juris Associations*, 2019, n°60, pp. 29-30.

GAVANON Isabelle, **LE MAREC** Valentin, « Application de contact tracing : « un choix individuel gage de responsabilité collective » encadré par le CEPD », *Dalloz actualité*, 21 avril 2020.

GERBER Nina, **GERBER** Paul, **VOLKAMER** Melanie, « Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior », *Computer & Security*, 2018, Volume 77, pp. 226-261.

GÉROT Mathilde, « Le renforcement des droits des personnes sur leurs données à caractère personnel – Aspects de droit interne », *Revue de droit international d'Assas,* 2019, n°2.

GHOSH Dipayan, « What You Need to Know About California's New Data Privacy Law », *Harvard Business Review,* 11 juillet 2018

GIANNOPOULOU Alexandra, « Algorithmic systems: the consent is in the detail? », *Internet Policy Review*, mars 2020, Volume 9, Issue 1.

GIL GONZÁLEZ Elena, **DE HERT** Paul, « Understanding the legal provisions that allow processing and profiling of personal data – an analysis of GDPR provisions and principles », *ERA Forum*, Springer, 2019, pp. 597-621.

GILLET Jean-Louis, « Réflexions sur le rapport de la Cour de cassation relatif aux « personnes vulnérables » (2010) », *Les Cahiers de la Justice*, 2019, n°4, pp. 649-653.

GILLET Jean-Louis, « À la recherche du consentement perdu », *Les Cahiers de la Justice*, 2021, n°4, pp. 659-664.

GIRER Marion, « À la recherche du juste consentement en matière de soins », *Les Cahiers de la Justice*, 2021, n°4, pp. 635-646.

GLEIZE Bérengère, « Vie privée des personnes morales : le rejet de l'anthropomorphisme », *Légipresse*, 2018, pp. 79-84.

GODEFROY Lêmy, « Éthique et droit de l'intelligence artificielle », *D.*, 2020, pp. 231-236.

GODEFROY Lêmy D., « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », *D.* 2016, pp. 438-444.

GONZÁLEZ FUSTER Gloria, **GUTWIRTH** Serge, « Opening up personal data protection : A conceptual controversy », *Computer Law & Security Review*, Volume 29, Issue 5, octobre 2013, pp. 531-539.

GONZÁLEZ CABAÑAS José, **CUEVAS** Ángel, **CUEVAS** Rubén, « Facebook Use of Sensitive Data for Advertising in Europe », *27th USENIX Security Symposium*, 2018, pp. 479-495.

GOODIN Robert E., « Permissible Paternalism: In Defense of the Nanny State », *Responsive Community*, 1991, n°42, pp. 42-51.

GOYARD-FABRE Simone, « La signification du contrat dans la « Doctrine du Droit » de Kant, *Revue de Métaphysique et de Morale*, 1973, n°2, pp. 189-217.

GRANADOS Nelson, **GUPTA** Alok, « Transparency Strategy: Competing with Information in a Digital World », *MIS Quarterly*, Juin 2013, vol. 37, pp. 637-641.

GRAY Colin M., « The Dark (Patterns) Side of UX Design », *CHI'18 : Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, avril 2018, n°534, pp. 1-14.

GRIGGIO Carla F., « Caught in the Network : The Impact of WhatsApp's 2021 Privacy Policy Update on Users' Messaging App Ecosystems », *CHI'22*, New Orleans, 29 avril-5 mai 2022, pp. 1-23.

GROFFE-CHARRIER Julie, « La loi est-elle dictée par le code ? », *Dalloz IP/IT*, 2020, pp 602-606.

G'SELL Florence, « Remarques sur les aspects juridiques de la « souveraineté numérique » », *Revues des Juristes de Sciences Po*, n°19, octobre 2020, pp. 1-19.

GUILLARME Bertrand, « Usages de la Responsabilité », *Revue française de science politique*, 2008/6, vol. 58, pp. 873-875.

GUILLOUD Olivier, « Le consentement dans tous ses états », *in* Association française de droit de la santé (dir.), *Consentement et santé*, Paris, Dalloz, 2014, pp. 1-18.

GUIOMARD Frédéric, « L'obscure clarté de la succession des actions collectives et individuelles en justice », *Revue de droit du travail*, 2021, n°10, pp. 597-601.

HAAS Gérard, **ASTIER** Stéphane, **BENELLI** Paul., « L'impact de la réforme du droit des obligations sur les contrats « digitaux » », *Revues des Juristes de Sciences Po*, n°13, mars 2017, pp. 53-62.

HAAS Gérard, **ASTIER** Stéphane, « Les biais de l'intelligence artificielle : quels enjeux juridiques ? », *Répertoire IP/IT et Communication*, juillet 2019.

HACKER Philipp *et al.*, « Explainable AI under contract and tort law: legal incentives and technical challenges », *Artificial Intelligence and Law*, 2020, pp. 415-439.

HADOT Pierre, **LAUGIER** Sandra, **DAVIDSON** Arnold, « Qu'est-ce que l'éthique ? », *Cités*, 2001/1, n°5, pp. 129-138.

HAMILTON Vivian E., « Immature Citizens and the State », *BYU Law Rev.*, 2010, pp. 1055-1147.

HAMON Ronan *et al.*, « Impossible Explanations? Beyond Explainable AI in the GDPR from a COVID-19 use case scenario », *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT'21)*, Nex York, Association for Computing Machinery, pp. 549-559.

HANSEN Marit, « User-Controlled Identity Management: the Key to the Future of Privacy? », *International Journal of Intellectual Property Management*, 2(4), 2008, pp. 325-344.

HARRIS Tristan, « How Technology is Hijacking Your Mind – from a Magician and Google Design Ethicist », *Medium*, disponible sur https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3.

HERRERA Carlos-Miguel, « Georges Ripert en politique », *Droits*, 2017/1, n°65, pp. 181-199.

HIJMANS Hielke, « Article 56. Competence of the lead supervisory authority », *in* KURNER Christopher, BYGRAVE Lee A., DOCKSEY Laura (dir.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press, 2020, pp. 913-926.

HILT Patrice, « L'action de groupe consacrée par la loi n°2014-344 du 17 mars 2014 relative à la consommation : peut-on s'en satisfaire ? », *Gazette du Palais*, avril 2014, n°114.

HIND Michael, « Explaining Explainable AI », *XRDS: Crossroads*, ACM, 2019, Volume 25, n°3, pp. 16-19.

HOFFMANN Chritian Pieter *et al.*, « Privacy Cynism : A New Approach to the Privacy Paradox », *Cyberpsychology : Journal of Psychosocial Research on CyberSpace*, 2016, Vol. 10, n°4, article 7.

HOIBIAN Sandra, « Demande de transparence ou de sincérité ? », *Constructif*, 2018/3, n°51

HOLLAND Christopher P., « The Importance of Trust and Business Relationships in the Formation of Virtual Organisations », *in* SIEBER Pascal, GRIESE Joachim (dir.), *Organizational Virtalness*, Simowa Verlag Bern, Proceedings of the VoNEt – Workshop April 27-28 1998, pp. 55-64.

HOLZEM Julie, « Les limites du consentement éclairé », *AJDA*, 2016, pp. 364-367.

HOLZINGER Andreas *et al.*, « Current Advances, Trends and Challenges of Machine Learning and Knowledge Extraction: From Machine Learning to Explainable AI », *in* HOLZINGER Andreas *and al.* (dir.), *Machine Learning and Knowledge Extraction*. *Lecture Notes in Computer Science*, Springer, 2018, pp. 1-8.

HUBERMAN Bernado A. « Valuating Privacy », *IEEE Security & Privacy*, 2005, pp. 22-25.

HUET Jérôme, « Adieu bon père de famille », *D.*, 2014, chronique 505.

HUM Pierre *et al.*, « Le refus de soin : forces et faiblesses du consentement », *Éthique et Santé*, Volume 12, Issue 1, mars 2015, pp. 56-63.

INGELFINGER Franz J., « Informed (but uneducated) consent », *in* HUMER James M., *Biomedical Ethics and the Law*, Springer US, 1979, XIV, pp. 265-267.

JACQUEMIN Zoé, « Les sanctions civiles comme outils de régulation de l'activité numérique », *in* CASTETS-RENARD Céline *et al.* (dir.), *Enjeux internationaux des activités numériques*, 1e édition, Bruxelles, Larcier, 2020, pp. 179-193.

JAUNET Alexandre, **MATONTI** Frédérique, « L'enjeu du consentement », *Raisons politiques*, 2012, n°46, pp. 5-11.

JEACLE Ingrid, **CARTER** Chris, « In TripAdvisor we trust: Rankings, calculative regimes and abstract systems », *Accounting, Organizations and Society*, Volume 36, Issues 4-5, mai-juin 2011, pp. 293-309.

JENSEN Carlos, **POTTS** Colin, « Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices », *in* DYKSTRA-ERICKSON Elizabeth, TSCHELIGI Manfred (dir.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 471-478.

JOLY Laurène, « Handicap – L'obligation de fournir un aménagement raisonnable », *Répertoire de droit du travail*, Juillet 2019, mis à jour en Octobre 2020.

JONES Meg Leta, **EDENBERG** Elizabeth, « Troubleshooting AI and Consent » *in* DUBBER Markus D., PASQUALE Frank, DAS Sunit, *The Oxford Handbook of Ethics of AI*, Oxford University Press, 2020, pp. 358-374.

JOURDAIN Édouard, « Intérêt général, intérêt individuel et raison collective : perspectives à partir de l'œuvre de Proudhon », *Astérion. Philosophie, Histoire des idées, Pensée politique,* 2017, n°17, disponible sur https://journals.openedition.org/asterion/3050.

KAHNEMAN Daniel, **TVERSKY** Amos, « Subjective Probability: A Judgement of Representativeness », *Cognitive Psychology*, Juillet 1972, Vol. 3, Issue 3, pp. 430-454.

KAMARA Irene, **DE HERT** Paul, « Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach, *Brussels Privacy Hub*, Vol. 4, n°12, août 2018, Working paper disponible sur ssrn : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228369

KARUNAGARAN Surya et al., « Privacy Protection Dashboard: A Study of Individual Cloud-Storage Users Information Privacy Protection Responses », *ACM SIGMIS Conference on Computer and People Research – SIGMIS-CPR'17*, Proceedings, 2017, pp. 181-182.

KEITH Mark J. *et al.*, « Privacy Fatigue: The Effect of Privacy Control Complexity on Consumer Electronic Information Disclosure », *International Conference on Information Systems (ICIS 2014),* Auckland, Nouvelle-Zélande, 14-17 décembre 2014, disponible sur ssrn

KESSOUS Emmanuel *et al.*, « L'économie de l'attention : entre protection des ressources cognitives et extraction de la valeur », *Sociologie du travail*, 2010, vol. 52, n°3

KILOVATY Ido, « Legally Cognizable Manipulation », *Berkeley Technology Law Journal*, 2019, vol. 34, pp. 449-502.

KINSH Patrick, « La banalisation de l'action en cessation dans l'intérêt collectif des consommateurs », *in* D'AVOUT Louis *et al.*, « Droit international privé de l'Union européenne (2020) », *Journal du droit international (Clunet)*, n°4, octobre 2021, chronique 8.

KINTSCH Walter, **KEENAN** Janice, « Reading rate and retention as function of the number of propositions in the base structure of sentences », *Cognitive Psychology*, 1973, Vol. 5(3), pp. 257-274

KINTSCH Walter, « The Role of Knowledge in Discourse Comprehension: A Construction-Intergration Model », *Psychological Review*, 1988, vol. 95, n°2, pp. 163-182.

KLIEGR Tomáš, BAHNÍK Štěpán, FÜRNKRANZ Johannes, , « A Review of Possible Effects of Cognitive Biases on Interpretation of Rule-Based Machine Learning Models », *Artificial Intelligence*, Juin 2021, Vol. 295.

KLEINING John, « The Nature of Consent », *in* MILLER Franklin, WERHEIMER Alan (dir.), *The Ethics of Consent: Theory and Practice*, Oxford, Oxford University Press, 2010, pp. 3-24.

KOBINA GABA Harold, « La protection collective des consommateurs en droit européen : nécessité d'une action de groupe ou de recours collectifs et raisons politico-économiques et juridiques », *Revue de la Recherche Juridique,* Presses Universitaires d'Aix-Marseille, 2015, pp. 1473-1490.

KÖRBER Torsten, « Lessons from the Hare and the Tortoise: Legally Imposed Selfregulation, Proportionality and the Right to Defence Under the DMA », *NZKart*, 2021, pp. 379-384.

KROLL Joshua A. *et al.* « Accountable Algorithms », *University of Pennsylvania Law Review*, 2018, Vol. 165, pp. 663-705.

KUBARA Michael, « Acrasia, Human Agency and Normative Psychology », *Canadian Journal of Philosophy*, octobre 1975, vol. 5, No. 2, pp. 215-232.

KUMAR Priya, « Corporate Privacy Policy Changes during PRISM and the Rise of Surveillance Capitalism », *Media and Communication*, 2017, Volume 5, Issue 1, pp. 63-65.

LACHAUD Eric, « Why the certification process defined in the General Data Protection Regulation cannot be successful », *Computer Law & Security Review*, Volume 32, Issue 6, décembre 2016, pp. 814-826.

LACHAUD Eric, « Accountability and Certification in the GDPR », *SSRN.com*, 22 octobre 2021, disponible sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3948093

LAFOND Pierre-Claude, « L'action de groupe française ou l'art de rater une belle occasion », *Revue internationale de droit comparé*, 2016, n°68, pp. 319-340.

LAGUEUX Maurice, « L'agent économique : rationalité maximale ou minimale », *Cahiers d'économie politique,* 2005/2, n°49, pp. 143-158.

LAISNEY Louis-Jérôme, « Pour en finir avec le « raisonnable » ! », *AJ contrat*, 2017, p. 6.

LARONZE Fleur, « La conciliation des intérêts par le juge judiciaire français », *Revue de droit canonique*, 2013, n°63, pp. 253-268.

LATINA Mathias, « Contrats : généralités Civ. », *Répertoire de droit civil*, Paris, Dalloz, Mai 2017, mis à jour en Novembre 2021.

LAURIN Yves, « L'enjeu européen d'un bicentenaire », *D.*, 2004, pp. 883-885.

LAZARO Christophe, **LE METAYER** Daniel, « Le consentement au traitement des données personnelles. Perspective comparative sur l'autonomie du sujet », *RJTUM*, 48-3, 2014, pp. 765-815.

LE CANNU Paul, « Le combat du voile et de la transparence », *Bulletin Joly Sociétés*, n°11,

LE GOFF Jacques, « Sortir du « cercle vicieux de la défiance » », *Esprit*, décembre 2007, disponible sur esprit.presse.fr.

LEMPEREUR Alain, « Le droit est Janus. Dualité rhétorique entre coexistence et conflit », *in* FRYDMAN Benoît, MEYER Michel (dir.), *Chaïm Perelman. De la nouvelle réthorique à la logique juridique*, Paris, Presses Universitaires de France, 2012, pp. 99-129.

LENAERTS Koen, « Le juge de l'Union européenne dans une Europe de la compliance » *in* FRISON ROCHE Marie-Anne, *Pour une Europe de la compliance*, Paris, Dalloz, 2019, pp. 1-12.

LEON Pedro Giovanni *et al.*, « Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens », *WPES '10: Proceedings of the 9th annual ACM workshop on Privacy in the electronic society,* Octobre 2010, pp. 93-104.

LÉONARD Thierry, « Yves, si tu exploitais tes données ? », *in* DE TERWANGNE Cécile *et al.* (dir.), *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde*, 1e édition, Bruxelles, Larcier, 2018, pp. 659-683.

LE GAC-PECH Sophie, « De la personne vulnérable au contractant vulnérable », *in* LE GAC-PECH Sophie, *Les droits du contractant vulnérable*, Bruxelles, Larcier, 2016, pp. 11-32.

LEPAGE Agathe, « Droits de la personnalité – Personnes titulaires de droits de la personnalité », *Répertoire de droit civil*, septembre 2009.

LE TOURNEAU Philippe, « Formation de la vente », *in* LE TOURNEAU Philippe (dir.), *Droit de la Responsabilité et des contrats 2021/2022*, Dalloz Action, 12e édition, 2020, p. 2016.

LEVALLOIS-BARTH Claire, **CHAUVET** Delphine, « Panorama national et international des labels relatifs aux données personnelles », *in* LEVALLOIS-BARTH Claire (dir.), *Signes de confiance. L'impact des labels sur la gestion des données personnelles*, Paris, Institut Mines-Télécom, pp. 64-90.

LEVALLOIS-BARTH Claire, « Les labels visant à susciter la crédibilité : des pratiques existantes vers l'amélioration de la qualité », *in* LEVALLOIS-BARTH Claire (dir.), *Signes de confiance – l'impact des labels sur la gestion des données personnelles*, Institut Mines-Télécom, Chaire Valeurs et Politiques des Informations Personnelles, janvier 2018, pp. 115-132.

LEVALLOIS-BARTH Claire, « Les mécanismes de labellisations issus du Règlement général sur la protection des données (RGPD) », *in* LEVALLOIS-BARTH Claire (dir.), *Signes de confiance. L'impact des labels sur la gestion des données personnelles*, Paris, Institut Mines-Télécom, 2018, pp. 135-152.

LEVALLOIS-BARTH Claire, « La confiance saisie par le droit » *in* LEVALLOIS-BARTH Claire (dir.), *Signes de confiance. L'impact des labels sur la gestion des données personnelles*, Paris, Institut Mines-Télécom, 2018, pp. 21-36.

Lextenso, « Class action française : les avocats au bord du chemin », *Gazette du Palais*, 7 mai 2013, n°127.

L'HAIDON Olivier, **PARASCHIV** Corina, « Choix individuel et décision fondée sur l'expérience », *Revue économique*, 2009/4, vol. 60, pp. 949-978.

LIBCHABER Rémy, « Réflexions sur les engagements perpétuels et la durée des sociétés », *Rev. Sociétés*, 1995, n°3, pp. 437-458.

LICARI François-Xavier, « Contrat. – Durée du Contrat, *JurisClasseur Civil Code*, 28 février 2017.

LIENHARD Claude, « Le droit du risque », *in* AGUILA Yann (dir.), *Quelles perspectives pour la recherche juridique ?*, Paris, Presses Universitaires de France, Droit et Justice, 2007, pp. 263-264.

LIVENAIS Thomas, « Le règlement général sur la protection des données, outil d'émancipation des consommateurs face aux objets connectés », *Revue de l'Union européenne*, 2020, n°634, pp. 48-52.

LIVINGSTONE Sonia, « Children: a special case for privacy? », *Intermedia*, 2018, 46(2) , pp. 18-23.

LOAYZA Daniel, « Dionysos au ventre. Notre sur le châtiment du vin dans Le Cyclope d'Euripide », *Odysseum – Ministère de l'éducation national et de la jeunesse,* 25 octobre 2019, disponible sur https://eduscol.education.fr/odysseum/dionysos-au-ventre

LUTZ Christoph, **HOFFMANN** Christian Pieter, **RANZINI** Giulia, « Data Capitalism and the User: an Exploration of Privacy Cynicism in Germany », *New Media & Society*, Vol. 22, Issue 7, pp. 1168-1187.

LYON David, « Surveillance Capitalism, Surveillance Culture and Data Politics », *in* BIGO Didier *and al.* (dir.), *Data Politics. Worlds, Subjects, Rights*, Londres, Routledge, 2019, pp. 64-77.

MACENAITE Milda, **KOSTA** Eleni, « Consent for processing children's personal data in the EU: following in US footsteps? », *Information & Communications Technology Law*, Volume 26, 2017, Issue 2, pp. 146-197.

MACKAAY Ejan, « Droit et économie – autonomie et fertilisation », *in* SCHWEITZER Serge, FLOURY Loïc (dir.), *Droit et économie. Des divergences aux convergences*, Dalloz, 2019, pp. 11-24.

MACLURE Jocelyn, **SAINT-PIERRE** Marie-Noëlle, « Le nouvel âge de l'intelligence artificielle : une synthèse des enjeux éthiques », *Les Cahiers de propriété intellectuelle,* Vol. 30, n°3, pp. 741-766.

