Le principe de transparence des traitements algorithmiques : de l'étude juridique d'un enjeu démocratique

Yann Paquier

Normandie Université

THÈSE

Pour obtenir le diplôme de doctorat

Spécialité SCIENCES JURIDIQUES

Préparée au sein de l'Université de Caen Normandie

Le principe de transparence des traitements algorithmiques : de l'étude juridique d'un enjeu démocratique

Présentée et soutenue par
YANN PAQUIER

Thèse soutenue le 10/11/2021 devant le jury composé de		
MME LUCIE CLUZEL-METAYER	Professeur des universités, Université Paris-Nanterre	Rapporteur du jury
MME NATHALIE NEVEJANS	Maître de conférences HDR, Université d'Artois	Rapporteur du jury
MME CATHERINE CHASSIN	Professeur des universités, Université Caen Normandie	Président du jury
M. JEAN-MANUEL LARRALDE	Professeur des universités, Université Caen Normandie	Directeur de thèse

Thèse dirigée par JEAN-MANUEL LARRALDE, Centre de recherches sur les droits fondamentaux et les évolutions du droit (Caen)

UNIVERSITÉ CAEN NORMANDIE

ED 98 DN Droit Normandie

CRDFED
CENTRE DE RECHERCHE SUR LES DROITS FONDAMENTAUX & LES ÉVOLUTIONS DU DROIT
EA2132

Remerciements

Je tiens particulièrement à remercier le Professeur Jean-Manuel Larralde d'avoir assuré la direction de cette thèse. Sa disponibilité, son humanité et son ouverture d'esprit m'ont permis d'aller jusqu'au bout de ces travaux. Il m'a laissé l'autonomie nécessaire à l'épanouissement de mes réflexions, ce dont j'avais besoin, tout en m'orientant comme il se devait. Cette liberté dans la recherche a été pour moi un élément essentiel à la réalisation d'un doctorat, qui reste une expérience hors du commun dans la confrontation aux idées et à soi-même. Je n'imaginais pas autre directeur de thèse.

A la Région Normandie qui a encouragé ces travaux en me finançant durant trois années.

A mes collègues du Centre de Recherche sur les Droits fondamentaux et les Evolutions du Droit, et à mes amis, que la pandémie nous on a un temps séparé.

À mon épouse, Clémentine, sans qui il m'aurait sans doute été impossible d'achever ces travaux. Son soutien sans faille lors des moments de doute et de désillusions doctorales m'a été précieux, et ne sont pas étrangers aussi bien au choix de cette aventure qu'à son aboutissement.

À ma famille, à mes parents, qui m'ont toujours accompagné et soutenu dans la réalisation de mes projets.

Enfin, à Maître Henri Allain, avocat au barreau de Caen, parti trop tôt, et avec qui j'ai eu la chance de travailler de nombreuses années. Sa gentillesse et son amitié m'ont aussi apporté la force de me lancer dans ce projet notamment pour me spécialiser en droit du numérique. Je lui dédie cette thèse.