MADER Reine-Claude, « Action de groupe à la française : premiers retours d'une association de consommateurs », *Gazette du Palais*, 27 octobre *2015, n°*300, p. 14.

MADGE Robert, « Five Loopholes in the GDPR », *Medium.com*, 27 août 2017, disponible sur https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b

MAINGUY Daniel, **DEPINCÉ** Malo, « L'action de groupe, nouvelle procédure du droit français de la consommation », *Droit et Patrimoine,* mai 2014, n°236, pp.

MALAURIE-VIGNAL Marie *et al.*, « Comment appréhender les abus et l'utilisation des données dans la relation d'une plateforme avec ses partenaires contractuels », *Contrats Concurrence Consommation*, n°12, décembre 2020, dossier 16.

MALER Eve, « Extending the Power of Consent with User-Managed Access: A Standard Architecture for Asynchronous, Centralizable, Internet-Scalable Consent », *2015 IEEE Security and Privacy Workshops*, San Jose, CA, 2015, pp. 175-179.

MALLET Éric, « Consentement à procréation », JCl. Notarial Formulaire, Fasc. 10, 01/03/2010 (dernière mise à jour : 08/10/2019).

MANGIAVILLANO Alexandre, « La clause Molière, une tartufferie ? », *D.*, 2017, p. 968.

MANSOURI Mohamed, « L'intelligence artificielle et la publicité : quelle éthique ? », *Enjeux numériques*, n°1, mars 2018, pp. 53-58.

MANTELERO Alessandro, « The future of consumer data protection in the E.U. Re-thinking the « notice and consent » paradigm in the new area of predictive analytics », *Computer Law & Security Review*, 2014, n°30, pp. 649-653.

MANTERELO Alessandro, « Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection », *Computer Law & Security Review*, Vol. 32, Issue 2, avril 2016, pp. 238-255.

MARES Radu, « Corporate transparency laws : A hollow victory ? », *Netherlands Quartely of Human Rights*, 2018, Volume 36, Issue 3, pp. 189-213.

MARIN Jean-Claude, « La compliance, un progrès », *in* BORGA Nicolas, MARIN Jean-Claude, RODA Jean-Christophe (dir.), *Compliance : Entreprise, Régulateur et Juge,* Paris, Dalloz, 2018, pp. 15-20.

MARTIAL-BRAZ Nathalie, « L'objectivation des méthodes d'interprétation : la référence à la « personne raisonnable » et l'interprétation *in favorem* », *Revue des contrats*, 2015, n°1, p. 193.

MARTY Frédéric, « La protection des algorithmes par le secret des affaires. Entre risques de faux négatifs et risques de faux positifs », *Revue internationale de droit économique*, 2019, n°2, pp. 211-237.

MARZANO Michela, « Qu'est-ce que la confiance ? », *Études*, 2010/1, Tome 412, pp. 53-63.

MATHEY Nicolas, « Les finalités du droit de la concurrence. Essai de téléologie du droit », *Contrats Concurrence Consommation*, n°12, décembre 2020, dossier 13.

MAHIEU René, « The Right of Access of Personal Data : a Genealogy », *Technology and Regulation*, 20 août 2021, Vol 2021, pp. 62-75.

MATHUR Arunesh *et al.*, « Dark Patterns at Scale: Findings from a Crawl of 11K Schopping Websites », *Proc. ACM Human-Comunter Interactions 3*, CSCW, article 81, novembre 2019, arXiv:1907.07032.

MATHUR Arunesh *et al.*, « What Makes a Dark Pattern… Dark? Design Attributes, Normative Considerations, and Measurements Methods », *CHI Conference on Human Factors in Computing Systems (CHI'21)*, 8-13 mai 2021, Yokohama, Japon, New York, ACM, pp. 1-27.

MATTATIA Fabrice, « Pour en finir avec le mythe du consentement RGPD », *La Semaine Juridique Administrations et Collectivités territoriales*, n°16, 20 avril 2020, 2121.

MAYNARD Ashley, **GREENFIELD** Patricia, « Le rôle des outils et des artefacts culturels dans le développement cognitif », *Enfance*, 2006/2, vol. 58, pp. 135-145.

MCDONALD Aleecia, **FAITH CRANOR** Lorrie, « The Cost of Reading Privacy Policies », *I/S: A Journal of Law and Policy for the Information Society*, 2008

MCGRUER Jonathan, « Emerging Privacy Legislation in the International Landscape: Strategy and Analysis for Compliance », *Washington Journal of Law, Technology & Arts*, Hiver 2020, Vol. 15, Issue 2, pp. 120-159.

MCKENNA Eoghan, **RICHARDSON** Ian, **THOMSON** Murray, « Smart meter data: Balancing consumer privacy concerns with legitimate applications », *Energy Policy*, Volume 41, février 2012, pp. 807-814.

MCKNIGHT D. Harrison, **KACMAR** Charles J., **CHOUDHURY** Vivek, « Shifting Factors and the Ineffectiveness of Third-Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business », *Electronic Markets*, Vol. 14, n°3, 2010, pp. 252-266.

MÉMETEAU Gérard, « La protection de principe par l'État des personnes les plus faibles et les plus vulnérables : libres propos », Éthique publique, vol. 3, n° 1, 2001, mis en ligne le 13 septembre 2016, disponible sur : http://journals.openedition.org/ethiquepublique/2614

MÉTAIS Philippe, **VALETTE** Élodie, « La directive actions représentatives : un nouvel élan pour les actions de groupe ? », *Dalloz actualité*, 16 décembre 2020.

METALLINOS Nathalie, « Accoutability – Le principe d'accountability : des formalités préalables aux études d'impact sur la vie privée (EIVP) », *Communication Commerce électronique*, n°4, avril 2018, dossier 11.

METALLINOS Nathalie, « Projet de recommandation de la CNIL sur les modalités pratiques de recueil du consentement au placement de cookies », *Communication Commerce électronique*, n°3, mars 2020, comm. 28.

METALLINOS Nathalie, « Transferts de données – Perspectives de sauvetage des « clauses contractuelles types », mais à quel prix ? », *Communication Commerce électronique*, n°4, avril 2020, comm. 35

MICHAEL Nathan, « Trustworthy AI: Why Does It Matter? », *National Defense*, octobre 2019, vol. 104, n°791, disponible sur https://www.nationaldefensemagazine.org/articles/2019/11/19/trustworthy-ai-why-does-it-matter.

MILLER Elizabeth *et al.*, « I Don't Know Why You Need My Data: A Case Study of Popular Social Media Privacy Policies », *CODASPY '22: Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy*, avril 2022, pp. 340-342.

MILLER Tim, «Explanation in Artificial Intelligence: Insights from the Social Sciences», *Artificial Intelligence*, Vol. 267, Février 2019, pp. 1-38.

MILNE George R., **CULNAN** Mary J., « Strategies for Reducing Online Privacy Risks: Why Consumer Read (or Don't Read) Online Privacy Notices », *Journal of Interactive Marketing*¸2004, 18(3), pp. 15-29.

MORAIS CARVALHO Jorge, **ARGA E LIMA** Francisco, **FARINHA** Martim, « Introduction to the Digital Services Act, Content Moderation and Consumer Protection », *Revista de Direito e Tecnologia*, Vol. 3, 2021, n°1, pp. 71-104.

MORANGE Jean, « Liberté », in ALLAND Denis, RIALS Stéphane (dir.), *Dictionnaire de la culture juridique*, Paris, Quadridge/Lamy-Puf, 2003, p. 945.

MOULTON Ben *et al.*, « From informed consent to informed request: do we need a new gold standard ? », *Journal of the Royal Society of Medicine*, 2013, Volume 106, Issue 10, pp. 391-394.

MOULY Jean, « Vie privée des salariés handicapés et information du comité d'entreprise : contresens sur l'article 8 de la Convention européenne des droits de l'homme », *D.*, 2005, pp. 469-471.

MUCHIELLI Julien, « Achat de votes à Corbeil : « On n'a jamais vu en France une ville livrée à un tel degré de corruption » », *Dalloz actualité*, 3 novembre 2020.

MYTHEN Gabe, « Sociology and the Art of Risk », *Sociology Compass*, 2008, pp. 299-316.

NERA Kenzo, « Biais de raisonnement et dangers des algorithmes », *TheConversation.com*, 19 août 2019, disponible sur https://theconversation.com/biais-de-raisonnement-et-dangers-des-algorithmes-120543

NETTER Emmanuel, « Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls », in NETTER Emmanuel (dir.), *Regards sur le nouveau droit des données personnelles*, CEPRISCA, Collection Colloques, pp. 5-31.

NETTER Emmanuel, « *E-Privacy* ou la poursuite de la guerre contre la publicité ciblée par d'autres moyens », *Dalloz IP/IT*, avril 2021, n°4, pp. 226-229.

NETTER Emmanuel, « À quoi sert le principe de transparence en droit des données personnelles ? », *Dalloz IP/IT*, novembre 2020, n°11, pp. 611-615.

NIGUSSE Girma, **DE DECKER** Bart, « Capabilities and Limitations of P3P », *Katholieke Universiteit Leuven*, Report CW 539, mai 2009.

NISSENBAUM Helen, « A Contextual Approach to Privacy Online », *Dædalus*, Fall 2011, Volume 140, Issue 4, pp. 32-44.

NORBERG Patricia A., **HORNE** Daniel R. **HORNE** David A., « The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviours », *The Journal of Consumer Affairs*, 2007, Vol. 41, n°1, pp. 100-126.

NOUWENS Midas *et al.*, « Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence », *CHI Conference on Human Factors in Computing Systems*, 25-30 avril 2020, Honolulu, arXiv:2001.02479.

OBAR Jonathan A., « The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services », *Information, Communication & Society*, 2020, Volume 23, Issue 1, pp. 128-147.

OBERMEYER Ziad *et al.* « Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations », *Science*, n°366(6464), 25 octobre 2019, pp. 447-453.

O'HARA Kieron, « Explainable AI and the Philosophy and Practice of an Explanation », *Computer Law & Security Review*, 2020, n°39, 105474.

O'NEIL Onora, « Some limits of Informed Consent », *Journal of Medical Ethics*, 2003, n°29, pp. 4-7.

OSIER Étienne, « Préface » *in* SCHOPENHAUER Arthur, *Sur la liberté de la volonté*, Hermann, 2011, Traduit de l'allemand par OSIER Étienne.

PAGANO Ugo, « Crisis of Intellectual Monopoly Capitalism », *Cambridge Journal of* Economics, 2014, Vol. 38, pp.1409-1429.

PAILLER Ludovic, « L'applicabilité spatiale du Règlement général sur la protection des données (RGPD) – Commentaire de l'article 3 », *Journal du droit international (Clunet)*, n°3, juillet 2018, doctr. 9.

PARK Taehwan, « Optimistic Bias and Preventive Behavioral Engagement in the Context of COVID-19 », *Research in Social and Administrative Pharmacy*, Vol. 17, Issue 1, janvier 2021, pp. 1859-1866.

PLANE Eugénie, « Le droit de la compliance : quel bénéfice pour l'entreprise ? » *in* SAVALL Henri, ZARDET Véronique (dir.), *Tétranormalisation : profusion des normes et développement des entreprises*, EMS Edition, Collection Management socio-économique et recherche-intervention, 2020, pp. 174-183.

PLAUT Victoria. C., **BARTLETT** Robert P., « Blind consent? A social psychological investigation of non-readership of click-through agreements », *Law and Human Behavior*, 2012, 36(4), pp. 293–311

PENNEAU Anne, « La certification », *JurisClasseur Environnement et Développement Durable*, Fasc. 5300, 1e janvier 2013, mis à jour le 13 septembre 2019

PEREZ-RUBIO Lourdes Blanco, « La liberté personnelle de consentement : fondement éthique et juridique », *in Des liens et des droits, Mélanges en l'honneur de Jean-Pierre Laborde*, Paris, Dalloz, 2015, pp. 797-804.

PERRAY Romain, « Données à caractère personnel. – Bases juridiques applicables aux traitements de données à caractère personnel. Traitement reposant sur le consentement préalable de la personne concernée. Dispositions générales », *JurisClasseur Communication*, Fasc. 932-71, 7 décembre 2020.

PERRAY Romain, « Les outils de la conformité au RGPD : des outils de valorisation », *Revue des affaires européennes*, 2021/1, pp. 35-47.

PESSIGLIONE Mathias, « Comment le cerveau motive le comportement : du circuit de la récompense au système des valeurs », *Bull. Acad. Natle Méd.*, 2014, 198, n°7, pp. 1283-1296.

PETARD Jean-Pierre, « Connaissance du droit et psychologie », *Revue juridique de l'Ouest*, 1989, pp. 103-109.

PETTERSON John Sören, « A brief evaluation of icons suggested for use in standardized information policies. Referring to the Annex in the first reading of the European Parliament on COM(2012) 0011 », *in* CAMENISH Jan, FISCHER-HÜBNER Simone, HANSEN Marit (dir.), *Privacy and Identity Management for the Future Internet in the Age of Globalisation*, Privacy

and Identity 2014, IFIP Advances in Information and Communication Technology, vol. 457, Springer. pp. 125-135.

PEYROU-BARTOLL Sylvie, « Covid-19 et droits fondamentaux : la protection des données à caractère personnel à l'épreuve de la pandémie », *in* DUBOUT Édouard, PICOD Fabrice (dir.), *Coronavirus et droit de l'Union européenne*, 1e édition, Bruxelles, Bruylant, 2021, pp. 201-222.

PHILLIPS Mark, « International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), *Human Genetics*, 2018, vol. 137, pp. 575-582

PIERRON Jean-Philippe, « Le chemin trouble du consentement. Du consentement formel au consentement existentiel », *Les cahiers de la justice*, 2021, pp. 563-572.

PIZZIO Jean-Pierre, « Exigences linguistiques en matière d'étiquetages des produits mis sur le marché », *D.*, 2000, p. 42.

PLAUT Victoria. C., **BARTLETT** Robert P., « Blind consent? A social psychological investigation of non-readership of click-through agreements », *Law and Human Behavior*, 2012, 36(4), pp. 293-311.

PONCE DEL CASTILLO Aída, « La stratégie numérique de l'Europe : centrée sur les personnes, sur les données ou sur les deux ? », *in* VANHERCKE Bart, SPASOVA Slavina (dir.), *Bilan social de l'Union européenne 2021. Les ambitions renaissantes par temps de redressement de l'Union*, Bruxelles, ETUI, 2022, pp. 89-114.

PONTIER Jean-Marie, « La certification, outil de la modernité normative », *D.*, 1996, pp. 355-364.

PONTIER Jean-Marie, « Le juge communautaire, la langue française et les consommateurs », *D.*, 2001, pp. 1458-1464.

PORTAL Brigitte, « De l'*empowerment* anglo-saxon au développement du pouvoir d'agir européen », *Le Sociographe* », 2016, n°55, pp. 83-97.

POULLET Yves, « Avant-propos. Le RGPD – une volonté de bien faire : certes ! … mais appropriée ? », *in* DE TERWANGNE Cécile, ROSIER Karen (dir.), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Paris, Larcier, 2018, 1e ed., pp. 7-22.

POULLET Yves, **ROUVROY** Antoinette, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in* BENYEKHLEF Karim, TRUDEL Pierre (dir.), *Etat de droit et Virtualité*, Montréal, Thémis, 2009, pp. 157-222.

POULLET Yves, « Numérique, droit et vulnérabilités », *in* MATHIEU Géraldine *et al.* (dir.), *L'étranger, la veuve et l'orphelin. Le droit protège-t-il les plus faibles ?*, Liber Amicorum Jacques Fierens, Bruxelles, Larcier, 2020, pp. 419-438.

POWERS Thomas M., **GANASCIA** Jean-Gabriel, « The Ethics of the Ethics of AI », *in* DUBBER Markus D., PASQUALE Frak, DAS Sunit, *The Oxford Handbook of Ethics of AI*, Oxford University Press, 2020, pp. 26-51.

PRADES Jean-Luc, « L'imagination participative. Empowerment, pouvoir d'agir et actepouvoir, *Sciences & Actions sociales*, 2015, n°2, pp. 198-216.

PROULX Serge, **GOLDENBERG** Anne, « Internet et la culture de la gratuité », *Revue du MAUSS*, 2010/1, n° 35, pp. 503-517

PURTOVA Nadezhda, « The law of everything. Broad concept of personal data and future of EU data protection law », *Law Information and Technology*, Vol. 10, 2018, Issue 1, pp. 40-81.

QUÉRÉ Louis, « La structure cognitive et normative de la confiance », *Réseaux*, 2001, n°108, pp. 125-152.

QUESNEL Martin, « Concurrence entre économie et droit aux racines de l'identité européenne », *in* CARPANO Éric, MARTI Gaëlle (dir.), *Démocratie et marché dans l'Union européenne en crise*, pp. 53-70.

RACHELS James, « Why Privacy is Important », *Philosophy and Public Affairs*, n°4, 1975, pp. 323-333

RACHO Tania, « La vulnérabilité dans la charte des droits fondamentaux de l'Union européenne », *in* TINIÈRE Romain, VIAL Claire (dir.), *Les dix ans de la Charte des droits fondamentaux de l'Union européenne. Bilan et perspectives*, Bruxelles, Bruylant, 2020, pp. 53-70.

RALLET Alain, « Valoriser ses données personnelles ? 3 scénarios », *Document de travail*, disponible sur la plateforme HAL : https://hal.archives-ouvertes.fr/hal-01909650

RASCHKE Philip *et al.*, « Designing a GDPR-Compliant and Usable Privacy Dashboard » *in* KOSTA Eleni *et al.* (dir.), *Privacy and Identity Management. The Smart Revolution*, 12th Annual IFI Summer School on Privacy and Identity Management, Ispra, Italy, September 4-8, 2017, Revised Selected Papers, Springer, pp. 1-17.

REIDENBERG Joel R., « Resolving Conflicting International Data Privacy Rules in Cyberspace », *Standford L. Rev.*, n°52, 2000, pp. 1315-1371.

REIDENBERG Joel R *et al.*, « Privacy Harms and the Effectiveness of the Notice and Choice Framework », *TPRC Conference Paper*, 2014, disponible sur SSRN : https://ssrn.com/abstract=2418247

REINDERNBERG Joel R. *et al.*, « Disagreeable Privacy Policies: Mismatches between meaning and users' understanding », *Berkeley Technology Law Journal*, 2015, Vol. 30:1, pp. 39-68.

REINER Günter, « Les dichotomies en droit », *in* AZZARIA Georges (dir.), *Les nouveaux chantiers de la doctrine juridique. Actes des 4e et 5e journées d'étude sur la méthodologie et l'épistémologie juridiques*, Laval, Éditions Yvon Blais, 2016, pp. 407-457.

REMPELL Scott, « Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas », *Florida Journal of International Law,* 2006, Vol. 18, Issue 3, Article 2.

RENIER Grégory, « Chapter 4 – Personal data class actions three years after the application of the GDPR », *in* JACQUEMIN Hervé (dir.), *Time to Reshape the Digital Society*, Bruxelles, Larcier, 2021, pp. 135-157.

RICHARDS Neil M., **HARTZOG** Woodrow, « The Pathologies of Digital Consent », *Washington University Law Review*, Vol. 96, Issue 6, pp. 1461-1503.

RICHMOND Riva, « A Loophole Big Enough for a Cookie to Fit Through », *The New York Times*, 17 septembre 2019, disponible sur https://bits.blogs.nytimes.com/2010/09/17/a-loophole-big-enough-for-a-cookie-to-fit-through/

RIGAUX François, « Le juge, arbitre de la certitude du droit », *in* MACKAAY Ejan (dir.), *Les certitudes du droit*, pp. 19-55.

RIVAL Madina, « Vers un lobbying éthique ? Ou comment pratiquer l'influence sans corruption », *Entreprise éthique*, Association Francophone de Comptabilité, 2006, n°24, pp. 20-27.