A Maître Henri Allain,

SOMMAIRE

Liste des principales abréviations

AAI	*Autorité administrative indépendante*
AFDA	*Association Française pour la Recherche en Droit Administratif*
AJDA	*Actualité juridique – Droit administratif*
AMF	*Autorité des marchés financiers*
APB	*Admission Post-Bac*
ARCEP	*Autorité de régulation des communications électroniques, des postes et de la distribution de la presse*
Art.	*Article*
ART	*Autorité de régulation des transports*
CADA	*Commission d'accès aux documents administratifs*
CC	*Conseil constitutionnel*
CCNE	*Comité consultatif national d'éthique*
CE	*Conseil d'Etat*
CEDH	*Convention européenne des droits de l'homme*
CEPD	*Contrôleur européen de la protection des données personnelles*
CEPEJ	*Conseil de l'Europe Commission européenne pour l'efficacité de la justice*
CIL	*Correspondant Informatique et Libertés*
CJUE	*Cour de Justice de l'Union européenne*
CNCDH	*Commission nationale consultative des droits de l'homme*
CNCTR	*Commission Nationale de Contrôle des Techniques de Renseignement*
CNN	*Conseil National du numérique*
CNPEN	*Comité national pilote d'éthique du numérique*
CNRS	*Centre national de la recherche scientifique*
Cons.	*Considérant*
Convention 108	*Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*
Cour EDH	*Cour européenne des droits de l'homme*
CPP	*Code de procédure pénale*
CRPA	*Code des Relations entre le Public et l'Administration*
CSA	*Conseil supérieur de l'audiovisuel*
CSP	*Code de la Santé Publique*
Dalloz IP/IT	*Revue Dalloz – Droit de la propriété intellectuelle et du numérique*
DDHC	*Déclaration des Droits de l'Homme et du Citoyen de 1789*
DGCCRF	*Direction Générale de la Concurrence, de la Consommation et de la Répression des fraudes*
DINSIC	*Direction interministérielle du numérique et du système d'information et de communication de l'Etat*
DINUM	*Direction Interministérielle du Numérique*
Dir.	*Sous la direction de*
DPD	*Délégué à la protection des données*
G29	*Groupe de travail de l'article 29 sur la protection des données personnelles*
HAS	*Haute autorité de santé*
Ibid	*Au même endroit*

Infra	*Voir plus bas*
INRIA	*Institut national de recherche en sciences et technologies du numérique*
LGDJ	*Librairie générale de droit et de jurisprudence*
LIL	*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (« Loi informatique et libertés »)*
LRN	*Loi pour une République Numérique*
MESRI	*Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation*
NTIC	*Nouvelles technologies de l'information et de la communication*
OCDE	*Organisation de coopération et de développement économiques*
PUC	*Presses Universitaires de Caen*
PUF	*Presses Universitaire de France*
QPC	*Question prioritaire de constitutionnalité*
RDP	*Revue du droit public*
RFDA	*Revue française de droit administratif*
RGPD	*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)*
RSC	*Revue de science criminelle et de droit pénal comparé*
SAFARI	*Système automatisé pour les fichiers administratifs et le répertoire des individus*
SSMVM	*Service de Surveillance du Marché des Véhicules et des Moteurs*
Supra	*Voir plus haut*
TA	*Tribunal Administratif*
TGI	*Tribunal de Grande Instance*

INTRODUCTION GENERALE

1. « *Ces algorithmes ne sont pas écrits par Dieu depuis le paradis* ». C'est en ces termes que s'exprimait Andreas Mundt, ancien Président de l'autorité fédérale de la concurrence allemande au sujet de la fluctuation des prix observée sur la plateforme de vente en ligne d'une compagnie aérienne en position dominante[1].

2. Ces algorithmes souvent associés à une recette de cuisine sont en réalité bien plus que cela. Nous en découvrons le plus souvent les effets par la voie de presse, parce qu'ils sont difficilement observables, surtout pour les profanes en informatique, alors que nous les suspectons régulièrement de menacer les droits et libertés et de concurrencer l'Etat, pourtant l'émanation de l'autonomie des citoyens en démocratie[2].

3. Bien que le numérique repose sur des infrastructures matérielles, un univers s'émancipe progressivement des lois de la physique qui règnent en maître dans notre monde. Lawrence Lessig l'avait déjà démontré avec son célèbre adage « *Code is law* »[3] : les architectures numériques conditionnent l'exercice des droits et libertés, y compris celles pensées sur le terrain classique[4]. Ce n'est pas la première fois que l'humanité est confrontée à une révolution nécessitant une régulation particulière. Mais les processus informatiques ont ceci de paradoxal que nous y laissons de nombreuses traces, sans pouvoir y observer aisément leur fonctionnement. Ces technologies demeurent comme nous le verrons le fruit d'une convergence entre plusieurs techniques demandant un haut niveau d'expertise.