RIZK Hadi, « Locke : la tolérance et le consentement, ou l'autolimitation du pouvoir politique », *L'enseignement philosophique*, 2015, 65e année, pp. 60-71.

ROBERT Cécile, « La transparence comme nouvel horizon des démocraties européennes : Genèses et usages d'une injonction ambivalente », *Politique européenne*, 2018, n°61, pp. 8-43.

ROBUSTELLI Ludovica, « La distinction entre les articles et 8 de la Charte dans la jurisprudence de la Cour de Justice de l'Union européenne », *in* TINIÈRE Romain, VIAL Claire (dir.), *Les dix ans de la Charte des droits fondamentaux de l'Union européenne. Bilan et perspectives*, Bruxelles, Bruylant, 2020, pp. 29-40.

RODRIGUES Rowena *et al.*, « The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR », *International Review of Law, Computers & Technology*, 2016, n°30(3), pp. 248-270.

RODRIGUES Rowena, **WRIGHT** David, **WADHWA** Kush, « Developing a privacy seal scheme (that works) », *International Data Privacy Law*, Volume 3, Issue 2, mai 2013, pp. 100-116.

RODRIGUEZ Karine, « Étude 59 – Associations de défense des consommateurs », *in* DUTHEIL Philippe-Henri (dir.), *Droit des associations et fondations*, Paris, Dalloz, Juriscorpus, 2016, mis à jour en Juillet 2022.

ROLLAND Louise, « Qui dit contractuel, dit juste. » (Fouillée) … en trois petits bonds, à reculons », *McGill Law Journal*, vol. 5, 2006, pp. 768-769.

ROSA Harmut, « Social Acceleration: Ethical and Political Consequences of a Desynchronized High-Speed Society », *in* ROSA Harmut (dir.), *High-Speed Society: Social Attention, Power, and Modernity*, Penn State Press, 2010, pp. 77-112.

ROSE Hubert, « Durée du travail : fixation et aménagement du temps de travail », *Répertoire du droit du travail*, Octobre 2020, mis à jour en Juillet 2022.

ROSIER Karen, « Titre 12 – La notion de « donnée à caractère personnel » a-t-elle encore un sens dans la protection des données de communications électroniques ? », *in* DEGRAVE Élise *et al.* (dir.), *Law, Norms and Freedom in Cyberspace / Droit, normes et libertés dans le cybermonde*, Larcier, Liber Amicorum Yves Poulet, 2018, pp. 699-714.

ROSSI Arianna, **PALMIRANI** Monica, « Can Visual Design Provide Legal Transparency? The Challenges of Icons for Data Protection », *Design Issues*, 2020, Vol. 36(3), pp. 82-96.

ROSSI Augustín, « How the Snowden Revelations Saved the EU General Data Protection Regulation », *The International Spectator*, 2018, vol. 53, n°4, pp. 95-111.

ROSSI Franscesca, « Building Trust in Artificial Intelligence », *Journal of International Affairs*, 2019, vol. 72, n°1, pp. 127-134.

ROUSSILLE Myriam, « Conflits d'intérêts : la transparence sauve-t-elle les apparences ? », *Bulletin Joly Bourse*, 2021, n°4, p. 1.

ROUVIÈRE Frédéric, « Le moment d'appréciation de l'erreur », *D.*, 2014, pp. 1782-1786.

ROUVROY Antoinette, **POULLET** Yves, « The Right to Informational Self Determination and the Value of Self Development: Reassessing the Importance of Privacy for Democracy », *in* GUTWIRTH Serge *and al.* (dir.), *Reinventing Data Protection?*, Springer Netherlands, pp. 45-76.

SAGHAI Yashar, « Salvaging the concept of nudge », *Journal of Medical Ethics*, 2013, n°39, pp. 487-493.

SAURON Jean-Luc, « Le RGPD : outil ou entrave de la société d'information ? », *Dalloz IP/IT*, 2018, pp. 17-22.

SCHALL Jeffrey D., « Neural Basis of Deciding, Choosing and Acting », *Nature Review Neuroscience*, 2001, 2, pp. 33-42.

SCHERMER Bart W., **CUSTERS** Bart, **VAN DER HOF** Simone, « The Crisis of Consent. How Stronger Legal Protection May Lead to Weaker Consent in Data Protection », *Ethics & Information Technology*, 2014, Vol. 15, pp. 171-182.

SCHOLTEN Matthé, **GATHER** Jakov, **VOLLMANN** Jochen, « Equality in the Informed Consent Process: Competence to Consent, Substitute Decision-Making, and Discrimination of Persons with Mental Disorders », *The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine*, Février 2021, Volume 46, Issue 1, pp. 108-136.

SCHWARTZ Ari, « Looking Back at P3P: Lessons for the Future », *Center for Democracy &* Technology, novembre 2009, disponible sur https://cdt.org/insights/looking-back-at-p3p-lessons-for-the-future/.

SCHWARTZ Paul M., « Privacy and Democracy in Cyberspace », *Vanderbilt Law* Review, vol. 52, 1999, pp. 1609-1999.

SCHWARTZ Paul M., « Internet Privacy and the State », *Connecticut Law Review,* 2000, Vol. 32, pp. 815-859.

SCHWARTZ Paul M., « The EU-U.S. Privacy Collision : A Turn to Institutions and Procedures », *Harvard Law Review*, 2013, vol. 126, pp. 1966-2008.

SCHWEITZER Heike, « The Art to Make Gatekeeper Positions Contestable and the Challenge to Know What is Fair: A Discussion of the Digital Markets Act Proposal, *ZEuP*, 2021, issue 3 pp. 522-523

SEMINARA Letizia, « Risk Regulation and the European Convention on Human Rights », *European Journal of Risk Regulation*, 2016, n°4, pp. 733-749.

SENOL Asuman *et al*., « Leaky Forms : A Study of Email and Password Exfiltration Before Form Submission », *USENIX Security'22*, pp. 1813-1830.

SERVERIN Évelyne, « Introduction. Une enquête juridique sur la place du collectif dans la justice contemporaine », *in* OMARJEE Ismaël, SINOPOLI Laurence (dir.), *Les actions en justice au-delà de l'intérêt personnel*, Dalloz, 2014, pp. 3-12.

SHIN Donghee, « The Effects of Explainability and Causability on Perception, Trust and Acceptance: Implications for Explainable AI », *International Journal of Human-Computer Studies*, 2021, vol. 146, 102551.

SIEGRIST Michael *et al.*, « Perception of Risk: the Influence of General Trust, and General Confidence », *Journal of Risk Research*, 2005, Volume 8, Issue 2, pp. 145-156.

SIMON Éric, « La confiance dans tous ses états », *Revue française de gestion*, 2007, n°175, pp. 83-94.

SIMON Herbert A., « Designing Organizations for an Information-Rich World », *in* GREENBERGER Martin (dir.), *Computers, Communications, and the Public Interest*, Baltimore, The Johns Hopkins Press, 1971, pp. 38-72.

SINOPOLI Laurence, « Chapitre 1. La légitimité des porteurs de l'action de groupe : entre représentation et qualité », », *in* OMARJEE Ismaël, SINOPOLI Laurence (dir.), *Les actions en justice au-delà de l'intérêt personnel*, Dalloz, 2014, pp. 23-42.

SLEEPER Manya *and al.* « The Post that Wasn't: Exploring Self-Censorship on Facebook », *Proceedings of the 2013 Conference on Comuter Supported Cooperative Work – CSCW'13*, pp. 793-802.

SMYRNAIOS Nikos, « L'effet GAFAM : stratégies et logiques de l'oligopole de l'internet », *Communication & Langages*, 2016/2, n°188, pp. 61-83.

SOLOVE Daniel, **SCHWARTZ** Paul M., « Privacy Law Fundamentals », *International Association of Privacy Professionals*, 2013, disponible sur SSRN : https://ssrn.com/abstract=1790262.

SOLOVE Daniel J., « The Myth of the Privacy Paradox », *George Washington Law Review*, 2021, Volume 89, Issue 1, pp. 1-51.

SPIEKERMANN Sarah, **GROSSKLAGS** Jens, **BERENDT** Bettina, « Stated Privacy Preferences versus Actual Behavious in EC Environments : a Reality Check », *in* BUHL Hans Ulrich, KREYER Nina, STECK Werner (dir.), *e-Finance*, Berlin, Springer, 2001, pp. 129-147.

SPIEKERMANN Sarah *et al.* « Data protection in Europe – Academics are taking a position », *Computer Law & Security Review*, avril 2013, 29(2), pp. 180-184.

SPINA ALÌ Gabriele, **YU** Ronald, « Artificial Intelligence between Transparency and Secrecy: From the EC Whitepaper to the AIA and Beyond », *European Journal of Law and Technology*, 2021, vol. 12, n°3, disponible sur https://ejlt.org/index.php/ejlt/article/view/754.

STAUTON Ciara, **SLOKENBERGA** Santa, **MASCALZONI** Deborah, « The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks », *European Journal of Human Genetics*, 2019, pp. 1159-1167.

STOEKLÉ Henri-Corto *et al.*, « Vers un consentement éclairé dynamique », *Med Sci (Paris)*, Vol. 33, No 2, 2017, pp. 188-192.

STOLJAR Natalie, « Informed Consent and Relational Conceptions of Autonomy », *Journal of Medicine and Philosophy*, 2011, n°36, pp. 375-384**.**

STORCK Michel, « Synthèse – Consentement », *JurisClasseur Civil Code*, mis à jour le 1e juin 2020.

STROUD Sarah, **SVIRSKY** Larisa, « Weakness of Will », Stanford Encyclopedia of Philosophy, publié le 14 mai 2008, révisé le 4 septembre 2019, disponible sur https://plato.stanford.edu/entries/weakness-will/

STUYCK Jules, *Fasc. 2000 : Politique européenne de la consommation*, JurisClasseur Europe Traité, 14 avril 2020,

SUSSER Daniel *et al.*, « Technology, autonomy, and manipulation », *Internet Policy Review*, 2019, vol. 8, issue 2.

SUSSER Daniel *et al.*, « Online Manipulation : Hidden Influence in a Digital World », *Georgetown Law Technology Review*, 2019, vol. 4.1, pp. 1-45.

SUSTEIN Cass R., « Do People Like Nudges? », *Administrative Law Review*, Vol. 68, n°2, pp. 177-232.

SUSTEIN Cass R., **THALER** Richard H., « Libertarian Paternalism is Not an Oxymoron », *The University of Chicago Law Review,* 2003, n°70(4), pp. 1159-1202.

SUSTEIN Cass R., « Fifty Shades of Manipulation », *J. Behavioral Marketing,* 2016, vol. 213, pp. 78-115.

S**USTEIN** Cass R., **THALER** Richard H. , « Libertarian Paternalism », *The American Economic Review*, Vol. 93, No. 2, Papers and Proceedings of the One Hundred Fifteenth Annual Meeting of the American Economic Association, Washington, DC, January 3-5, 2003, pp. 175-179.

SWIRE Peter, « Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment », *North Carolina Law Review*, 2012, vol. 90, n°5, pp. 1371-1416.

TAMBOU Olivia, « L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ? », *Revue Lamy de Droit de l'Immatériel*, avril 2016, pp. 43-48.

TANG Jie, **AKRAM** Umair, **SHI** Wenjing, « Why people need privacy? The role of privacy fatigue in app user's intention to disclose privacy based on personality traits », *Journal of Enterprise Information Management*, 2021, Vol. 34, n°4,

TAVANI Herman T. « Philosophical theories of privacy: Implications for an adequate online privacy policy », *Metaphilosophy*, 38.1, 2007, pp. 1-22.

TAYLOR Curtis, **LIAD** Wagman, « Consumer Privacy in Oligopolistic Markets : Winners, Losers and Welfare », *International Journal of Industrial Organization*, vol. 34, mai 2014, pp. 80-84

TCHIDER Charlotte A., « The Consent Myth: Improving Choice for Patients of the Future », 96 *Wash. U. L. Rev.*, 2018-2019, pp. 1505-1536.

TESFAY Welderufael B. *et al*., « PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation », *Fourth ACM International Workshop on Security and Privacy Analytics – IWSPA '18,* Proceedings, pp. 15-21.

THALER Richard H., « Nudge, not sludge », *Science*, vol. 361, issue 6401, 2018, p. 431.

THELISSON Eva, « Towards Trust, Transparency, and Liability in AI/AS Systems », *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17)*, 10#7, pp. 5215-5216.

TINIÈRE Romain, « Propos introductifs », *in* TINIÈRE Romain, VIAL Claire (dir.), *Les dix ans de la Charte des droits fondamentaux de l'Union européenne. Bilan et perspectives*, Paris, Bruylant, 2020, pp. 11-26.

TOSI-DUPRIET Isabelle, « Le consentement aux atteintes aux droits de la personnalité, un fait juridique : la doctrine *Ancel* », *in* DEUMIER Pascale *et al.* (dir.), *Mélanges en l'honneur de Pascal Ancel*, 1e édition, Bruxelles, Larcier, 2021, pp. 587-601.

TRACOL Xavier, « "Schrems II": The return of the Privacy Shield », *Computer Law & Security Review*, Vol. 39, novembre 2020, 105484.

TROADEC Bertrand, « La relation entre culture et développement cognitif : une introduction », *Enfance*, 2006/2, vol. 58, pp. 108-117

TUORI Kaarlo, « La Constitution économique parmi les Constitutions européennes », *Revue internationale de droit économique*, 2011/4, Tome XXV, pp. 559-599.

UNGER Wayne, « Katz and Covid-19. How a Pandemic Changed the Reasonable Expectation of Privacy », *Hastings Science and Technology Law Journal*, Volume 12, 2020, pp. 39-82.

USUNIER Laurence, « L'action de groupe européenne au milieu du gué », *RTD Civ.*, 2021, pp. 370-375.

VAN DER HOF Simone, « I Agree or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World », *Wisconsin International Law Journal*, vol. 34, no. 2, Winter 2016, pp. 409-445.

VERBRUGGEN Valérie, « Titre 1 – RGPD : cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne », *in* DE TERWANGNE Cécile, ROSIER Karen (dir.), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Paris, Larcier, 2018, 1e ed., pp. 25-58.

VIALLA François, « Enjeux et logique de l'information comme préalable au consentement », *in* AFDS (dir.), *Consentement et santé*, Paris, Dalloz, 2014, pp. 35-44.

VIALLA François, « Bref retour sur le consentement éclairé », *D.*, 2011, pp. 292-295.

VINEY François, « L'expansion du « raisonnable » dans la réforme du droit des obligations : un usage déraisonnable ? », *D.*, 2016, pp. 1940-1941.

VOHS Kathleen D. *and al.*, « Making Choices Impairs Subsequent Self-Control: A Limited-Resource Account of Decision Making, Self-Regulation, and Active Initiative », *Journal of Personality and Social Psychology*, 2008, Vol. 94, n°5, pp. 883-898.

VON GRAFENSTEIN Max, **JAKOBI** Tibo, **STEVENS** Gunnar, « Effective data protection by design through interdisciplinary research methods : The example of *effective* purpose specification by applying user-Centred UX-design methods », *Computer Law & Security Review*, vol. 46, septembre 2022, pp. 1-22

VUGTS Anastasia *et al.*, « How autonomy is understood in discussions on the ethics of nudging », *Behavioural Public Policy*, 2008, Volume 4, Issue 1, pp. 108-123.

WALDMAN Ari Ezra, « Cognitive biases, dark patterns, and the "privacy paradox" », *Current Opinion in Psychology*, Volume 31, 2020, pp. 105-109.

WALKER Kent, « The Costs of Privacy », *Harvard Journal of Law and Public Policy*, vol. 25, 2001, pp. 87-128.

WARD Jonathan Stuart, **BARKER** Adam, « Undefined By Data: A Survey of Big Data Definitions », 20 septembre 2013, arXiv:1309.5821.

WEST Sarah Myers, **WHITTAKER** Meredith, **CRAWFORD** Kate, « Discriminating Systems: Gender, Race, and Power in AI », *AI Now Institute*, avril 2019, disponible sur https://ainowinstitute.org/discriminatingsystems.pdf

WESTIN Alan F., « Privacy and Freedom », *Wash. & Lee L. Rev.*, n°25, pp. 1064-1075.

WEINSTEIN Michael A., « The Uses of Privacy in Good Life», *in* PENNOCK J. Roland, CHAPMAN, John W. (dir.), *Nomos XIII: Privacy*, New York, Atherton Press, 1971, pp. 88-104.

WEITZNER Daniel J. *and al.*, « Information Accountability », *Communications of the ACM*, 2008, Vol. 51, n°6, pp. 82-87.

WILLIAMS Betsy Anne *et al.*, « How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions and Policy Implications », *Journal of Information Policy*, 2018, Vol. 8, pp. 78-115.

WOODS Daniel W., **BÖHME** Rainer, « The Commidification of Consent », *Computer & Security*, avril 2022, volume 115, disponible sur https://www.sciencedirect.com/science/article/pii/S0167404822000049

WU Heng *et al.*, « The Role of Push_Pull Technology in Privacy Calculus: The Case of Location Based Services », *Journal of Management of Information Systems*, 2009, 26:3, pp. 135-174.

WU Kuang-Wen *et al.* « The effect of online privacy policy on consumer privacy concern and trust », *Computers in Human Behavior*, Volume 28, Issue 3, mai 2012, p. 889-897

WU Tim, « Blind Spot ; Attention Economy and the Law », *Antitrust Law Journal*, 2019, vol. 82, n°3, pp. 771-806.

YUHAS Katherine, « Subscribe Here For More: Analyzing the Video Privacy Protection Act in the Mobile Era », *Southern Illinois University Law Journal*, 2008, 42(2), pp. 389-408.

ZAEEL Razieh Nokhbeh, « PrivacyCheck v3 : Empowering Users with Higher-Level Understanding of Privacy Policies », *WSDM '22: Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining*, Février 2022, pp. 1593-1596.

ZIELINSKI Agata, « Le libre choix. De l'autonomie rêvée à l'attention aux capacités », *Gérontologie et société*, 2009/4, vol. 32, n°131, pp. 11-24.

ZIMMERMANN Christian *et al.*, « Privacy Dashboards: Reconciling data-driven business models and privacy », *2014 Ninth International Conference on Availability, Reliability and Security*, Fribourg, 2014, pp. 152-157.

ZOLYNSKI Célia, **LE ROY** Marylou., **LEVIN** François, « L'économie de l'attention saisie par le droit », *Dalloz IP/IT*, 2019, pp. 614-622.

ZOLYNSKI Célia, **LE ROY** Marylou, « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *Legicom*, 2017, pp. 105-114.

Z**OLYNSKI** Célia, « Protection + Agentivité, la nouvelle équation pour penser les relations entre consommateurs et intelligences artificielles », *in* CANAL FORGUES ALTER Éric, HAMROUNI Maïa-Oumeïma (dir.), *Intelligence artificielle*, Bruxelles, Bruylant, 2021, pp. 193-206.

ZUBCEVIC Oriane, « Le « California Consumer Privacy Act » est-il le RGPD américain ? », *Éditions Législatives*, 28 janvier 2020

ZUBOFF Shoshana, « Le capitalisme de la surveillance. Un nouveau clergé », *Esprit*, 2019, n°5, pp. 63-77.

ZUIDERVEEN BORGESIUS Frederik J. *et al.*, « Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation », *European Data Protection Law Review*, Volume 3, Issue 3, pp. 353-368.

V. DOCUMENTS INSTITUTIONNELS

A. NATIONAUX

1. Avis, recommandations, guides et lignes directrices

CNCDH, 22 mai 2018, *Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique*.

CNCDH, 7 avril 2022, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*.

CNIL, *Délibération 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et autres traceurs visés par l'article 32-II de la loi du 6 janvier 2018*.

CNIL, *Délibération n°2018-303 du 6 septembre 2018 portant adoption d'une recommandation concernant le traitement de données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance et abrogeant la délibération n°2017-222 du 20 juillet 2017*.

CNIL, *Délibération n°2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs)*.

CNIL, *Délibération n°2020-01 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « coolies et autres traceurs ») et abrogeant la délibération n°2019-093 du 4 juillet 2019*.