4. Cette difficulté observationnelle inhérente à la nature de l'informatique n'est pas sans conséquence puisqu'elle entraîne pour effet une difficile régulation faute de cartographie de cet environnement, alors que toute régulation n'est rendue possible que par la constatation d'un fait juridique, qui, s'il ne nous apparaît pas, ne peut être saisi par les corps constitués de l'Etat et le débat politique. Les incidences du numérique sont si difficiles à évaluer que nous en suspectons

[1] AGENCE FRANCE PRESSE, Prix des billets : Lufthansa dans le viseur du gendarme Allemand, *L'Express* [en ligne]. 28 décembre 2017. [Consulté le 25 janvier 2021]. Disponible à l'adresse : https://lexpansion.lexpress.fr/actualites/1/actualite-economique/prix-des-billets-lufthansa-dans-le-viseur-du-gendarme-allemand_1972198.html

[2] Selon Marie-Anne Cohendet il convient d'entendre par l'autonomie des citoyens, « *ce qui essentiel pour que la démocratie existe (…)* » c'est-à-dire que « *nous n'obéissions qu'à nous-même ou au moins à la volonté de la majorité des citoyens librement exprimée* », COHENDET M-A., *Droit constitutionnel, LGDJ*, 2015, p. 71.

[3] LESSIG L., *Code and Other Laws of Cyberespace, Basic Books*, 1999, 320 p.

[4] A cet égard, les anthropologues en lieu et place de la distinction monde virtuel/monde réel, s'accordent davantage sur la distinction terrain en ligne/terrain classique. Voir en ce sens, BOELLSTORFF T., *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*, Princeton University Press, 2008, 344 p. (*Un anthropologue dans* Second Life. *Une expérience de l'humanité virtuelle*, trad. franç. SERVAIS O., et DHEN G., Academia-L'Harmattan, Louvain-la-Neuve, 2013, 470 p.).

les dérives potentielles, mais elles ne restent la plupart du temps que supputations tant les preuves manquent.

5. La révolution numérique marque l'informatisation de la société à marche forcée, parfois à outrance sans que nous ne pensions les conséquences de son déploiement sur les individus et la société. Pourtant, le numérique « *augmente le pouvoir des individus* »[5], et en cela il est parfois qualifié de facilitateur concernant l'exercice de nombreuses libertés telles que la liberté d'expression[6]. De l'autre, son opacité encourage un positionnement insidieux de puissances de nature différentes, aussi bien de la part d'acteurs privés que publics par l'intermédiaire de cet outil : l'algorithme informatique. Il est donc enjeu de pouvoir et il pénètre désormais tous les secteurs de la société. En plus de ne pas être neutres, les algorithmes exercent des incidences sur l'effectivité des droits et libertés, voire sur l'efficacité de l'ordre juridique, ce qui constitue un risque (I).

6. En outre, comme l'indique Lawrence Lessig,

> « *Nous devrions interroger l'architecture du cyberespace comme nous interrogeons le code du Congrès. Si nous ne le faisons pas, ou si nous n'apprenons pas à le faire, la pertinence de notre tradition constitutionnelle s'estompera. L'importance de notre engagement envers les valeurs fondamentales, par le biais d'une constitution adoptée de manière consciente, s'estompera. La menace que cette époque représente pour les libertés et les valeurs dont nous avons hérité nous échappera. La loi du cyberespace sera celle que le cyberespace codera, mais nous aurons perdu notre rôle dans l'établissement de cette loi* »[7].

7. C'est la raison pour laquelle, afin d'appréhender le mieux possible ledit fait juridique pour l'interroger et le réguler, une nouvelle organisation de l'Etat, reposant sur le respect d'autonomie des citoyens en démocratie par l'intermédiaire d'un principe de transparence des outils de cette nouvelle sphère doit être capable de protéger les individus et la société dans son

[5] CARDON D., *Culture numérique, Presses de la fondation nationale des sciences politiques*, 2019, p. 7.
[6] LA RUE F., *Report of the special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Rapport des Nations Unies, mai 2011.
[7] LESSIG L., *Code Is Law: on liberty in cyberspace*, Harvard Magazine, 1er janvier 2000. Traduit de l'anglais « *We should interrogate the architecture of cyberspace as we interrogate the code of Congress. Unless we do, or unless we learn how, the relevance of our constitutional tradition will fade. The importance of our commitment to fundamental values, through a self-consciously enacted constitution, will fade. We will miss the threat that this age presents to the liberties and values that we have inherited. The law of cyberspace will be how cyberspace codes it, but we will have lost our role in setting that law* ».

ensemble, des ingérences des gouvernants et des acteurs privés (II). Il s'agit d'une clé de voûte indispensable au respect des libertés.

I - Le risque algorithmique

8. Sans entrer dans la typologie des algorithmes car il ne s'agit pas de travaux en informatique, il convient tout de même de s'intéresser à une brève histoire de l'informatique (A) ainsi qu'aux incidences du recours aux algorithmes sur la société et les personnes (B) afin de cerner au mieux la nature du risque algorithmique.

A - Brève histoire de l'informatique

1 - La rencontre de l'algorithme et de la machine

9. L'histoire des algorithmes remonte à l'Antiquité. Même s'ils n'étaient pas encore désignés en tant que tel sous cette dénomination, des scribes de Mésopotamie et d'Egypte utilisaient déjà des processus mathématiques pour faciliter de nombreux calculs comme en matière agricole ou pour répartir une succession[8]. En ce sens, l'algorithme est un « *ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations* »[9]. Bien que les Grecs poursuivirent d'importants travaux en algorithmique, il faudra attendre le célèbre mathématicien médiéval perse Al-Khwârizmî, notamment père de l'algèbre, pour que le terme « algorithme » apparaisse, étant issu de la traduction latine de son patronyme[10].

10. Toutefois, la rencontre de l'algorithme et de l'informatique est plus tardive puisqu'elle implique la découverte des premières machines et la volonté de s'en servir pour aboutir à la résolution automatique de problèmes. François Pellegrini et Sebastien Canevet notent que les premières machines à tisser automatiques commercialisées par Joseph-Marie Jacquard en 1801 peuvent être considérées comme les ancêtres des ordinateurs. Mais leur fonctionnement ne dépendait pas d'un programme informatique[11]. Les machines programmables feront leur

[8] DOWEK G., « Les origines de l'informatique », *Cahiers philosophiques*, Réseau Canopé, n° 141, 2015/2, p. 7 à 15.
[9] LAROUSSE, Définition « Algorithme », *Larousse.fr* [en ligne]. [Consulté le 2 mars 2018]. Disponible à l'adresse : https://www.larousse.fr/dictionnaires/francais/algorithme/2238
[10] PIRE B., AL-KHWARIZMI, *Encyclopædia Universalis* [en ligne]. [Consulté le 29 juin 2021]. Disponible à l'adresse : https://www.universalis.fr/encyclopedie/al-khwarizmi/
[11] François Pellegrini et Sébastien Canevet notent que « *si les perforations des plaques de carton symbolisant le motif à tisser représentaient des données conditionnant le résultat produit par le métier à tisser, elles ne constituaient pas à proprement parler un programme. En effet, le motif des perforations, s'il pouvait renseigner un tisserand sur ce que produirait un métier auquel il serait fourni, ne portait pas en revanche d'informations autres que le résultat à produire, dont il n'était qu'une simple transposition* », PELLEGRINI F., CANEVET S., *Droit des logiciels*, *PUF*, 2013, p. 27.

apparition plus tardivement, et ouvriront ensuite la voie à la machine universelle d'Alan Turing en 1936, notamment par le calcul binaire de l'information. C'est la fusion de la machine et de la « *programmabilité* » qui aboutira à la naissance de l'ordinateur moderne[12], et donc du mariage entre le traditionnel algorithme et l'informatique. Le passage du signal analogique au numérique marque donc une révolution[13] et un changement de paradigme.

2 - Le fonctionnement d'un ordinateur

11. Mais avant d'évoquer les incidences de ces algorithmes sur les personnes et la société, il est nécessaire d'aborder brièvement et le plus simplement possible le fonctionnement d'un ordinateur, ne serait-ce car le droit est amené à recourir à ces notions, pour comprendre les termes clés que nous utiliserons tout le long de ces travaux.

12. Un ordinateur se définit comme « *une machine programmable de traitement de l'information. Il est constitué d'une mémoire permettant de stocker les programmes et leurs données, et d'un processeur exécutant les instructions des programmes, afin d'effectuer des calculs sur les données* »[14]. Il est alors constitué d'une partie matérielle et logicielle. Un ordinateur peut exécuter une pluralité d'algorithmes retranscrits dans un programme.