CNIL, *Guide pratique. Les durées de conservation*, juillet 2020, 21 pages.

CNIL, *Guide de sensibilisation au RGPD pour les collectivités territoriales*, 2021, 43 pages.

CNNum, « Stop Covid », *Avis du Conseil national du Numérique*, 24 avril 2020.

Défenseur des droits, *La Convention relative aux droits des personnes handicapées. Comprendre et mobiliser la Convention pour défendre les droits des personnes handicapées*, Guide, décembre 2016.

2. Rapports et études

Assemblée nationale, *Étude d'impact du projet de loi relatif à la consommation*, 30 avril 2013, disponible sur https://www.assemblee-nationale.fr/14/projets/pl1015-ei.asp#P2643_381570.

Assemblée nationale, *Rapport d'information sur le bilan et les perspectives des actions de groupe*, déposé en application de l'article 145 du Règlement par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, 11 juin 2020, n°3085.

Assemblée nationale, *Rapport d'information sur les plateformes numériques déposé en application de l'article 145 du Règlement par la Commission des affaires économiques*, présenté par Mme Valérie FAURE-MUNTIAN et M. Daniel FASQUELLE, députés, 24 juin 2020, n°3127.

Assemblée nationale, *Rapport fait au nom de la Commission des affaires européennes sur la proposition de résolution européenne (n°4195) relative à la protection des personnes,* enregistré à la Présidence de l'Assemblée nationale le 7 octobre 2021.

Assemblée nationale, **Sénat,** *Pour une intelligence artificielle maîtrisée, utile et démystifiée,* Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, n°4594 et 464, 15 mars 2017.

CNIL, Rapport d'activité, 2012, La Documentation française.

CNIL, Rapport d'activité, 2014, La Documentation française.

CNIL, Rapport d'activité, 2017, La Documentation française.

CNIL, Rapport d'activité, 2019, La Documentation française.

CNIL, Rapport d'activité, 2020, La Documentation française**.**

CNNum, *Ambition numérique. Pour une politique française et européenne de la transition numérique,* Rapport remis au Premier ministre, juin 2015.

Conseil d'État, *Le numérique et les droits fondamentaux*, Les rapports du Conseil d'État, 2014

Cour de cassation, « Étude : Les personnes vulnérables dans la jurisprudence de la Cour de cassation », *Rapport 2009*

DGCCRF, *État des lieux de la réglementation encadrant l'information du consommateur*, Document de travail, décembre 2012

GOUZES Gérard, *Rapport fait au nom de la commission des Lois constitutionnelles, de la législation et de l'administration générale de la république sur le projet de loi (n°3250), relatif à la protection des personnes physiques à l'égard des traitement 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, Rapport à l'Assemblée Nationale n°3526, enregistré à la Présidence de l'Assemblée nationale le 9 janvier 2002.

LINC, « La forme des choix. Données personnelles, design et frictions désirables », *Cahiers IP Innovation & Prospective*, n°6.

Sénat, « L'action de groupe à la française : parachever la protection des consommateurs », *Rapport d'information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail sur l'action de groupe,* 26 mai 2010, n°499.

Sénat, « Le devoir de souveraineté numérique », *Rapport n°7 (2019-2020) de M. Gérard Longuet, fait au nom de la commission d'enquête,* déposé le 1er octobre 2019.

Sénat, *Rapport fait au nom de la commission d'enquête sur la souveraineté numérique,* 1e octobre 2019, Session ordinaire, disponible sur https://www.senat.fr/rap/r19-007-2/r19-007-2.html

Sénat, « Mieux organiser la Nation en temps de crise », *Rapport d'information*, 8 juillet 2020, disponible sur http://www.senat.fr/rap/r19-609/r19-60935.html

TÜRK Alex, *Rapport fait au nom de la commission des Lois constitutionnelles, de la législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée nationale, relatif à la protection des personnes physiques à l'égard des traitement 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,* Rapport au Sénat n°218, Annexe au procès-verbal de la séance du 19 mars 2003.

3. Discours, allocations et auditions

Assemblée Nationale, *Audition de Mme Fleur Pellerin, ministre déléguée auprès du ministre du redressement productif, chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique*, Commission des affaires européennes, 2 octobre 2013, disponible sur https://www.assemblee-nationale.fr/14/europe/c-rendus/c0084.asp#P5_269

SAUVÉ Jean-Marc, « À quoi sert la concurrence ? », *Allocation d'ouverture du colloque organisé par la revue Concurrences à l'Assemblée nationale le 4 décembre 2014*, disponible sur https://www.conseil-etat.fr/actualites/discours-et-interventions/a-quoi-sert-la-concurrence

SAUVÉ Jean-Marc, « Transparence et efficacité de l'action publique », *Intervention lors de l'Assemblée générale de l'administration*, 3 juillet 2017, disponible sur le site du Conseil d'État

: https://www.conseil-etat.fr/actualites/discours-et-interventions/transparence-et-efficacite-de-l-action-publique

4. Débats et autres publications au journal officiel

Assemblée nationale, Amendement n°146 présenté par Mme Mme Rubin, Mme Autain, M. Bernalicis, M. Coquerel, M. Corbière, Mme Fiat, M. Lachaud, M. Larive, M. Mélenchon, Mme Obono, Mme Panot, M. Prud'homme, M. Quatennens, M. Ratenon, Mme Ressiguier, M. Ruffin et Mme Taurine, visant à modifier l'article 4 de la loi n°2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle,* Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une république numérique, décembre 2017.

Journal Officiel de la République Française (JORF), 5 octobre 1977 (séance du 4 octobre 1977), p. 5792, disponible sur http://archives.assemblee-nationale.fr/5/cri/1977-1978-ordinaire1/002.pdf.

PEYRAT Bernard, « La publicité ciblée en ligne », *Communication présentée en séance plénière*, CNIL, 5 février 2009.

PEYREFITTE Alain, Garde des sceaux, Journal Officiel de la République Française (JORF), 5 octobre 1977 (séance du 4 octobre 1977), p. 5789, disponible sur http://archives.assemblee-nationale.fr/5/cri/1977-1978-ordinaire1/002.pdf.

Sénat, Résolution européenne pour une réforme des conditions d'utilisation des mesures conservatoires prévues par le règlement (CE) n°1/2003 du Conseil relatif à la mise en œuvre des règles de concurrence, Session extraordinaire, 8 septembre 2017.

Sénat, Question d'actualité au gouvernement n°0934G de M. Claude Malhuret, publiée dans le JO Sénat du 3 octobre 2019, disponible sur https://www.senat.fr/questions/base/2019/qSEQ19100934G.html.

Sénat, Déclaration de Mme Agnès Pannier Runacher, ministre de l'industrie, sur la souveraineté économique de la France, au Sénat le 4 mai 2021, *Débat organisé au Sénat à la demande du groupe Les Républicains*, disponible sur https://www.vie-publique.fr/discours/279908-agnes-pannier-runacher-04052021-souverainete-economique.

VILLA Lucien, Journal Officiel de la République Française (JORF) n°79 A.N., 5 octobre 1977, p. 5787.

5. Communiqués de presse, communications et échanges épistolaires

Autorité de la concurrence, « L'Autorité sanctionne Google à hauteur de 150 M€ pour abus de position dominante », *Communiqué de presse,* 20 décembre 2019, disponible sur https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/lautorite-sanctionne-google-hauteur-de-150-meu-pour-abus-de-position.

CNIL, « Google's new privacy policy : incomplete information and uncontrolled combination of data across services » *Communiqué de presse,* 16 octobre 2012.

CNIL, *Charte des contrôles de la CNIL*, version du 5 août 2020.

CNNum, « 5 questions à Maryanne Wolf : « Nous devons comprendre ce que fait chaque technologie, et être capables de choisir » », *cnnumerique.fr*, 20 mai 2021, disponible sur https://cnnumerique.fr/5-questions-maryanne-wolf-nous-devons-comprendre-ce-que-fait-chaque-technologie-et-etre-capables-de

CNNum, « Pour un numérique au service des savoirs. De l'informatisation à la capacitation », *cnnumérique.fr*, mai 2021, disponible sur https://cnnumerique.fr/files/uploads/2021/CNNum_Pour_un_numerique_au_service_des_savoirs_mai_2021.pdf

Défenseur des droits, « Intelligence artificielle : la Défenseure des droits appelle à replacer le principe de non-discrimination au cœur du projet de règlement de la Commission européenne », *Communiqué de presse*, Paris, 21 juin 2022.

Conseil national des barreaux (CNB), *Dix propositions du Conseil national des barreaux au Président de la République*, CNB.avocat.fr, mai 2017.

Conseil national des barreaux (CNB), *Réponses du candidat Emmanuel Macron aux questions du CNB,* CNB.avocat.fr, mai 2017.

6. Sites internet institutionnels

Autorité de la concurrence, « Les vertus de la concurrence », disponible sur https://www.autoritedelaconcurrence.fr/fr/les-vertus-de-la-concurrence.

BPI France, « Silver économie : la mise en orbite », *bpifrance.fr,* 16 juin 2016, disponible sur https://www.bpifrance.fr/nos-actualites/silver-economie-la-mise-en-orbite

CNIL, « Anciennes normes », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/les-cadres-de-reference/anciennes-normes

CNIL, « Big data », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/definition/big-data

CNIL, « Ce qu'il faut savoir sur la certification », *CNIL.fr*, 17 février 2021, disponible sur https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-la-certification

CNIL, « Certification des compétences du DPO : la CNIL adopte deux référentiels », *CNIL.fr*, 11 octobre 2018, disponible sur https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels

CNIL, « Comment concilier les durées de conservation et les archives », *CNIL.fr*, 18 septembre 2019, https://www.cnil.fr/fr/comment-concilier-les-durees-de-conservation-et-les-archives

CNIL, « Comment se passe un contrôle de la CNIL ? », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/comment-se-passe-un-controle-de-la-cnil

CNIL, « Conformité RGPD : comment informer les personnes et assurer la transparence ? », CNIL.fr, 26 juillet 2019, *CNIL.fr*, disponible sur https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence

CNIL, « Conformité RGPD : comment recueillir le consentement des personnes ? », *CNIL.fr*, 3 août 2018, disponible sur https://www.cnil.fr/fr/les-bases-legales/consentement.

CNIL, « Cookies et traceurs : que dit la loi ? », *CNIL.fr*,1er octobre 2020, disponible sur https://www.cnil.fr/fr/cookies-et-traceurs-que-dit-la-loi

CNIL, « Cookies walls et monétisation des données personnelles : les enjeux juridiques et éthiques », *CNIL.fr*, 31 mai 2021, disponible sur https://www.cnil.fr/en/node/121204

CNIL, « Cookies : solutions pour les outils de mesure d'audience », *CNIL.fr*, 8 mars 2021, disponible sur https://www.cnil.fr/fr/cookies-solutions-pour-les-outils-de-mesure-daudience

CNIL, « Évènement : la CNIL organise la première édition du Privacy Research Day, 18 février 2022, disponible sur https://www.cnil.fr/fr/evenement-la-cnil-organise-la-premiere-edition-du-privacy-research-day

CNIL, « Fichier de lobbying : sanction de 400 000 euros à l'encontre de la société MONSANTO », *CNIL.fr*, 28 juillet 2021, disponible sur https://www.cnil.fr/fr/fichier-de-lobbying-sanction-de-400-000-euros-lencontre-de-la-societe-monsanto

CNIL, « L'intérêt légitime : comment fonder un traitement sur cette base légale ? », *CNIL.fr*, 2 décembre 2019, disponible sur https://www.cnil.fr/fr/les-bases-legales/interet-legitime

CNIL, « L'intérêt légitime : comment fonder un traitement sur cette base légale ? », *CNIL.fr*, 2 décembre 2019, disponible sur https://www.cnil.fr/fr/les-bases-legales/interet-legitime

CNIL, « La CNIL appelle à des évolutions dans l'utilisation des outils collaboratifs états-uniens pour l'enseignement supérieur et la recherche », *CNIL.fr*, 27 mai 2021, disponible sur https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche

CNIL, « La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques », *CNIL.fr*, 17 juin 2020, disponible sur https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras

CNIL, « La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société Google LLC », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la

CNIL, « La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD », *CNIL.fr*, 2 décembre 2019, disponible sur https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales

CNIL, « La Plateforme des données de santé (Health Data Hub) », *CNIL.fr*, 9 février 2021, disponible sur https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub

CNIL, « Les pouvoirs de la formation restreinte », *CNIL.fr*, 25 octobre 2019, disponible sur https://www.cnil.fr/fr/les-pouvoirs-de-la-formation-restreinte

CNIL, « Nouvelles règles pour les cookies et autres traceurs : bilan de l'accompagnement de la CNIL et actions à venir », *CNIL.fr*, 2 avril 2021, disponible sur https://www.cnil.fr/fr/nouvelles-regles-cookies-et-autres-traceurs-bilan-accompagnement-cnil-actions-a-venir

CNIL, « Publicité ciblée en ligne : quels enjeux pour la protection des données personnelles ? », *CNIL.fr*, 14 janvier 2020, disponible sur https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles

CNIL, « Quantified self », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/definition/quantified-self

CNIL, « Silver économie et données personnelles », *Pack de conformité*, novembre 2017, disponible sur https://www.cnil.fr/sites/default/files/atoms/files/pack_silver_economie_v4.pdf

CNIL, « Solutions de mesure d'audience exemptées de consentement : la CNIL lance un programme d'évaluation », *CNIL.fr*, 8 mars 2021, disponible sur https://www.cnil.fr/fr/solutions-de-mesure-daudience-exemptees-de-consentement-la-cnil-lance-un-programme-devaluation

CNIL, « Spartoo : sanction de 250 000 euros et injonction sous astreinte de se conformer au RGPD », *CNIL.fr*, 5 août 2020, disponible sur https://www.cnil.fr/fr/spartoo-sanction-de-250-000-euros-et-injonction-sous-astreinte-de-se-conformer-au-rgpd

CNIL, « Startup : comment faire de votre conformité RGPD un avantage concurrentiel ? », *CNIL.fr*, disponible sur https://www.cnil.fr/fr/startup-comment-faire-de-votre-conformite-rgpd-un-avantage-concurrentiel

CNIL, « Véhicules connectés et données personnelles », *Pack de conformité*, octobre 2017

CNIL, « Vie privée des enfants : une protection insuffisante sur les sites Internet », *CNIL.fr*, 2 septembre 2015, disponible sur https://www.cnil.fr/fr/vie-privee-des-enfants-une-protection-insuffisante-sur-les-sites-internet-0

CNIL, 10 février 2022, « Utilisation de Google Analytics et transferts de données vers les États-Unis : la CNIL met en demeure un gestionnaire de site web », 10 février 2022, disponible sur https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure

CNNum, « Le Conseil », disponible sur https://cnnumerique.fr/le-conseil

Commission européenne, « Big data », *Europa.eu*, disponible sur https://digital-strategy.ec.europa.eu/en/policies/big-data

Commission européenne, « Excellence et confiance en matière d'intelligence artificielle », *ec.europa.eu*, disponible sur https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_fr

Commission européenne, « Une Europe adaptée à l'ère numérique », *ec.europa.eu*, disponible sur https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_fr

Conseil européen, **Conseil de l'Union européenne**, « Réglementer l'utilisation des données des dossiers passagers (PNR) », disponible sur https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/passenger-name-record/.

DUMAS Anne-Gaëlle, « Zoom sur l'action de groupe en matière de consommation », *justice.gouv.fr*, 12 mars 2015, disponible sur http://www.textes.justice.gouv.fr/dossiers-thematiques-10083/loi-du-170314-sur-laction-de-groupe-12775/zoom-sur-laction-de-groupe-en-matiere-de-consommation-27936.html

HARY Estelle, « Dark patterns : quelle grille de lecture pour les réguler ? », 2 septembre 2019, disponible sur https://linc.cnil.fr/dark-patterns-quelle-grille-de-lecture-pour-les-reguler

LINC, « Les données personnelles : un levier pour différents régulateurs », 5 juillet 2019, disponible sur https://linc.cnil.fr/en/node/114185

Ministère de l'économie et des finances, Labo Société numérique, « Lyon, Nantes et la Rochelle jettent les bases du self data territorial », *labo.societenumerique.gouv.fr*, 18 juillet 2019, disponible sur https://labo.societenumerique.gouv.fr/2019/07/18/lyon-nantes-et-la-rochelle-jettent-les-bases-du-self-data-territorial/

Ministère de l'Économie, des finances et de la relance, « AOP-AOC, IGP, AB … : les labels de qualité dans l'alimentation », 10 décembre 2021, disponible sur https://www.economie.gouv.fr/particuliers/aop-aoc-igp-stg-labels-certification-alimentation

Ministère de l'Économie, des finances et de la relance, « Comprendre l'action de groupe en 5 questions », *Bercy Infos*, 28 juin 2017, disponible sur https://www.economie.gouv.fr/particuliers/action-de-groupe

Ministère de l'Économie, des finances et de la relance, « Denrées alimentaires : quelles sont les règles d'étiquetage ? », 3 juin 2021, disponible sur https://www.economie.gouv.fr/particuliers/denrees-alimentaires-regles-etiquetage

Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, « Qu'est-ce que la silver économie ou économie des seniors ? », *Bercy Infos*, 14 novembre 2017, disponible sur https://www.economie.gouv.fr/entreprises/silver-economie-definition

Ministère de l'intérieur, « Alicem, la première solution d'identité numérique régalienne sécurisée », *L'actu du ministère*, 12 février 2020, disponible sur https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee

Ministère de la Transition économique et de la Cohésion des territoires, Ministère de la transition énergétique, « L'Union européenne, droits des personnes handicapées et accessibilité », *ecologie.gouv.fr*, 21 mai 2021, disponible sur https://www.ecologie.gouv.fr/lunion-europeenne-droits-des-personnes-handicapees-et-accessibilite

B. UNION EUROPÉENNE

A. Décisions

Commission européenne, Décision d'adéquation (UE) 2016/1250 de la Commission européenne du 12 juillet 2016.

B. Communications, positions et recommandations

Commission des communautés européennes, *Communication interprétative de la Commission concernant l'emploi des langues pour la commercialisation des denrées alimentaires suite à l'arrêt « Peeters »*, 10 novembre 1993, COM (92) 532 final.

Commission européenne, *Multilinguisme : un atout pour l'Europe et un engagement* commun, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 18 septembre 2008, {SEC(2008) 2443} {SEC(2008) 2444} {SEC(2008) 2445}.

Commission européenne, *Une approche globale de la protection des données à caractère personnel dans l'Union européenne*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Bruxelles, 4 novembre 2010, COM(2010) 609 final.

Commission européenne, *Un agenda du consommateur européen – Favoriser la confiance et la croissance,* Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Bruxelles, 22 mai 2012, COM(2012) 225 final.

Commission européenne, *Une meilleure protection et de nouvelles perspectives – Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018,* Communication de la Commission au Parlement européen et au Conseil, Bruxelles, 24 janvier 2018, COM(2018) 43 final.

Commission européenne, *Les règles en matière de protection des données comme instrument pour créer un climat de confiance dans l'UE et au-delà – bilan »*, Communication de la Commission au Parlement européen et au Conseil, Bruxelles, 24 juillet 2019, COM(2019) 374 final.

Commission européenne, *Une stratégie européenne pour les données*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Bruxelles, 19 février 2020, COM(2020) 66 final.

Commission européenne, *Façonner l'avenir numérique de l'Europe*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Bruxelles, 19 février 2020, COM(2020) 67 final.

Commission européenne, *Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données*, Communication de la Commission, 17 avril 2020, 2020/C-124.

Commission européenne, *La protection des données : un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique – deux années d'application du règlement général sur la protection des données,* Communication de la Commission au Parlement européen et au Conseil, Bruxelles, 24 juin 2020, COM(2020) 264 final.

Commission européenne, *Farm to Fork Strategy. For a fair, healthy and environmentally-friendly food system*, Communication de la Commission au Parlement européen et au Conseil, Bruxelles, 20 mai 2020, COM(2020) 381 final. .