13. Ainsi, « *on qualifie de numérique un algorithme qui a été conçu pour être implémenté dans un code informatique destiné à faire tourner une simulation ou un calcul sur un ou plusieurs microprocesseurs d'un ordinateur* »[15]. En d'autres termes, nous avons choisi le qualificatif de traitement algorithmique car il s'agit de la rencontre d'un code informatique et de son exécution par un ordinateur. Comme le note François Pellegrini[16], l'algorithme renvoie à une abstraction pour résoudre un problème, tandis qu'un programme informatique est ce que l'on souhaite faire faire à un ordinateur. Enfin, le traitement est « *ce qui s'exécute effectivement et peut être soumis à des aléas et erreurs transitoires issues de l'environnement* »[17]. Une attention particulière doit donc être donnée au code source puisqu'il est la retranscription en

---

[12] DOWEK G., « Les origines de l'informatique », *op. cit*.
[13] Comme l'indique Dominique Cardon, « *c'est la magie du codage informatique, une fois les informations transformées en chiffres, il est possible de conduire l'ensemble des opérations qui sont à l'origine de la révolution numérique : les données peuvent être stockées et archivées dans des fichiers ; elles peuvent être déplacées et échangées et donc favoriser la communication à distance et la coopération ; elles peuvent, enfin, être calculées et transformées de mille et une manières. L'informatique et les ordinateurs sont les agents de ces transformations* », CARDON D., *Culture numérique*, *op. cit.*, p. 23.
[14] PELLEGRINI F., CANEVET S., *Droit des logiciels, op. cit.*, p. 557.
[15] JEAN A., *De l'autre côté de la Machine, Voyage d'une scientifique au pays des algorithmes*, *Editions de l'observatoire*, 2019, p. 42.
[16] PELLEGRINI F., « Les algos : ni loyaux, ni éthiques ! », *Blog Binaire Le Monde* [en ligne]. 27 mars 2017. [Consulté le 25 avril 2020]. Disponible à l'adresse : https://www.lemonde.fr/blog/binaire/2017/03/27/les-algos-ni-loyaux-ni-ethiques/
[17] *Ibid*.

informatique de l'abstraction des algorithmes composants le logiciel. La commission d'accès aux documents administratifs (CADA) définit le code source comme « *un ensemble de fichiers informatiques qui contient les instructions devant être exécutées par un micro-processeur* »[18].

14. Bien que nous y revenions plus tard, il convient donc d'affirmer dès à présent que les algorithmes ne sont pas neutres puisqu'ils sont conçus pour résoudre un problème identifié[19]. La programmation consiste à implanter dans un logiciel le ou les algorithme(s) devant être exécutés par un ordinateur, ce qui sera effectué par l'intermédiaire d'un compilateur dont l'objectif est de retranscrire le programme sous forme binaire afin qu'il soit lisible par la machine. Cette étape est délicate, car il convient de mettre dans un langage informatique les algorithmes que l'on cherche à exécuter par l'ordinateur. Pour cela, certains arbitrages doivent être opérés pour qu'ils soient en adéquation avec ce que la machine permet. Comme l'indique un adage en informatique, « *cette machine m'énerve, elle fait ce que je lui ai dit de faire, et pas ce que je veux qu'elle fasse* »[20]. On comprend donc d'ores et déjà que les logiciels permettent l'automatisation de la résolution de problèmes, mais dans les limites matérielles de l'ordinateur.

15. L'informatique est aussi une pluralité de processus complexes et difficilement observables, demandant une solide expérience pour être compris, lorsque l'état de l'art le permet, et susceptible de se heurter à des erreurs. Des erreurs peuvent interférer à chaque étape du processus, c'est-à-dire de la conception de l'algorithme à son implémentation, puis à son exécution par l'ordinateur. Il peut donc arriver qu'un code informatique soit bien conçu, mais son exécution va engendrer des effets tout autres que ce qui était prévu[21]. Prendre connaissance des algorithmes qui ont vocation à être implantés dans un programme informatique ou d'un code source ne renseigne pas avec exactitude que le résultat généré par la machine est correct. D'autres problèmes peuvent également apparaître sans constituer des erreurs de programmation, mais plutôt en amont lors de la conception des modèles de l'algorithme. Il peut s'agir de biais algorithmiques. Aurélie Jean indique que « *toute modélisation reste une approximation de la réalité* »[22]. Ainsi, ce qui n'est pas prévu dans le modèle, n'est pas pris en compte par l'ordinateur, et le développement de ce modèle est susceptible de biais

[18] CADA, avis n° 20161989 du 23 juin 2016.
[19] Dominique Cardon précise qu'« *il est en effet vain de demander aux algorithmes d'être « neutres » alors qu'ils sont généralement conçus pour choisir, trier, filtrer ou ordonner les informations selon certains principes* », CARDON D., « Le pouvoir des algorithmes », *in La Datacratie, Revue Pouvoirs*, n° 164, janvier 2018, p. 63 à 73.
[20] Cet adage est notamment relaté par François Pellegrini dans son ouvrage sur le droit des logiciels, p. 65.
[21] PELLEGRINI F., Chaînes de confiance et périmètres de certification : le cas des systèmes de "vote électronique", Rapport de recherche, RR-8553, 2014, *INRIA* [en ligne]. 27 juillet 2014, mis à jour le 11 février 2021. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://hal.inria.fr/hal-01010950v4
[22] JEAN A., *De l'autre côté de la Machine, Voyage d'une scientifique au pays des algorithmes, op. cit.*, p. 80.

algorithmiques, d'ailleurs souvent issus de biais cognitifs humains, et pouvant engendrer, par exemple, des discriminations[23] s'ils sont amenés à être déployés pour fonder des décisions ayant des incidences sur les personnes.

16. Il est également possible de rencontrer de tels biais inférés par les données exploitées s'il s'agit d'un programme auto-apprenant[24]. De plus, et sans entrer dans le détail, il existe aujourd'hui plusieurs classes de traitements algorithmiques allant du plus simple au plus complexe. Les méthodes les plus sophistiquées retiennent aujourd'hui une attention toute particulière : il s'agit de l'intelligence artificielle (IA). Bien qu'il existe des tentatives de définitions juridiques, (que nous serons amenés à aborder), sa définition ne fait cependant pas l'unanimité, y compris chez les informaticiens. Toutefois, il est possible de considérer qu'il s'agit d'une pluralité de techniques visant à résoudre toujours plus de problèmes, de préférence par eux-mêmes par l'intermédiaire d'un apprentissage effectué sur le fondement de nombreuses données. Les données et leurs paramétrages utilisés par ces systèmes jouent donc un rôle encore plus significatif que les algorithmes implantés dans le programme, ce qui leur vaut le qualificatif de boîte noire. Il n'est pas aisé au regard de l'état de l'art en informatique de comprendre l'intégralité du processus ayant mené au calcul final du logiciel, raison pour laquelle l'observation d'un tel système en comparaison à la compréhension d'un simple fichier « Excel » utilisé par une équipe pédagogique d'une université pour calculer la moyenne des notes d'un candidat[25], n'est pas de même nature. L'opacité technique se heurte donc parfois à la compréhension de ces systèmes. Concrètement, comme le note Yann LeCun, « *un système entraînable peut être vu comme une boite noire avec une entrée, par exemple une image, un son, ou un texte, et une sortie qui peut représenter la catégorie de l'objet dans l'image, le mot prononcé, ou le sujet dont parle le texte. On parle alors de systèmes de classification ou de reconnaissance des formes.* »[26]. Ce sont donc des systèmes qui vont être privilégiés pour effectuer des recommandations, voire identifier des contenus illicites. Ces systèmes se généralisent depuis le début des années 2010, alors qu'il ne s'agit pas de techniques récentes

[23] Voir particulièrement en ce sens, CHAPENET J., LEQUESNE ROTH C., « Discrimination et biais genrés : les lacunes juridiques de l'audit algorithmique », *Recueil Dalloz*, 2019, p. 1852.

[24] Selon le Conseil constitutionnel les algorithmes auto-apprenants sont « *des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement* », CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*, § 71.

[25] Nous faisons évidemment référence aux algorithmes locaux de « *Parcoursup* » utilisés par certaines équipes pédagogiques afin de s'en servir comme aide à la prise de décisions, en calculant automatiquement des moyennes, voire hiérarchiser des candidatures entre elles, dans le cadre de la sélection à l'entrée de certaines filières universitaires. Pour plus de précisions, *Infra*., n° 429.