Commission européenne, Haut représentant de l'Union pour les affaires étrangères, « The EU's Cybersecurity Strategy for the Digital Decade », *Joint Communication to the European Parliament and the Council*, Bruxelles, 16 décembre 2020, JOIN(2020) 18 final.

Commission européenne, *Lettre ouverte destinée à Mr Aleid Wofsen*, Bruxelles, 06/03/2020, (2020)1417369.

Commission européenne, « Speech by Executive Vice-President Margrethe Vestager : Building trust in technology », 29 octobre 2020, disponible sur https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/speech-executive-vice-president-margrethe-vestager-building-trust-technology_en.

Commission européenne, *Livre blanc sur l'intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance*, Bruxelles, 19 février 2020, COM(2020) 65 final.

Conseil de l'Union européenne, Recommandation du Conseil relative à une approche globale de l'enseignement et de l'apprentissage des langues, 22 mai 2019, 2019/C 189/03.

Conseil de l'Union européenne, *Façonner l'avenir numérique de l'Europe*, Conclusions du Conseil, Bruxelles, 9 juin 2020, 8711/20.

Conseil européen, *Position of the Council at first reading with a view to the adoption of a regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Bruxelles, 6 avril 2016, 5419/16.

Haut représentant de l'Union pour les affaires étrangères, « The EU's Cybersecurity Strategy for the Digital Decade », *Joint Communication to the European Parliament and the Council*, Bruxelles, 16 décembre 2020, JOIN(2020) 18 final.

C. Débats, amendements et résolutions

Conseil de l'Union européenne, *Débat d'orientation sur le mécanisme de guichet unique*, Bruxelles, 26 mai 2014, Dossier interinstitutionnel 2012/0011(COD), 10139/14.

Parlement européen, *Resolution on the Constitution of the European Union*, A3-0064/94, publié au Journal Officiel des Communautés européennes le 28 février 1994.

Parlement européen , Commission LIBE, *Committee report tabled for plenary, 1st reading/single reading*, A7-0402/2013.

Parlement européen, Commission LIBE, *Draft report on the Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data*, 2009-2014, PE506.045

Parlement européen, *European Parliament legislative resolution of 12 March 2014 on 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 the free movement of such data (General Data Protection Regulation*), Procédure legislative ordinaire : première lecture, Strasbourg, 12 mars 2014, COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

Parlement européen, 20 mai 2021, *Résolution sur l'arrêt rendu par la Cour de justice de l'Union européenne le 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems (« arrêt Schrems II »)*, 2020/2789(RSP).

Parlement européen, *Résolution législative du Parlement européen du 12 mars 2014 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)(COM(2012)0011 – C7-0025/2012 – 2012/011(COD)*, P7-TA(2014)0212.

Parlement européen, *Résolution du Parlement européen du 25 octobre 2018 sur l'exploitation des données des utilisateurs de Facebook par Cambridge Analytica et les conséquences en matière de protection des données* (2018/2855(RSP)).

Parlement européen, *Résolution du Parlement européen contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle,* Bruxelles, 20 octobre 2020.

Parlement européen, Protection of individuals with regard to the processing of personal data – processing of personal data for the purpose of crime prevention (debate), Strasbourg, 11 mars 2014, CRE 11/03/2014 – 13, 2012/0011 (COD).

Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures, « Amendements (2) 602-885 », *Projet de rapport 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),* 4 mars 2013, COM(2012)0011 – C7-0025/2012.

TICĂU Silvia-Andriana, Bernd LANGE, Amendement 1114 proposé à l'article 11 paragraphe 2 du RGPD.

Commission des libertés civiles, de la justice et des affaires intérieures, *Committee report tabled for plenary, 1st reading/single reading*, A7-0402/2013.

D. Études et rapports

BEYER-KATZENBERGER Malte, « What if the next generation of the internet was an 'Internet of Me'? », *Futurium*, Commission européenne, 2 décembre 2016, disponible sur https://ec.europa.eu/futurium/en/blog/what-if-next-generation-internet-was-internet-me.html.

Commission des Communautés européennes, *Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)*, Rapport de la Commission, Bruxelles, 15 mai 2003, COM(2003) 265 final.

Commission européenne, *Data Protection Certification Mechanisms. Study on Article 42 and 43 of the Regulation (EU) 2016/679*, Final Report, février 2019.

CRÉMER Jacques *et al.*, *Competition policy for the digital era*, Commission européenne, 2019.

Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle, *Lignes directrices en matière d'éthique pour une IA digne de confiance,* Commission européenne, 8 avril 2019.

Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle, *Policy and Investment Recommendations for Trustworthy AI*, Commission européenne, 26 juin 2019.

ENISA, *Privacy and Security in Personal Data Clouds*, Final Report, novembre 2016.

RODRIGUES Rowena *et al., EU Privacy seals project: Inventory and analysis of privacy certification schemes. Final Report*, Luxembourg, 2013, Publications Office of the European Union.

CEDH, *Guide sur l'article 8 de la Convention européenne des droits de l'homme. Droit au respect de la vie privée et familiale, du domicile et de la correspondance,* mis à jour le 21 août 2020.

Parlement européen, *Rapport sur l'intelligence artificielle à l'ère du numérique*, 5 avril 2022, 2020/2266(INI).

E. Communiqués de presse

Commission européenne, « La Commission propose des mesures pour stimuler le partage des données et soutenir les espaces européens de données », *Communiqué de presse*, Bruxelles, 25 novembre 2020.

Commission européenne, « Une Europe adaptée à l'ère du numérique : La Commission propose de nouvelles règles et actions en faveur de l'excellence et de la confiance dans l'intelligence artificielle », *Communiqué de presse*, Bruxelles, 21 avril 2021, disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_1682.

Commission européenne, « Pratiques anticoncurrentielles : la Commission inflige à Google une amende de 2,42 milliards d'euros pour abus de position dominante sur le marché des moteurs de recherche en favorisant son propre service de comparaison de prix », *Communiqué de presse*, Bruxelles, 27 juin 2017, disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/IP_17_1784.

Parlement européen, *Online advertising : the impact of targeted advertising on advertisers, market access and consumer choice*, Policy Department for Economic, Scientific and Quality of Life Policies, juin 2021.

Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures, *Projet de rapport 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)*, 16 janvier 2013, COM(2012)0011 – C7-0025/2012.

Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures, « Amendements (2) 602-885 », *Projet de rapport 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))*, 4 mars 2013, COM(2012)0011 – C7-0025/2012.

Parlement européen, *Rapport sur la proposition 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 »)*, 20 octobre 2017, Commission LIBE, 2017/003COD.

Parlement européen, *Rapport sur une approche globale de la protection des données à caractère personnel dans l'Union européenne*, Commission des libertés civiles, de la justice et des affaires intérieures, 22 juin 2011, A7-0244/2011.

Parlement européen, *Rapport sur la proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques)*, Strasbourg, 30 novembre 2021.

Conseil de l'Union européenne, « Confidentiality of electronic communications: Council agrees its position on ePrivacy rules », *Communiqué de presse*, 10 février 2021.

Conseil de l'Union européenne, « Confidentialité des communications électroniques : le Conseil arrête sa position sur des règles en matière de vie privée et de communications électroniques », *Communiqué de presse*, 10 février 2021.

ENISA, « Cloud Certification Scheme : Building Trusted Cloud Services Across Europe », Communiqué de presse, *Enisa.europa.eu*, 22 décembre 2020, disponible sur https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme.

F. Statistiques

Commission européenne, « Attitudes on Data Protection and Electronic Identity in the European Union », *Rapport*, Special Eurobarometer 359, juin 2011.

Commission européenne, *Special Eurobarometer 431 : Data Protection*, 2015.

Commission européenne, *Digital Rights and Principles*, Special Eurobarometer 518, septembre-octobre 2021.

Eurostat, « Structure et vieillissement de la population », ec.europa.eu, 21 décembre 2020, disponible sur https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Structure_et_vieillissement_de_la_population&oldid=510188.

C. CONSEIL DE L'EUROPE

ZUIDERVEEN BORGESIUS Frederik, *Discrimination, Artificial Intelligence and Algorithmic Decision-Making*, Strasbourg, Conseil de l'Europe, 2018.

Conseil de l'Europe, *Responsabilité et IA*, Strasbourg, Conseil de l'Europe, septembre 2019, rapporté par Karen Yeung.

Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *L'autodétermination informationnelle à l'ère de l'Internet. Éléments de réflexion sur la Convention n°108 destinés au travail futur du Comité consultatif,* Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, 2004, T-PD 04 final.

Conseil de l'Europe, **Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère** personnel (Convention 108), *Lignes directrices sur la reconnaissance faciale*, 28 janvier 2021.

Conseil de l'Europe, « Intelligence Artificielle et Protection des données », *Lignes directrices sur l'intelligence artificielle et la protection des données,* adoptées par le Comité de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108), 25 janvier 2019.

Comité *ad hoc* sur l'intelligence artificielle (CAHAI), *Vers une régulation des systèmes d'IA. Perspectives internationales sur l'élaboration d'un cadre juridique fondé sur les normes du Conseil de l'Europe dans le domaine des droits de l'homme, de la démocratie et de l'État de droit*, Étude du Conseil de l'Europe, décembre 2020, DGI (2020) 16.

Conseil de l'Europe, *Discrimination, intelligence artificielle, et décisions algorithmiques,* étude du Professeur Frederik ZUIDERVEEN BORGESIUS, Strasbourg, Publication de la Direction générale de la Démocratie, Conseil de l'Europe, 2018, 99 pages .

D. ORGANISATION DES NATIONS UNIES (ONU)

Rapporteur spécial sur le droit à la vie privée, *Lettre adressée à l'Inde concernant le projet de loi sur la protection des données*, 12 novembre 2018.

Rapporteur spécial sur le droit à la vie privée, *Projet de lignes directrices concernant la confidentialité des données dans le cadre de l'intelligence artificiel*, Appel à contribution, terminé le 2 novembre 2020.

OMS, *Déclaration sur la promotion des droits des patients en Europe*, Amsterdam, 1994.

OMS, « Prise en charge de l'abus de substances psychoactives », disponible sur https://www.who.int/substance_abuse/terminology/definition1/fr/.

UNICEF, « La Convention relative aux droits de l'enfant – Version pour les enfants », *unicef.org*, disponible sur https://www.unicef.org/fr/convention-droits-enfant/convention-droits-version-enfants.

UNICEF et al., *Adapting the Child-Friendly Example of the Convention on the Rights of the Child (Convention) with and for Children in your Context*, p. 4, disponible sur https://www.childrightsconnect.org/wp-content/uploads/2019/08/cf_crc_translation_guide_final.pdf.

Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), **Commission mondiale d'éthique des connaissances scientifiques et des technologies (COMEST)**, *Étude préliminaire sur l'éthique de l'intelligence artificielle*, Paris, 26 février 2019, SHS/COMEST/EXTWG-ETHICS-AI/2019/1.

DUTTON William H. *et al.*, *Freedom of Connection – Freedom of Expression. The Changing Legal and Regulatory Ecology Shaping the Internet*, Paris, Unesco, 2011, 105 pages.

E. CONFERENCE DES COMMISSAIRES A LA PROTECTION DES DONNEES ET A LA VIE PRIVEE (ICDPPC)

Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), *Proposed Resolution on Improving the Communication of Data Protection and Privacy Information Practices*, 25th International Conference of Data Protection & Privacy Commissioners, Sydney, 12 septembre 2003.

Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), *Déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence*

artificielle, 40e conférence internationale des commissaires à la protection des données et de la vie privée, Bruxelles, 23 octobre 2018.

Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), *Résolution sur des normes internationales de vie privée*, Madrid, 4-6 novembre 2009, 31e Conférence.

Conférence des commissaires à la protection des données et à la vie privée (ICDPPC), *Resolution on improving the communication of data protection and privacy information practices*, Sydney, 12 septembre 2003.

F. FORUM ÉCONOMIQUE MONDIAL (WORLD ECONOMIC FORUM)

Word Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage*, Industry Agenda, Février 2013, disponible sur http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

G. ÉTRANGERS

1. Allemagne

Bundeskartellamt, « Bundeskartellamt prohibits Facebook from combining user data from different sources », *Bundeskartellamt.de*, 7 février 2019, disponible sur https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html

2. Belgique

APD, « Cookies et autres traceurs », disponible sur https://www.autoriteprotectiondonnees.be/citoyen/themes/internet/cookies

APD, « Prise de température dans le cadre de la lutte contre le Covid-19 », mis à jour le 4 février 2021, disponible sur https://www.autoriteprotectiondonnees.be/citoyen/themes/covid-19/prise-de-temperature

APD, « L'APD remet de l'ordre dans l'industrie de la publicité en ligne : IAB Europe est tenue responsable d'un mécanisme qui viole le RGPD », 2 février 2022, disponible sur https://www.autoriteprotectiondonnees.be/professionnel/iab-europe-est-tenue-responsable-d-un-mecanisme-qui-viole-le-rgpd

3. Canada

Commission de l'éthique en science et en technologie, « Cambridge Analytica : la citoyenneté numérique et la démocratie mises à l'épreuve », *ethique.gouv.qc.ca*, 23 mars 2018, disponible sur https://www.ethique.gouv.qc.ca/fr/actualites/ethique-hebdo/eh-23-mars-2018/

4. États-Unis

FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers*, 2012.

FTC, *Privacy Online: A report to Congress*, 1998, available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf

FTC, « FTC Sues Facebook for Illegal Monopolization », 9 décembre 2020, disponible sur https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization

WARNER R. Mark, « Lawmaker Announce Additional Support for Bipartisan, Bicameral Legislation to Ban Manipulative 'Dark Patterns' », *Communiqué de presse*, 15 juin 2022, disponible sur https://www.warner.senate.gov/public/index.cfm/2022/6/lawmakers-announce-additional-support-for-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns

US Department of Health, Education & Welfare, « Records Computers and the Rights of Citizens », *Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, 1973

MURIS Timothy J., *Hearing before the Comitee on Commerce, Science and Transportation, United States Senate,* Second Session 25 avril 20021, S. 2201, Online Personal Privacy

U.S. House of Representatives, *Investigation of Competition in Digital Markets*, Majority Staff Report and Recommendation, Subcommittee on Antitrust, Commercial and Administrative Law of the Committee of the Judiciary, 2020.

MURIS Timothy J., *Hearing before the Comitee on Commerce, Science and Transportation, United States Senate,* Second Session 25 avril 20021, S. 2201, Online Personal Privacy Act

5. Italie

GPDP, « Tik Tok, a rischio la privacy dei minori: il Garante avvia il procedimento contro il social network », *gpdp.it*, 22 décembre 2020, disponible sur https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9508923

GPDP, « Tik Tok : Italian SA warns against « personalised » ads based on legitimate interest », 12 juillet 2022, disponible sur https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9788342#english

6. Luxembourg

CNPD, « Agrément des organismes de certification », disponible sur https://cnpd.public.lu/fr/professionnels/Certification/agrement.html

CNPD, « Le schéma de certification « GDPR CARPA » », *cnpd.public.lu*, disponible sur https://cnpd.public.lu/fr/professionnels/Certification/gdpr-carpa.html

CNPD, *GDPR-Certified Assurance Report Based Processing Activities*, Document to the attention of organizations that want to obtain certification of processing activities under the GDPR-CARPA certification mechanism, v. 1.0, 29 p.

7. Pays-bas

AP, « Websites moeten toegankelijk blijven bij weigeren tracking cookies », 9 mars 2019, disponible sur https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies

AP, « AP: veel websites vragen op onjuiste wijze toestemming voor plaatsen tracking cookies », 10 décembre 2019, disponible sur https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op-onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies

AP, « Company fined for processing employees' fingerprint data", 30 avril 2020, disponible sur https://autoriteitpersoonsgegevens.nl/en/news/company-fined-processing-employees%E2%80%99-fingerprint-data

AP, « Hoe legt de AP de juridische normen rond cookiewalls uit? », disponible sur https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_ap_cookiewalls.pdf

8. Roumanie

ANSPDCP, 17 octobre 2019, « The 4th Fine for the Application of GDPR », disponible sur le site https://www.dataprotection.ro/index.jsp?page=A_patra_amenda&lang=en

ANSPDCP, « Another sanction for the violation of GDPR », *dataprotection.ro*, 22/08/2020, disponible sur https://www.dataprotection.ro/index.jsp?page=Alta_sanctiune_RGPD&lang=en

9. Royaume-Uni

ICO, « What are the rules on cookies and similar technologies », disponible sur https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/

ICO, « When is consent appropriate? », *Consent*, disponible sur https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/

ICO, « International transfers after the UK exit from the EU Implementation Period », *ICO.org.uk*, disponible sur. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/ (consulté en septembre 2021).

ICO, *Democracy disrupted? Personal information and political influence*, 11 janvier 2018

VI. LÉGISLATIONS

A. NATIONALES

A. Législation et codes

Déclaration des droits de l'homme et du citoyen, 1789

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Journal Officiel de la République Française, Loi et décrets, n°006, 7 janvier 1978.

Loi n°94-665, 4 août 1994 relative à l'emploi de la langue française, dite loi Toubon, *JO* 5 août 1994

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JO °143 du 22 juin 2004.

Loi n°2016-1321 du 7 octobre 2016 (Loi pour une République Numérique)

Loi n°2016-1546 du 18 novembre 2016 de modernisation de la justice du XXIe siècle

Loi n°2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

Loi n°2020-699 du 10 juin 2020 relative à la transparence de l'information sur les produits agricoles et alimentaires

Loi n°2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

Ministère de la santé, de la famille et des personnes handicapées, Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, Journal officiel du 17 mars 2004, n°65, pp. 5206-5209.

Code de la consommation

Code pénal

Code des postes et des communications électroniques, tel que modifié par l'article 115 de la loi n°2014-344 du 17 mars 2014

B. Propositions législatives

Assemblée Nationale, *Proposition de loi pour un nouveau de régime de l'action de groupe*, Enregistré à la Présidence de l'Assemblée nationale le 15 septembre 2020, n°3329.

Assemblée nationale, *Proposition de loi relative à une société plus inclusive pour les personnes en situation de handicap*, n°798, 21 mars 2018, renvoyée à la Commission des affaires sociales.

Sénat, *Proposition de loi visant à garantir le libre choix du consommateur dans le cyberespace*, proposée par la sénatrice Sophie Primas et plusieurs de ses collègues, Texte n°48(2019-2020), déposé au Sénat le 10 octobre 2019.

Sénat, *Proposition de règlement relative aux marches contestables et équitables dans le secteur numérique (législation sur les marchés numériques) dite Digital Markets Act – Examen du rapport de la proposition de résolution européenne et de l'avis politique de Mmes Florence Blatrix Contat et Catherine Morin-Desailly*, Extrait du compte rendu de la réunion de la commission des affaires européennes du 7 octobre 2021, disponible sur https://www.senat.fr/ue/pac/EUR000006741.html

B. DE L'UNION EUROPÉENNE

A. Traités

Charte des droits fondamentaux de l'Union européenne.

Traité sur le fonctionnement de l'Union européenne (TFUE).

Traité sur l'Union européenne (TUE).

B. Règlements

Règlement (CE) 1371/2007 du Parlement européen et du Conseil du 23 octobre 2007 sur les droits et obligations des voyageurs ferroviaires

Règlement (CE) 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I)

Règlement (UE) 1177/2010 du Parlement européen et du Conseil du 24 novembre 2010 concernant les droits des passagers voyageant par mer ou par voie de navigation intérieure et modifiant le règlement (CE) n°2006/2004

Règlement (UE) 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale

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) (RGPD).

Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n°45/2001 et la décision n°1247/2002/CE.

Règlement (UE) 1029/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité)

C. Directives

Directive 79/112/CEE du Conseil, du 18 décembre 1978, relative au rapprochement des législations des États membres concernant l'étiquetage et la présentation des denrées alimentaires destinées au consommateur final ainsi que la publicité faite à leur égard

Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs

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 97/4/CE du Parlement européen et du Conseil, du 27 janvier 1997, modifiant la directive 79/112, *JO L. 43*

Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société d'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »)

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 (directive vie privée et communications électroniques).

Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/550/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) no 2006/2004 du Parlement européen et du Conseil (« directive sur les pratiques commerciales déloyales »)

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

Directive (UE) 2016/280 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.

Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

Directive (UE) 2016/943 du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, 8 juin 2016.

Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE.

D. Proposition législatives

Commission européenne, 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), Bruxelles, 25 janvier 2012, COM(2012) 11 final.

Commission européenne, *Impact Assessment*, Commission staff Working Paper Accompanying the document 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) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC/2012/0072 final.

Commission européenne, 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 »), COM/2017/010 final – 2017/03(COD).

Commission européenne, *Proposition de Directive du Parlement européen et du Conseil relative aux actions représentatives dans le domaine de la protection des intérêts collectifs des consommateurs et abrogeant la directive 2009/22/*CE, Bruxelles, 11 avril 2018, COM(2018) 184 final.

Commission européenne, Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, COM/2020/825 final.

Commission européenne, Proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), COM(2020) 842 final.

Commission européenne, Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM/2021/206 final.

Conseil de l'Union européenne, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications – Mandate for negiciations with EP*, Bruxelles, 10 février 2021, 2017/0003(COD).

Conseil de l'Union européenne, *Proposition de Règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation*

sur les marchés numériques) – Lettre du président du COREPER à la présidente de la Commission IMCO, Bruxelles, 11 mai 2022, 2020/0374 (COD).

E. INTERNATIONALES

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, version amendée par les Protocole n°11 et n°14, Rome, 1950.
Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (« Convention 108 »), Strasbourg, 28 janvier 1981.
Convention sur les droits de l'homme et de la biomédecine, Oviedo 1997.

Organisation des Nations unies, *Déclaration universelle des droits de l'Homme*, Paris, 10 décembre 1946, résolution 217 A(III).
Organisation des Nations unies, *Pacte international relatif aux droits civils et politiques*, 16 décembre 1966, adopté et ouvert à la signature, à la ratification et à l'adhésion par l'Assemblée générale dans sa résolution 2200A(XXI).
Convention des Nations unies relatives aux droits des personnes handicapées.
OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, 23 septembre 1980.
APEC Privacy Framework.

F. <u>Étrangères</u>

1. Australie

Australian Privacy Act.

2. États-Unis

Californian Consumer Privacy Act.
California Privacy Rights Act.
Colorado Privacy Act.
Senate of the United States, S.1084, *A Bill to Prohibit the Usage of Exploitative and Deceptive Practices by Large Online Operators and to Promote Consumer Welfare in the Use of*

Behavioural Research by Such Providers, introduite devant le Sénat le 9 avril 2019, 116e Congrès, 1e session, disponible sur https://www.congress.gov/bill/116th-congress/senate-bill/1084/text.

Children's Online Privacy Protection Rule (COPPA).

3. Brésil

Lei Geral de Proteção de Dados (LGPD).

4. Thaïlande

Personal Data Protection Act (PDPA).

VII. JURISPRUDENCE

A. UNION EUROPEENNE

A. Tribunal de la fonction publique de l'Union européenne

Tribunal de la fonction publique de l'Union européenne, 19 juillet 2016, Oprena / Commission européenne, F-67/15.

B. Arrêts de grande chambre de la CJCE/CJUE

CJCE, Gde Ch., 5 octobre 2004, *Pfieiffer e.a.*, C-397//01 à C-403/01.

CJCE, Gde Ch., 16 décembre 2008, *Satamedia*, C-73/07.

CJUE, Gde ch., 9 novembre 2010, *Volker und Markys Schecke et Eifert*, C-92/09 et C-92/03

CJUE, Gde ch., 8 avril 2014, *Digital Rights Ireland Ltd*, C-293/12

CJUE, Gde Ch.,13 mai 2014, *Google Spain*, C-131/12.

CJUE, Gde ch., 6 octobre 2015, *Maximilian Schrems c. Data Protection Commissionner*, C-362/14

CJUE, Gde Ch., 15 février 2016, *J. N. c. Staatssecretaris van Veiligheid en Justitie*, C-601/15.

CJUE, Gde Ch. 21 décembre 2016, *Tele2 Sverige AB*, C-203/15.

CJUE, Gde Ch., 16 décembre 2008, *Satamedia*, C-73/07.

CJUE, Gde ch ., 1e octobre 2019, *Planet49 GmbH*, C-673/17

CJUE, Gde Ch.,16 juillet 2020, *Facebook Ireland et Schrems*, C-311/18

CJUE, Gde Ch., 15 juin 2021, *Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA c. Gegevensbeschermingsautoriteit*, C-645/19

CJUE, Gde Ch., 22 juin 2021, *Randstad Italia SpA*, C-439/19

C. Arrêts de la CJCE/CJUE

CJCE, 5e ch., 18 juin 1991, *ASBL Piageme et BVBA* Peeters, C-369/89

CJCE, 5e ch., 12 octobre 1995, *Groupement des producteurs, importateurs et agents généraux d'eaux minérales étrangères, VZW (Piageme) e.a.,* C-85/94

CJCE, 12 septembre 2000, *Geoffroy et Casino France SNC*, C-366/98

CJCE, 27 juin 2000, *Océano Grupo Editorial SA*, C-240/98 à C-244/98

CJCE, 5e ch., 24 janvier 2002, *Commission / Italie*, C-372/99

CJCE, 6e ch., 1e octobre 2002, *Karl Heinz Henkel*, C-167/00

CJUE, 15 novembre 2008, *Satakunnan Markkinapörssi et Satamedia*, C-73/07

CJUE, 3e ch., 24 novembre 2011, *ASNEF et FECEMD c. Administración del Estado,* C-468/10 et C-469/10.

CJUE, 1e ch., 26 avril 2012, Nemzeti Fogyasztóvédelmi Hatóság, C-472/10

CJUE, 1e ch., 22 novembre 2012, *Westbahn Management GmH*, C-136/11

CJUE, 3e ch., 7 novembre 2013, *IPI c. Geoffrey Englebert e.a.*, C-473/12.

CJUE, 17 juillet 2014, *YS*, C-141/12 et C-372/12.

CJUE, 3e ch., 1e octobre 2015, *Smaranda Bara e.a.*, C-201/14

CJUE, 3e ch., 28 juillet 2016, *Verein für Konsumenteninformation c. Amazon EU SARL*, C-191/15

CJUE, 2e ch., 19 octobre 2016, *Breyer*, C-582/14

CJUE, 2e ch., 20 décembre 2017, *Peter Nowak c. Data Protection Commissioner*, C-434/16

CJUE, 5e ch., 7 novembre 2019, *Kanyeba*, C-349/18 à C-351/18

CJUE, 3e ch., 11 décembre 2019, *TK c. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18

CJUE, 1e ch., 9 juillet 2020, *VKI c. Volkswagen*, C-343/19.

CJUE, 2e ch., 11 novembre 2020, *Orange Romãnia*, C-61/19.

CJUE, 3e ch, 17 décembre 2020, *A.M. contre E.M.*, n°667/19

CJUE, 5e ch., 17 mars 2021, *Academia de Studii Economice din Bucureşti*, C-585/19

CJUE, 3e ch., 20 mai 2021, *CNP*, C-913/19

CJUE, 10 juin 2021, affaires jointes C776-19 à C-782/19.

CJUE, 5e ch., 17 juin 2021, *MICM*, C-597/19

CJUE, 1e ch., 15 juillet 2021, *DG, EH*, C-152/10 et C-218/20

CJUE, 4e ch., 2 septembre 2021, *Irish Ferries Ltd*, C-570/19

D. Conclusions de l'avocat général auprès de la CJCE/CJUE

Conclusions de l'avocat général Mme Eleanor SHARPSTON, *YS et autres*, présentées le 12 décembre 2013, C-41/12 et C-372/12.

Conclusions de l'avocat général M. Pedro RUZ VILLALON, *Smaranda Bara e.a.*, présentées le 9 juillet 2015, C-201/14.

Conclusions de l'avocat général Mme Julianne KOKOTT, *Peter Nowak c. Data Protection Officer*, présentées le 20 juillet 2017, C-434/16.

Conclusions de l'avocat général M. Marciej SZPUNAR, *Planet 49 GmbH*, présentées le 21 mars 2019, C-673/17.

Conclusions de l'avocat général M. Henrik SAUGMANDSGAARD ØE, *Data Protection Commissionner c. Facebook Ireland Limited, Maximilian Schrems*., présentées le 19 décembre 2019, C-311/18, §120.

Conclusion de l'avocat général M. Jean Richard DE LA TOUR, *Facebook Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V,* présentées le 2 décembre 2021, C-319/20.

E. Affaires pendantes

CJUE, Demande de décision préjudicielle, *Facebook Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V* ,déposée le 15 juillet 2020, C-319/20.

B. COUR EUROPEENNE DES DROITS DE L'HOMME

A. Arrêts de grande chambre

CEDH, Gde ch., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, 30562/04 et 30566/04

CEDH, Gde ch., 27 juin 2017, *Satakunnan Markkinapörssi et Satamedia Oy c. Finlande,* req. n°913/13.

B. Arrêts

CEDH, 16 décembre 1992, *Niemetz c. Allemagne*, req. n° 13710/88

CEDH, 19 février 1997, *Laskey et autres c. Royaume-Uni,* req. 21627/93 ; 21628/93 ; 21974/93.

CEDH, 25 juin 1997, *Halford c. Royaume-Uni*, req. n°20605/92.

CEDH, 16 février 2000, *Amann c. Suisse*, req. n°27798/95

CEDH, 4e section, 29 avril 2002, *Pretty c. Royaume-Uni*, req. 2346/02.

CEDH, 1e section, 17 février 2005, *K. A. et A. D. c. Belgique,* req. 42758/98 et 45558/99

C. NATIONALE

1. Conseil constitutionnel

Conseil constitutionnel, DC, 25 juillet 1989, n°89-257.

Conseil constitutionnel, DC, 13 mars 2014, n°2015-690

Conseil constitutionnel, Décision n°2021-976/977 QPC du 25 février 2022.

Conseil constitutionnel, Décision n°2022-987 QPC du 8 avril 2022

2. Conseil d'État

CE, 10e et 9e sous-sections réunies, 11 mars 2015, n° 369624.

CE, 10e ch., 30 décembre 2015, *Association Juricom et associés*, n°376845

CE, 30 septembre 2019, *La Quadrature du Net*, n°433069.

CE, 19 juin 2020, n°420810.

CE, 10e et 9e chambres réunies, 19 juin 2020, n°430810, *Société Google LLC*.

CE, 10e et 9e ch. réunies, 19 juin 2020, *Association des agences-conseil et a.*, n°434684.

LALLET Alexandre, Conclusions, CE 10e et 9e ch. Réunies, *Association des agences conseil en communication et autres*, n°434684.

CE, ordonnance, 26 juin 2020, *Caméra thermiques à Lisses*, n°441065.

CE, ord. 13 octobre 2020, *Association Le Conseil national du logiciel libre et autres,* n°444937.

CE, 10e et 9e chambres réunies, 4 novembre 2020, n°432656.

CE, 10e et 9e ch. réunies, 10 décembre 2020, n°429571.

CE, juge des référés, 4 mars 2021, *Google LLC et Google Ireland Limited*, n°449212.

3. Cour de cassation

Cass. Soc., 22 février 2000, n°97-44.339.

Cass. Civ. 1e, 14 novembre 2000, n°99-10.778

Cass. Civ. 1e, 17 mars 2016, *C. c. Société Boulangerie Pre*, n°15-14.072

Cass. Civ. 1e, 9 octobre 2001, n°00-14.

Cass. Civ. 2, 10 mars 2004, n°02-16.354, Publié au bulletin.

Cass. Civ. 1e, 17 mars 2016, *C. c. Société Boulangerie Pre*, n°15-14.072

Cass. Soc., 28 novembre 2018, n°1704.

4. Cours d'appel

Cour d'appel de Paris, pôle 5, ch. 2, 23 mars 2012.
CA Montpellier, 23 mars 2017, n°14/01306

5. Tribunaux de Grande instance

TGI Paris, 7 août 2017, *UFC Que Choisir c. Twitter Inc et Twitter International Company*, n° RG 14/07300.
TGI Paris, 12 février 2019, Union Fédérale des consommateurs – Que choisir c. Société Google Inc., 14/07224.
TGI Paris, 17 septembre 2019, n°16/01008.

D. ÉTRANGERE

1. Autriche

BVwG, 25 novembre 2019, W211 2210458-1/10.
OGH (Cour suprême autrichienne), 15 novembre 2018, 9 Ob 38/19g.

2. Espagne

Tribunal Supremo, Sala de lo Civil, 12/01/2001, Jose Manuel Martinez-Pereda Rodriguez, n°3688/1995.

3. États-Unis

United States District Court, Central District of California, *Kellie Black v. Snap Inc. et al.*, Class Action Complaint for Violation of the Federal Securities Laws, Case 2:21-cv-08892.
United States District Court, **Southern District Court of New-York**, *Google LLC*, Second amended Complaint, Civil Action No : 1 :21-md-03010-PKC

4. Italie

Cass Civ., Sec. I, 2 juillet 2018, *Newsletter, e-mail pubblicitarie e consenso,* 17278/2018.
Cass. Civ., 25 mai 2021, 14381/2021

5. Pays-bas

LG Rostock, 15 septembre 2020, 3 O 762/1

Rechtbank Midden-Nederland, 23/11/2020, *VoetbalTV BV et Autoriteit Persoonsgegevens*, UTR20/23/15

Raad van State, 27/07/2022, *VoetbalTV BV et Autoriteit Persoonsgegevens*, 20100045/1/43

VIII. AUTORITÉS DE CONTRÔLE, CONTROLEUR EUROPÉEN DES DONNÉES ET COMITÉ EUROPEEN DES DONNÉES

A. CONTROLEUR EUROPÉEN DES DONNÉES, COMITÉ EUROPÉEN DES DONNÉES ET GROUPE DE TRAVAIL DE L'ARTICLE 29 (G29)

EDPS, *Avis du contrôleur européen des données sur la communication de la Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée – « Une approche globale de la protection des données à caractère personnel dans l'Union européenne »*, 2011/C, 181/01.

EDPS, *Avis du contrôleur européen de la protection des données sur le parquet,* 2012.

EDPS, *Commentaire du CEPD sur la communication de la Commission – Un agenda du consommateur européen – Favoriser la confiance et la croissance,* 16 juillet 2012, disponible sur https://edps.europa.eu/data-protection/our-work/publications/comments/european-consumer-agenda-boosting-confidence-and_fr

EDPS, *Avis 9/2016 sur les systèmes de gestion des informations personnelles. Vers une plus grande autonomie des utilisateurs dans la gestion et le traitement des données à caractère personnel*, 20 octobre 2016.

EDPS, *Avis 10/2017 sur les garanties et dérogations prévues à l'article 89 du RGPD dans le cadre d'une proposition de règlement concernant les statistiques intégrées sur les exploitations agricoles*, 20 novembre 2017.

EDPS, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017

EDPS, *Avis 6/2017 du CEPD sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement « vie privée et communications électroniques »),* 24 avril 2017.

EDPS, *Avis 8/2018 du CEPD sur le paquet législatif « Une nouvelle donne pour les consommateurs »*, 5 octobre 2018,

EDPS, *Avis n°01/2021 concernant la proposition de législation sur les services numériques*, Bruxelles, 10 février 2021

EDPS, *Opinion 2/2021 on the Proposal for a Digital Markets Act*, 10 février 2021,

EDPS, **AEPD,** « 10 misunderstandings related to anonymisation », *AEDP-EDPS joint paper*, 27 avril 2021.

EDPB, *Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement*, 4 juin 2019, version 3.0

EDPB, *Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679*, adoptées le 25 mai 2018

EDPB, *Déclaration du comité européen de la protection des données sur la révision de la directive ePrivacy et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques,* 25 mai 2018.

EDPB, *Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3)*, 12 novembre 2019.

EDPB, *Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées*, version 2.0, 8 octobre 2019,

EDPB, *Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par* défaut, version 2.0, adoptées le 20 octobre 2020

EDPB, *Avis 5/2019 relatif aux interactions entre la directive « vie privée et communications électroniques » et le RGPD,* 12 mars 2019.

EDPB, *Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE,* 10 novembre 2020.

EDPB, *Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19,* Adoptées le 21 avril 2020

EDPB, *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/579*, version 1.1., adoptées le 4 mai 2020

EDPB, *Avis 14/2020 sur le projet de décision de l'autorité de contrôle compétente irlandaise concernant l'approbation des exigences relatives à l'agrément d'un organisme de certification au titre de l'article 43, paragraphe 3*, adopté le 25 mai 2020.

EDPB, *Opinion 15/2020 on the draft decision of the competent supervisory authority of Germany regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 25 mai 2020.

EDPB, *Opinion 16/2020 on the draft decision of the competent supervisory authority of the Czech Republic regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 25 mai 2020.

EDPB, *Opinion 21/2020 on the draft decision of the competent supervisory authority of the Netherlands regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 15 août 2020

EDPB, *Opinion 22/2020 on the draft decision of the competent supervisory authority of Gree regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 15 août 2020.

EDPB, *Opinion 23/2020 on the draft decision of the competent supervisory authority of Italy regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 15 août 2020

EDPB, *Opinion 26/2020 on the draft decision of the competent supervisory authority of Denmark regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43*, adopté le 7 décembre 2020.

EDPB, *Opinion 30/2020 on the draft decision of the competent supervisory authority of Austria regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 7 décembre 2020.

EDPB, *Recommandations 02/2021 sur la base juridique pour le stockage des données relatives aux cartes de crédit dans le seul but de faciliter la poursuite des transactions en ligne*, adoptées le 19 mai 2021.

EDPB, *Opinion 12/2021 on the draft decision of the competent supervisory authority of Portugal regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 23 mars 2021.

EDPB, *Opinion 13/2021 on the draft decision of the competent supervisory authority of Romania regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 23 mars 2021.

EDPB, *Opinion 19/2021 on the draft decision of the competent supervisory authority of Hungary regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 1e juin 2021.

EDPB, *Opinion 25/2021 on the draft decision of the competent supervisory authority of Lithuania regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 20 juillet 2021

EDPB, *Opinion 35/2021 on the draft decision of the competent supervisory authority of Belgium regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 30 novembre 2021.

EDPB, *Opinion 36/2021 on the draft decision of the competent supervisory authority of Norway regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 30 novembre 2021.

EDPB, *Opinion 38/2021 on the draft decision of the competent supervisory authority of Latvia regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 20 juillet 2021.

EDPB, *Guidelines 01/2022 on data subjects rights – Right of access*, Version 1.0, adoptées le 18 janvier 2022 (ouvertes à consultation publique).

EDPB, *Guidelines 3/2022 on Dark patterns in social media platform interfaces : How to recognise and avoid them »*, 14 mars 2022, version 1.0.

EDPB, *Opinion 12/2022 on the draft decision of the competent supervisory authority of France regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 4 juillet 2022.

EDPB, *Opinion 13/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditations of a certification body pursuant to Article 43.3 (GDPR)*, adopté le 4 juillet 2022.

EDPB, EDPS, *Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down hamonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 juin 2021, 5/2021

Amurabi SAS, *A user-centric perspective – Guidelines 3/2022 on Dark Patterns in social media platform interfaces*, 2 mai 2022, disponible sur https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/AmurabiUserCentricPerspectiveDarkPatternsGuidelines.pdf

Data & Marketing Association Finland, *DMA Finland opinion on EDPB draft Guidelines 3/2022 on Dark Patterns in social media platform interfaces : How to recognize and avoid*

them, 2 mai 2022, disponible sur https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/DMA%20Finland_EDPB_Dark_Patterns_02042022.pdf

Spolek pro ochranu osobních údajů, *Comments on the EDPB's draft Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*, 2 mai 2022, disponible sur https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2022_05_02%20-%20SpOOU_EFDPO%20-%20EDPB_Guidelines_dark_patterns%20%28final%20-%20en%29.pdf

ZWENNE Gerrit-Jan, « Comments. EDPB Guidelines 01/2022 on Data Subject Access, version 1.0, adopted on 18 January 2022 », soumis le 9 mars 2022, disponible sur https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/ZWENNE_COMMENTS_on_EDPB-guidelines_01_2022_DSARs_DEF.pdf

EDPB, « Austrian DPA fines controller in the medical sector », 12 août 2019, https://edpb.europa.eu/news/national-news/2019/austrian-dpa-fines-controller-medical-sector_en.

EDPB, « EDPB Stakeholder Workshop on Legitimate Interest », edpb.europa.eu, 16 novembre 2020, disponible sur https://edpb.europa.eu/news/news/2020/edpb-stakeholder-workshop-legitimate-interest_en.

EDPB, « EDPB establishes cookie banner taskforce », *News,* 27 septembre 2021, disponible sur https://edpb.europa.eu/news/news/2021/edpb-establishes-cookie-banner-taskforce_en.

Groupe de travail « Article 29 », *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware*, adoptée le 23 février 1999, WP 17.

Groupe de travail « Article 29 », *Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union*, adoptee le 17 mai 2001, WP43.

Groupe de travail « Article 29 », *Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel*, adopté le 13 septembre 2001, WP 48.

Groupe de travail « Article 29 », *Opinion on More Harmonised Information Provisions*, version proposée le 25 novembre 2004 pour discussion et adoption, WP 100.

Groupe de travail « Article 29 », *Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995,* adopté le 25 novembre 2005, WP 114.

Groupe de travail « Article 29 », *Document de travail sur la protection des données à caractère personnel de l'enfant (cas particulier de l'école)*, 18 février 2008, WP 147.

Groupe de travail « Article 29 », *Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche*, adopté le 4 avril 2008, WP 148.

Groupe de travail « Article 29 », *L'avenir de la protection de la vie privée – Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel*, 1er décembre 2009, WP 168.

Groupe de travail « Article 29 », *Avis 15/2011 sur la définition du consentement*, 13 juillet 2011, WP 187.

Groupe de travail « Article 29 », *Opinion 03/2013 on purpose limitation*, adopté le 2 avril 2013, WP 203.

Groupe de travail « Article 19 », *Document de travail 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies*, adopté le 2 octobre 2013, WP 208.

Groupe de travail « Article 29 », *Avis 06/2014 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,* adopté le 9 avril 2014, WP 217.

Groupe de travail « Article 29 », *Lignes directrices relatives au droit à la portabilité des données*, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, WP 242 rev.01.

Groupe de travail « Article 29 », *Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant*, adoptées le 13 décembre 2016, vision révisée et adoptée le 5 avril 2017, WP 244 rev.01

Groupe de travail « Article 29 », *Opinion 2/2017 on data processing at work*, adoptées le 8 juin 2017, WP 249.

Groupe de travail « Article 29 », *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, adoptées le 3 octobre 2017, Version révisée et adoptée le 6 février 2018, WP251 rev.01.

Groupe de travail « Article 29 », *Lignes directrices sur le consentement au sens du règlement 2016/679*, adoptées le 28 novembre 2017, Version révisée et adoptée le 10 avril 2018, WP 259 rev. 01.

Groupe de travail « Article 29 », *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, adoptées le 29 novembre 2017, version révisée et adoptée le 11 avril 2018, WP260 rev. 01.

B. CNIL

1. Avis et autorisations

CNIL, Délibération n°2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » (demande d'avis n°20006919).

CNIL, Délibération n° 2020-055 du 14 mai 2020 autorisant la société IMPLICITY à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude portant sur le développement et la validation d'algorithmes de prédiction des crises de décompensation cardiaque chez les patients porteurs d'implants cardiaques connectés, intitulée "HYDRO". (Rectificatif) (Demande d'autorisation n° 920054).

CNIL, Délibération n°2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » (demande d'avis n°20008032).

2. Avertissements, mises en demeures et sanctions

CNIL, Délibération de la formation restreinte n°2012-214 du 19 juillet 2012 portant avertissement à l'encontre de la société X.

CNIL, Délibération de la formation restreinte n°2013-420 du 3 janvier 2014 prononçant une sanction pécuniaire à l'encontre de la société X.

CNIL, Délibération de la formation restreinte n°2014-041 du 29 janvier 2014 prononçant une sanction pécuniaire à l'encontre de l'association X.

CNIL, Délibération de la formation restreinte n°2015-155 du 1 juin 2015 prononçant une sanction pécuniaire à l'encontre de la société X.

CNIL, Décision n°2016-007 du 26 janvier 2016 mettant en demeure les sociétés X et Y.

CNIL, Décision n° 2016-083 du 26 septembre 2016 mettant en demeure la société X.

CNIL, Délibération de la formation restreinte SAN-2017-006 du 27 avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés X et Y.

CNIL, Délibération de la formation restreinte SAN-2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société Google LLC.

CNIL, Délibération de la formation restreinte n°SAN-2019-010 du 21 novembre 2019 concernant la société Futura Internationale

CNIL, Décision MED 2019-035 du 31 décembre 2019 mettant en demeure la société ELECTRICITE DE France (EDF).

CNIL, Décision MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des solidarités et de la santé.

CNIL, Délibération de la formation restreinte SAN-2020-003 du 28 juillet 2020 concernant la société X.

CNIL, Délibération de la formation restreinte SAN-2020-008 du 18 novembre 2020 concernant la société Carrefour France.

CNIL, Délibération de la formation restreinte SAN-2020-009 du 18 novembre 2020 concernant la société Carrefour Banque.

CNIL, Délibération de la formation restreinte SAN-2020-012 du 7 décembre 2020 concernant les sociétés Google LLC et Google Ireland Limited.

CNIL, Délibération de la formation restreinte SAN-2020-013 du 7 décembre 2020 concernant la société Amazon Europe Core.

CNIL, Délibération de la formation restreinte n°SAN-2020-018 du 8 décembre 2020 concernant la société NESTOR SAS.

CNIL, Délibération de la formation restreinte SAN-2021-012 du 26 juillet 2021 concernant la société MONSANTO COMPANY.

C. AUTORITÉS DE CONTRÔLE ÉTRANGÈRES

1. Allemagne

Berliner Beauftrage für Datenschutz und Informationsfreheit (BlnBDI), 15 octobre 2021, décision 521.13874.13.

2. Belgique

APD, 17 septembre 2019, décision quant au fond 8/2019

APD, 17 décembre 2019, décision quant au fond 12/2019.

APD, 14 juillet 2020, décision quant au fond 37/2020.

APD, 20 juillet 2020, Décision quant au fond 41/2020.

APD, 28 juillet 2020, Décision quant au fond 39/2020.

APD, 9 novembre 2020, Décision quant au fond72/2020.

APD, 13 novembre 2020, Décision quant au fond 73/2020.

APD, 20 janvier 2021, Décision quant au fond 04/2021.

APD, 17 février 2021, Décision quant au fond 24/2021.

APD, 2 février 2022, Décision sur le fond 21/2022.

3. Danemark

Datatilsynet, 11 février 2020, 2018-32-0357.

Datatilsynet, 18 juin 2020, 2020-431-0085.

Datatilsynet, 9 novembre 2020, 20/01949 (PVN-2020-13).

Datatilsynet, 11 décembre 2020, 2020-31-3354.

Datatilsynet, 1e mars 2021, 2019-431-0052.

4. Espagne

AEPD, PS-00273-2019, publiée le 9 avril 2019.

AEPD, PS-00397-2019, publiée le 4 juillet 2019.

AEPD, PS-00278-2019, publiée le 3 février 2020.

AEPD, PS-00315-2019, publiée le 14 février 2020.

AEPD, PS-00187-2019, publiée le 25 février 2020.

AEPD, PS-00134-2020, publiée le 23 juillet 2020.

AEPD, PS-00479-2019, publiée le 5 août 2020.

AEPD, PS-00036-2020, publiée le 6 août 2020.

AEPD, PS-00030-2020, publiée le 9 octobre 2020.

AEPD, PS-00227-2020, publiée le 10 novembre 2020.

AEPD, PS-00070-2019, publiée le 11 décembre 2020.

AEPD, PS-00477-2019, publiée le 13 janvier 2021.

AEPD, PS-00151-2020, publiée le 14 avril 2021.

AEPD, PS-00177-2021, publiée le 10 juin 2021.

AEPD, PS-00377-2021, publiée le 18 octobre 2021.

AEPD, PS-00224-2021, publiée le 13 janvier 2022.

5. Finlande

Tietosuojavaltuutetun toimisto, 26 mai 2020, 8393/161/2019

6. Grèce

HDPA, 30 juillet 2019, 26/2019

HDPA, 30 juillet 2020, 23/2020

HDPA, 3 août 2020, 24/2020

7. Italie

GPDP, 2 juillet 2020, 9445180.

GPDP, 16 septembre 2021, 9704032.

GPDP, 16 décembre 2021, 9735672.

8. Irlande

DPC, 20 août 2021, Whatsapp Ireland Limited - IN-18-12-2

DPC, 6 octobre 2021, *Draft Decision, LB (through NOYB) v. Facebook Ireland Limited*, Draft Decision for the purposes of article 60 GDPR of the Data Protection Commission made pursuant to Section 113(2)(a) of the Data Protection Act 2018

9. Pologne

UODO, 16 octobre 2019, ZSPR.421.7.2019, disponible sur https://uodo.gov.pl/decyzje/ZSPR.421.7.2019

10.Roumanie

ANSPDCP, 4 août 2020, *Asociația de proprietari Bl. FC 5, orașul Năvodari, județul Constanța*

11.Royaume-Uni

ICO, 11 octobre 2018, IRQ0872554 (disponible sur https://ico.org.uk/media/about-the-ico/disclosure-log/2616227/irq0872554-disclosure.pdf).

ICO, 10 mai 2021, *ICO Monetary Penalty on Tested.me Ltd* (Monetary Penalty Notice).

12.Slovénie

IP, 5 novembre 2019, 0712-1/2019/2504

VIII. PRESSE

1. Tribunes

ABITEBOUL Serge, **DOWEK** Gilles, « La propriété des données personnelles est une fausse bonne idée », *LeMonde.fr*, 5 février 2018, disponible sur https://www.lemonde.fr/idees/article/2018/02/05/la-propriete-des-donnees-personnelles-est-une-fausse-bonne-idee_5252158_3232.html

AMIECH Matthieu, « Groupe Marcuse : Notre libre-arbitre est aspiré par Internet », *Marianne,* 19 août 2019, disponible sur https://www.marianne.net/agora/entretiens-debats/groupe-marcuse-notre-libre-arbitre-est-aspire-par-internet

AULAS Adrien, « Faut-il en finir avec le dogme du consentement ? », 15 avril 2019, disponible sur https://aeonlaw.eu/faut-il-en-finir-avec-le-dogme-du-consentement/

BRETON Thierry, « Tout ce qui est interdit dans l'espace public sera aussi interdit dans l'espace online », France Inter, Le Grand entretien, 14 décembre 2020, disponible sur https://www.franceinter.fr/emissions/l-invite-de-8h20-le-grand-entretien/l-invite-de-8h20-le-grand-entretien-14-decembre-2020

CHAPUS Lucie, **D'YVOIRE** Anne-Victoire, « Le développement d'une intelligence artificielle éthique est un enjeu primordial pour les entreprises », *LeMonde.fr,* 15 novembre 2019, Tribune, disponible sur https://www.lemonde.fr/idees/article/2019/11/15/le-developpement-d-une-intelligence-artificielle-ethique-est-un-enjeu-primordial-pour-les-entreprises_6019262_3232.html

COMBE Emmanuel, « Face aux GAFA, les autorités antitrust ont un rôle essentiel pour s'assurer que la compétition reste ouverte », *LeMonde.fr*, Tribune, 14 juin 2019, disponible sur https://www.lemonde.fr/idees/article/2019/06/14/emmanuel-combe-face-aux-gafa-les-autorites-antitrust-ont-un-role-essentiel-pour-s-assurer-que-la-competition-reste-ouverte_5476264_3232.html?xtmc=&xtcr=1

CRAWFORD Kate, « Artificial Intelligence's White Guy Problem », *The New York Times,* 25 juin 2016, disponible sur https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html

DALMONT Cyrille, « Données personnelles : pourquoi le RGPD est déjà dépassé », *LesEchos.fr*, 22 novembre 2019, disponible sur https://www.lesechos.fr/idees-debats/cercle/donnees-personnelles-pourquoi-le-rgpd-est-deja-depasse-1149930

DENIS Marie-Laure, « Coronavirus : « Les applications de « contact tracing » appellent à une vigilance particulière », *LeMonde.fr*, Pixels, 5 avril 2020, disponible sur https://www.lemonde.fr/pixels/article/2020/04/05/coronavirus-les-applications-de-contact-tracing-appellent-a-une-vigilance-particuliere_6035639_4408996.html

DIXON Helen, « L'antitrust doit prendre en compte la protection des données personnelles », déclare la présidente de la CNIL irlandaise », *Les Echos*, 29 novembre 2019, disponible sur https://www.lesechos.fr/tech-medias/hightech/lantitrust-doit-prendre-en-compte-la-protection-des-donnees-personnelles-declare-la-presidente-de-la-cnil-irlandaise-1152341

MADGE Robert, « Five Loopholes in the GDPR », *Medium.com*, 27 août 2017, disponible sur https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b

NAUGHTON John, « Good Luck in Making Google Reveal its Algorithm », *The Guardian*, 13 novembre 2016, disponible sur https://www.theguardian.com/commentisfree/2016/nov/13/good-luck-in-making-google-reveal-its-algorithm

RUBELLIO Luc, « GAFAM : « L'indépendance de la France se joue à pile ou face » », *Marianne.net*, 3 mai 2021, disponible sur https://www.marianne.net/agora/tribunes-libres/gafam-lindependance-numerique-de-la-france-se-joue-a-pile-ou-face

SAFIRE William, « Nosy Parker Lives », New York Times, 23 septembre 1999, disponible sur nytimes.com.

S.S. Rana & Co, « Loopholes in the General Data Protection Regulation », *Lexology.com*, 4 juin 2018, https://www.lexology.com/library/detail.aspx?g=95a63603-1714-444f-be36-28e3006ac734

VON DER LEYEN Ursula, « Ce qui est interdit dans le monde réel doit être aussi interdit en ligne », *Le Figaro*, 29 janvier 2021, disponible sur https://www.lefigaro.fr/vox/monde/ursula-von-der-leyen-ce-qui-est-interdit-dans-le-monde-reel-doit-etre-aussi-interdit-en-ligne-20210129

2. Presse généraliste

Le Monde, « Une division de l'informatique est créée à la chancellerie "Safari" ou la chasse aux Français », *LeMonde.fr*, Archives, 21 mars 1974, disponible sur https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux-francais_3086610_1819218.html

L'Obs, « Le Lay : « nous vendons du temps de cerveau » », *Nouvelobs.com*, 11 juillet 2004, disponible sur https://www.nouvelobs.com/culture/20040710.OBS2633/le-lay-nous-vendons-du-temps-de-cerveau.html

Le Monde, « Safari et la (nouvelle) chasse aux français », *LeMonde.fr*, BugBrother, 23 décembre 2010, disponible sur https://www.lemonde.fr/blog/bugbrother/2010/12/23/safari-et-la-nouvelle-chasse-aux-francais/

Le Figaro, « Données personnelles : plus de 3000 amendements en Europe », *LeFigaro.fr*, 15 mars 2013, disponible sur https://www.lefigaro.fr/medias/2013/03/15/20004-20130315ARTFIG00552-donnees-personnelles-plus-de-3000-amendements-en-europe.php.

The Guardian, « NSA Prism program taps in to user data of Apple, Google and others », *TheGuardian.com*, 7 juin 2013, disponible sur https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (consulté en juillet 2021).

Le Monde, « Des utilisateurs de Facebook « manipulés » pour une expérience psychologique », *LeMonde.fr*, Pixels, 30 juin 2014, disponible sur https://www.lemonde.fr/pixels/article/2014/06/30/des-utilisateurs-de-facebook-manipules-pour-une-experience-psychologique_4447625_4408996.html

Les Echos, « Le paradoxe des données personnelles », *LesEchos.fr*, 18 juin 2015, disponible sur https://www.lesechos.fr/2015/06/le-paradoxe-des-donnees-personnelles-249939

France Inter, « Logiciels libres et administrations : l'impossible mariage ? », *FranceInter.fr*, 15 septembre 2016, disponible sur https://www.franceinter.fr/info/la-bataille-des-logiciels-libres-reste-ca-mener-dans-l-administration

La Tribune, « Protection des données : les entreprises européennes mal préparées », LaTribune.fr, 18 octobre 2016, disponible sur https://www.latribune.fr/technos-medias/internet/la-reglementation-europeenne-sur-les-donnees-mal-comprise-par-les-entreprises-608575.html

The Guardian, « Margrethe Vestager : « We are doing this because people are angry », *TheGuardian.com*, Interview, 17 septembre 2017, disponible sur

https://www.theguardian.com/world/2017/sep/17/margrethe-vestager-people-feel-angry-about-tax-avoidance-european-competition-commissioner

Le Temps, « Le RGPD, la révolution du consentement », *letemps.ch*, 11 février 2018, disponible sur https://www.letemps.ch/societe/rgpd-revolution-consentement

Les Echos, « La nouvelle ère du consentement numérique », *lesechos.fr*, 29 mai 2018, disponible sur https://www.lesechos.fr/idees-debats/cercle/la-nouvelle-ere-du-consentement-numerique-132946

The Guardian, « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », *TheGuardian.com*, 17 mars 2018, disponible sur https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

The New York Times, « Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens », *NYTimes.com*, 19 mars 2018, disponible sur https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Le Figaro, « Pourquoi Amazon achète la start-up Ring pour un milliard de dollars », *LeFigaro.fr*, 1e mars 2018, disponible sur https://www.lefigaro.fr/secteur/high-tech/2018/03/01/32001-20180301ARTFIG00305-pourquoi-amazon-achete-la-start-up-ring-pour-un-milliard-de-dollars.php

Le Monde, « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », *LeMonde.fr*, Pixels, 22 mars 2018, disponible sur https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html

Le Monde, « Jan Philipp Albrecht, forçat du RGPD », *LeMonde.fr*, 24 mai 2018

Les Echos, « La Californie se dote d'un RGPD », *LesEchos.fr*, 2 juillet 2018, disponible sur https://www.lesechos.fr/tech-medias/hightech/la-californie-se-dote-dun-rgpd-133913

Reuters, « Amazon scraps secret AI recruiting tool that showed bias against women », *Reuters.com*, 11 octobre 2018, disponible sur https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

Le Monde, « Au Parlement européen, l'ombre du Brexit plane sur le débat consacré à Cambridge Analytica », *LeMonde.fr*, 23 octobre 2018, disponible sur https://www.lemonde.fr/pixels/article/2018/10/23/facebook-au-parlement-europeen-l-ombre-du-brexit-plane-sur-le-debat-consacre-a-cambridge-analytica_5373348_4408996.html

BBC, « *Facebook fined £500,000 for Cambridge Analytica scandal* », *bbc.com*, 25 octobre 2018, disponible sur https://www.bbc.com/news/technology-45976300

BBC, « Fake Cambridge Analytica ad hits Facebook », *bbc.com*, 31 octobre 2018, disponible sur https://www.bbc.com/news/technology-46043578

The Register, « Washington Post offers invalid cookie consent under EU rules – ICO », 19 novembre 2018, disponible sur https://www.theregister.com/2018/11/19/ico_washington_post/

France Inter, « Être influençable, est-ce vraiment grave ? », *La Petite Philo*, France Inter, 21 mars 2019, disponible sur https://www.franceinter.fr/emissions/la-petite-philo/la-petite-philo-21-mars-2019

Le Monde, « Les géants du web sont-ils devenus trop puissants ? Les États-Unis ouvrent une enquête », *LeMonde.fr*, Économie, Vie en ligne, 23 juillet 2019, disponible sur https://www.lemonde.fr/economie/article/2019/07/23/ouverture-d-une-enquete-antitrust-sur-les-societes-high-tech_5492664_3234.html

France Culture, « L'expansion des BATX, les GAFAM chinois », *franceculture.fr*, 16 septembre 2019, disponible sur https://www.franceculture.fr/numerique/lexpansion-des-batx-les-gafam-chinois

Les Echos, « Le droit à la vie privée rempart ultime contre l'hégémonie des Gafam », *LesEchos.fr*, 9 décembre 2019, disponible sur https://www.lesechos.fr/idees-debats/editos-analyses/le-droit-a-la-vie-privee-rempart-ultime-contre-lhegemonie-des-gafam-1154706

Les Echos, « La Chine se prépare à réguler ses propres géants du Web », *LesEchos.fr*, 7 janvier 2020, disponible sur https://www.lesechos.fr/tech-medias/hightech/la-chine-se-prepare-a-reguler-ses-propres-geants-du-web-1160949

Forbes, « Les NATU vont-elles rejoindre les GAFAM ? », *Forbes.fr*, 12 février 2020, disponible sur https://www.forbes.fr/technologie/les-natu-vont-elles-rejoindre-les-gafam/

La Tribune, « Le « RGPD californien », une loi modèle, exportable au reste des États-Unis », *Latribune.fr*, 22 février 2020, disponible sur https://www.latribune.fr/economie/international/le-rgpd-californien-une-loi-modele-exportable-au-reste-des-etats-unis-840240.html

Le Monde, « La justice américaine ouvre une procédure contre Google pour abus de position dominante », *LeMonde.fr*, 20 octobre 2020, disponible sur https://www.lemonde.fr/international/article/2020/10/20/la-justice-americaine-ouvre-une-procedure-contre-google-pour-abus-de-position-dominante_6056727_3210.html

Le Monde, « La « cour suprême » de Facebook va commencer à recevoir des réclamations d'utilisateurs », *LeMonde.fr*, 22 octobre 2020, disponible sur

https://www.lemonde.fr/pixels/article/2020/10/22/la-cour-supreme-de-facebook-va-commencer-a-recevoir-des-reclamations-des-utilisateurs_6057009_4408996.html

The Guardian, « The US government wants to break up Facebook. Good – it's long overdue », *TheGuardian.com*, 11 décembre 2020, disponible sur https://www.theguardian.com/commentisfree/2020/dec/11/us-government-break-up-facebook-long-overdue

Ouest France, « Suspension du compte Twitter de Donald Trump : le pouvoir des GAFA inquiète la classe politique », *Ouest-France.fr*, 9 janvier 2021, disponible sur https://www.ouest-france.fr/monde/etats-unis/donald-trump/suspension-du-compte-twitter-de-donald-trump-le-pouvoir-des-gafa-inquiete-la-classe-politique-7112708

Le Monde, « La liberté d'expression à l'heure du numérique ou la difficile quête de l'équilibre sur les réseaux sociaux », *LeMonde.fr*, 2 avril 2021, disponible sur https://www.lemonde.fr/idees/article/2021/04/02/reseaux-sociaux-et-liberte-d-expression-inventer-des-dispositifs-pour-proteger-nos-democraties_6075320_3232.html

Les Echos, « Facebook recentre son projet de monnaie numérique sur le dollar », *LesEchos.fr*, 14 mai 2021, disponible sur https://www.lesechos.fr/finance-marches/marches-financiers/facebook-recentre-son-projet-de-monnaie-numerique-sur-le-dollar-1315154

Le Monde, « En Chine, le « crédit social » des citoyens fait passer les devoirs avant les droits », *LeMonde.fr*, 16 janvier 2020, disponible sur https://www.lemonde.fr/idees/article/2020/01/16/le-credit-social-les-devoirs-avant-les-droits_6026047_3232.html

The Guardian, « Will Ireland's corporation tax rise see tech companies leave Dublin? », *TheGuardian.com*, 23 octobre 2021, disponible sur https://www.theguardian.com/world/2021/oct/23/will-irelands-corporation-tax-rise-see-tech-companies-leave-dublin

Public Sénat, « GAFAM : le Parlement européen s'attaque au « Far-West » du numérique », 20 janvier 2022, disponible sur https://www.publicsenat.fr/article/politique/gafam-le-parlement-europeen-s-attaque-au-far-west-du-numerique-191984

Le Monde, « Publicité en ligne : Bruxelles soupçonne Google et Facebook d'avoir faussé la concurrence », *Le Monde.fr*, 11 mars 2022, disponible sur https://www.lemonde.fr/economie/article/2022/03/11/publicite-en-ligne-bruxelles-soupconne-google-et-facebook-d-avoir-fausse-la-concurrence_6117107_3234.html

Le Monde, « Le « nudging » ou comment inciter les individus à adopter des comportements écoresponsables », *LeMonde.fr*, 7 avril 2022, disponible sur

https://www.lemonde.fr/planete/article/2022/04/07/le-nudging-ou-comment-inciter-les-individus-a-adopter-des-comportements-ecoresponsables_6121043_3244.html

Le Monde, « Tiktok change ses conditions d'utilisation au mépris du consentement de ses utilisateurs », *LeMonde.*fr, 9 juin 2022, disponible sur https://www.lemonde.fr/pixels/article/2022/06/09/tiktok-change-ses-conditions-d-utilisation-au-mepris-du-consentement-de-ses-utilisateurs_6129594_4408996.html

Le Figaro, « TikTok suspend une mise à jour imposant la publicité ciblée en Europe », *LeFigaro.fr*, 12 juillet 2022, disponible sur https://www.lefigaro.fr/flash-eco/tiktok-suspend-une-mise-a-jour-imposant-la-publicite-ciblee-en-europe-20220712

3. Presse spécialisée

NextInpact, « Edward Snowden : Veut-on sacrifier toute notre vie privée au profit de la sécurité ? », *Nextinpact.com*, 11 décembre 2014, disponible sur https://www.nextinpact.com/article/16367/91358-edward-snowden-veut-on-sacrifier-toute-notre-vie-privee-au-profit-securite (consulté en décembre 2022).

ZDNet, « Le RGPD exige (enfin) un consentement éclairé », *zdnet.fr*, 7 décembre 2017, disponible sur https://www.zdnet.fr/actualites/le-rgpd-exige-enfin-un-consentement-eclaire-39861032.htm

Le Journal du Net, « Le consentement aux données est-il vraiment nécessaire », *JournalduNet.com*, 14 septembre 2018, disponible sur https://www.journaldunet.com/solutions/cloud-computing/1211333-le-consentement-aux-donnees-est-il-vraiment-necessaire/

NextInpact, « Privacy Shield : la CNIL irlandaise devrait payer la facture monstre des frais de Max Schrems », 2 novembre 2020, disponible sur https://www.nextinpact.com/lebrief/44457/privacy-shield-cnil-irlandaise-devrait-payer-facture-monstre-frais-max-schrems

JDSSupra, « The end of dark patterns in "cookie walls": German court bans deceptive design », *Jdsupra.com*, 21 janvier 2021, disponible sur https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/

Next Inpact, « Le Digital Markets Act expliqué ligne par ligne », *Nextinpact.com*, 25 janvier 2021, disponible sur https://www.nextinpact.com/article/45317/le-digital-markets-act-explique-ligne-par-ligne

Next Inpact, « La vie privée, ça va payer », *Nextinpact.com,* 3 février 2021, disponible sur https://www.nextinpact.com/article/45876/la-vie-privee-ca-va-payer

NextInpact, « L'assurance maladie se prononce contre Microsoft », *Nextimpact.com*, 22 février 2021, disponible sur https://www.nextinpact.com/lebrief/46167/health-data-hub-assurance-maladie-se-prononce-contre-microsoft

Next Inpact, « La Commission enquête sur les mystères de Jedi Blue, l'accord publicitaire entre Google et Facebook », 14 mars 2022, disponible sur https://www.nextinpact.com/lebrief/68607/la-commission-enquete-sur-mysteres-jedi-blue-laccord-publicitaire-entre-google-et-facebook

IX. ORGANISMES PUBLICS, ONG, ASSOCIATIONS ET ENTREPRISES DU SECTEUR PRIVÉ

AGREMOB, « Nos actions », *Agremob.com*, disponible sur https://agremob.com/nos-actions/.

Aikakausmedia *et al.*, « L'Europe ne peut pas se permettre de manquer la révolution des données », 7 mars 2018, disponible sur https://www.fftelecoms.org/nos-travaux-et-champs-dactions/reglementation-et-fiscalite/e-privacy-lettre-ouverte-europe/.

Alias.dev, « Durées de conservation », disponible sur https://www.durees-de-conservation.fr/.

Axeptio, « Tout savoir sur les taux d'opt-in cookies chez Axeptio », *Axeptio.eu*, disponible sur https://www.axeptio.eu/post/tout-savoir-sur-les-taux-dopt-in-cookies-chez-axeptio.

BCG, *Leveraging GDPR to Become a Trusted Data Steward.*

Brave Software, « Basic Attention Token (BAT). Blockchain Based Digital Advertising », 10 février 2021, pp. 12-13, disponible sur https://basicattentiontoken.org/static-assets/documents/BasicAttentionTokenWhitePaper-4.pdf.

Calendly, *Avis sur la politique de confidentialité, disponible sur https://calendly.com/fr/privacy (consulté en juillet 2022).*

Common sense, https://privacy.commonsense.org/resource/evaluation-questions.

Convert, « Consent vs. Legitimate Interest: Which Should You Choose for Marketing? », *Convert.com,* 5 juin 2019, disponible sur https://www.convert.com/blog/privacy/consent-vs-legitimate-interest/

Crédoc, *Baromètre du numérique 2018*, 18e édition.

Desmarais Avocats, « RGPD : le consentement n'est pas systématique », *Desmarais-Avocats.fr*, disponible sur https://www.desmarais-avocats.fr/rgpd-le-consentement-nest-pas-systematique/.

DEVERGRANNE Thibaut, « RGPD : arrêtez de demander le consentement ! », *donneespersonnelles.fr*, disponible sur https://www.donneespersonnelles.fr/rgpd-arretez-le-consentement.

Didomi, « Some cookies are dropped on my website before consent », *Didomi.io*, disponible sur https://support.didomi.io/some-cookies-are-dropped-on-my-website-before-consent .

EF EPI, *Un classement de 100 pays et régions par compétences en anglais,* édition 2020, disponible sur https://www.ef.com/cafr/epi/.

EGAN Erin, *Charting a Way Forward – Data Portability and Privacy*, Facebook, septembre 2019, 21 p.

FING, *Self Data Territorial*, Feuille de route pour une implémentation du Self Data par les villes en France et en Europe, novembre 2021.

ForbrukerRådet, *Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*, 27 juin 2018.

Future of Privacy Forum, *Comparing Privacy Laws: GDPR v. CCPA*, novembre 2018, p. 23, disponible sur https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf .

GHOSH Dipayan, « What You Need to Know About California's New Data Privacy Law », *Harvard Business Review*, 11 juillet 2018, disponible sur https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

Google Ad Manager, « Ad Manager and Ad Exchange program policies. Publisher integration with the IAB TCF v. 2.0 », Google Ad Manager Help, disponible sur https://support.google.com/admanager/answer/9805023?hl=en&ref_topic=28145.

Google, « Web Push Notifications: Timely, Relevant, and Precise », *Google.com*, Web fundamentals, 12 février 2019, disponible sur https://developers.google.com/web/fundamentals/push-notifications .

HuckBlackwell, « How do the CPRA, CPA, and VCDPA treat dark patterns », *JDSupra*, 17 mars 2022, disponible sur https://www.jdsupra.com/legalnews/how-do-the-cpra-cpa-and-vcdpa-treat-5714239/.

INSEE, « Écart de salaires en équivalent temps plein entre femmes et hommes », Insee.fr, *Tableau de bord de l'économie française*, 5 mai 2021, disponible sur https://www.insee.fr/fr/outil-interactif/5367857/details/40_SOC/44_EGF/44G_Figure7.

Institut Montaigne, *Algorithms: Please Mind the Bias!*, Institutmontaigne.org, mars 2020, p. 6, disponible sur https://www.institutmontaigne.org/ressources/pdfs/publications/algorithms-please-mind-bias.pdf.

Irish Council for Civil Liberties, « Europe's enforcement paralysis. ICCL's 2021 report on the enforcement capacity of data protection authorities », 2021.

KUNER Christopher, « The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law », *Bloomberg BNA Privacy and Security Law Report*, 6 février 2012.

La Quadrature du Net, « Pour l'interopérabilité des géants du web : lettre commune de 75 organisations », *Laquadrature.net*, 21 mai 2019, disponible sur

https://www.laquadrature.net/2019/05/21/pour-linteroperabilite-des-geants-du-web-lettre-commune-de-45-organisations/.

Microsoft, « Answering Europe's Call: Storing and Processing EU Data in the EU », *Microsoft.com*, 6 mai 2021, disponible sur https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/.

Mine, https://saymine.com/.

MyData, https://mydata.org/.

Mydex, https://mydex.org/.

Nextcloud, https://nextcloud.com/fr_FR/.

None of your business, « 226 complaints lodged against deceptive cookie banners », *noyb.eu*, 9 août 2022, disponible sur https://noyb.eu/en/226-complaints-lodged-against-deceptive-cookie-banners.

None of Your Business, « DPC ordered to pick up most of the legal bill of EU-US data transfer case », *noyb.eu*, 30 octobre 2020, disponible sur https://noyb.eu/en/dpc-ordered-pick-most-legal-bill-eu-us-data-transfer-case.

None of Your Business, « More Cookie Banners to go Second Wave of Complaints Underway », 4 mars 2022, disponible sur https://noyb.eu/en/more-cookie-banners-go-second-wave-complaints-underway.

None of Your Business, « Noyb aims to end « cookie banner terror » and issues more than 500 GDPR complaints », 31 mai 2021, disponible sur https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints.

NOYB, « Irish DPC greenlights Facebook "GDPR bypass" », *noyb.eu*, 13 octobre 2021, disponible sur https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass.

Privacy board, https://www.privacyboard.co/software/visitor-analytics.

Privacy Monitor, https://www.privacymonitor.com/articles/privacy-guide/.

Privacy Patterns, "Privacy Dashboard", *Privacypatters.org*, disponible sur https://privacypatterns.org/patterns/Privacy-dashboard.

Privacy Patterns, « Privacy Dashboard », *Privacypatters.org*, disponible sur https://privacypatterns.org/patterns/Privacy-dashboard .

Privacy Rating, https://www.privacyrating.info/#/about.

Privacyscore, https://privacyscore.org/.

Proviti, « GDPR: Legitimate Interest vs. Consent », *Blog.proviti.com*, 6 juin 2018, disponible sur https://blog.protiviti.com/2018/07/06/gdpr-legitimate-interest-vs-consent/.

Ranking Digital Rights, https://rankingdigitalrights.org/index2019/categories/privacy/.

S.S. Rana & Co, « Loopholes in the General Data Protection Regulation », *Lexology.com,* 4 juin 2018, disponible sur https://www.lexology.com/library/detail.aspx?g=95a63603-1714-444f-be36-28e3006ac734.

Sarbacane, « Le RGPD rend-il obligatoire le consentement ? », *Sarbacane.com*, disponible sur https://www.sarbacane.com/help/rgpd/general-rgpd/rgpd-consentement.

Solid Project, https://solidproject.org/.

UFC Que Choisir, « Labels alimentaires et signes de qualité. Promesses non tenues : une révision s'impose ! », *QueChoisir.org*, 28 septembre 2021, disponible sur https://www.quechoisir.org/action-ufc-que-choisir-labels-alimentaires-et-signes-de-qualite-promesses-non-tenues-une-revision-s-impose-n94920/.

UIE, « Do users change their settings? », *uie.com*, 14 septembre 2011, disponible sur https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/.

UNAPEI, *L'information pour tous. Règles européennes pour une information facile à lire et à comprendre*, 2009.

Union française du Marketing Direct, *Charte sur la publicité ciblée et la protection des internautes*, 2010.

Usable Privacy, https://usableprivacy.org/learn_more.

VACAS Federico, **BOISSON** Laurène, « Les Français et l'anglais : seuls 21% estiment avoir un niveau satisfaisant », *Ipsos.com*, 23 septembre 2019, disponible sur https://www.ipsos.com/fr-fr/les-francais-et-langlais-seuls-21-estiment-avoir-un-niveau-satisfaisant.

We are social, Digital 2021 France, Special Report, disponible sur https://wearesocial.com/fr/blog/2021/01/digital-2021-france/.

Weizenbaum institute, *Annual Report*, 2018-2019.

WWF, **Greenpeace**, **BASIC**, *Étude des démarches de durabilité dans le domaine alimentaire*, Rapport d'analyse transverse, juin 2021, 58 p.

X. STANDARDS ET ORGANISMES DE STANDARDS

ETSI, *Securing Artificial Intelligence (SAI); Problem Statement*, ETSI, Group Report, ETSI GR SAI 004, décembre 2020, version 1.1.1, ETSI GR SAI 004.

International Electrotechnical Commission (IEC), « SEG 10. Ethics in Autonomous and Artificial Intelligence Applications », *IEC.ch*, disponible sur https://www.iec.ch/dyn/www/f?p=103:187:616184075401079::::FSP_ORG_ID,FSP_LANG_ID:22827,34.

ISO, « Standards by ISO/IEC JTC 1/SC 42. Artificial Intelligence. », *ISO.org*, disponible sur https://www.iso.org/committee/6794475/x/catalogue/.

ISO/CEI, *Évaluation de la conformité – Exigences pour les organismes certifiant les produits, les procédés et les services*, ISO/CEI 17065 :2012, septembre 2012, disponible sur https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v2:fr.

ISO/IEC AWI TR 24368 « Information technology – Artificial Intelligence – Overview of ethical and societal concerns ».

The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design : A Vision for Proritizing Human Well-being with Autonomous and Intelligent Systems*, IEEE, 1e edition, 2019, p. 23, disponible sur https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html.

W3C, « The Platform for Privacy Preferences1.1 (P3P1.1) Specification », *W3C Working Group Note*, 13 novembre 2006, Retiré le 30 août 2018, disponible sur https://www.w3.org/TR/P3P11/#P3P1.1.

INDEX ALPHABÉTIQUE

TABLE DES MATIERES

TABLE DES FIGURES

RESUME EN FRANÇAIS

Face au développement de la technologie de l'information et de la communication, le contrôle des données à caractère personnel par les individus est devenu un enjeu majeur au sein de l'Union européenne. Le Règlement européen sur la protection des données (RGPD) a ainsi été adopté dans une logique d'*empowerement* (empouvoirement) de la personne concernée par le traitement, en renforçant la réalité du consentement, évaluée comme la traduction fidèle de la manifestation de volonté. L'évaluation du mécanisme de consentement montre la volonté du législateur de rester fidèle à la volonté de la personne concernée, par la multiplication des garanties s'appliquant à la demande, au contrôle et au retrait du consentement. Or, si le consentement RGPD a été une évolution législative permettant à la personne concernée d'obtenir plus de contrôle de ses données à caractère personnel, force est de constater que ce consentement présente tout de même des limites. Ces limites appellent à une réflexion juridique de fond afin de déterminer les situations où le consentement nécessite des garanties supplémentaires pour être valide ou des précisions supplémentaires pour s'articuler correctement avec d'autres dispositions juridiques et les situations où le consentement est à proscrire du fait de l'incapacité de la personne concernée d'émettre un consentement libre et éclairé.

RESUME EN ANGLAIS

Faced with the development of information and communication technology, the individual's control of personal data has become a major issue in the European Union. The European Data Protection Regulation (GDPR) was thus adopted with a view to empowering the data subject, by reinforcing the reality of consent, assessed as the faithful translation of the manifestation of will. The evaluation of the consent mechanism shows the legislator's desire to remain faithful to the will of the data subject, by multiplying the guarantees applying to the request, supervision, and withdrawal of consent. However, if the GDPR consent is a legislative evolution providing the data subject with more control over his or her personal data, consent still has its limits. These limits call for a fundamental legal reflection in order to determine the situations where consent requires additional guarantees to be valid or additional clarifications to be correctly articulated with other legal provisions, and the situations where consent is to be prohibited because of the inability for the data subject to give a free and informed consent.