[26] LECUN Y., Qu'est-ce que l'intelligence artificielle ?, *Collège de France* [en ligne]. [Consulté le 28 octobre 2020]. Disponible à l'adresse : https://www.college-de-france.fr/site/yann-lecun/Recherches-sur-l-intelligence-artificielle.htm#:~:text=On%20pourrait%20dire%20que%20l,humains%20et%20%C3%A0%20certains%20animaux.&text=Le%20domaine%20de%20l'IA,comme%20essentiel%20%C3%A0%20l'intelligence.

puisqu'elles sont le fruit de travaux menés dans les années quatre-vingt, et dont l'application pratique a été rendue possible par les progrès techniques[27].

17. Nous serons parfois tout de même amenés à utiliser le terme d'« algorithme » en tant que synonyme de traitement, car certaines normes juridiques assimilent les deux notions, ce que nous ne pouvons pas ignorer dans notre réflexion, à moins que nous fassions référence à un processus particulier du fonctionnement de l'informatique, auquel cas nous serons amenés à le préciser. La notion de « traitement algorithmique » a également été retenue car il s'agit du qualificatif le plus englobant pour appréhender l'observation de l'entièreté d'un processus décisionnel : de l'algorithme, de son implémentation dans un code informatique, à son exécution par l'ordinateur. Le terme de traitement est par ailleurs celui retenu dans de nombreux régimes juridiques tels que par exemple la « Loi Informatique et Libertés » (LIL) de 1978[28] ou encore la « Loi pour une République Numérique »[29] (LRN) concernant les décisions administratives individuelles fondées sur un tel processus. Ce qualificatif ne nous empêche pas par ailleurs d'évoquer, lorsque le droit le prévoit spécifiquement, l'étude des régimes abordant seulement l'algorithme ou les caractéristiques de celui-ci. Les réflexions menées ont impliqué une connaissance des enjeux du numérique, raison pour laquelle, lors des démonstrations il sera question de revenir sur certaines notions précédemment développées pour que le lecteur puisse poursuivre au mieux les argumentaires.

B - Les incidences des algorithmes sur la société et le droit

18. Cette étude ne vise pas l'exhaustivité en matière de caractéristiques et d'effets juridiques induits par la révolution numérique dans la mesure où toutes les conséquences issues du recours aux algorithmes sont évolutives et n'ont pas encore été découvertes. En revanche, il convient d'évoquer l'émergence de nouveaux enjeux, du fait du déploiement des traitements algorithmiques dans tous les domaines de la société, ce qui constitue une problématique de nature démocratique et juridique.

19. Il ne fait nul doute que la révolution numérique s'accélère. Comme le note Dominique Cardon,

[27] *Ibid*.
[28] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[29] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

« *Avec l'augmentation massive des données numériques, la pertinence des services offerts par les grandes plateformes du Web se concentre de plus en plus dans leur capacité à trier, hiérarchiser, recommander ou personnaliser les informations au terme d'un ensemble de calculs qui n'ont jamais connu un déploiement à si grande échelle. Plus que la simple collecte des données numériques, souvent figurée comme le principal enjeu du Big Data, c'est donc la force et la précision des calculs (notamment leur capacité à effectuer des traitements massifs en temps réel) qui expliquent l'émergence des algorithmes comme une nouvelle figure du pouvoir* »[30].

20. Mais avant d'aborder les géants privés du numérique qui exercent par l'intermédiaire des algorithmes un certain pouvoir, il convient de revenir à la genèse des incidences du numérique sur le droit. Car comme tout fait juridique ayant des conséquences significatives sur la société, il implique ensuite une réaction. Les enjeux spécifiques au numérique ont émergé dès l'après Seconde Guerre mondiale lors de l'avènement de l'ordinateur lorsqu'il est aussi bien apparu comme vecteur de progrès[31] que d'inquiétude, posant nécessairement la question de l'éthique des chercheurs et ingénieurs développant et mettant en œuvre ces nouveaux outils.

21. Accompagnant la sortie du célèbre ouvrage de Norbert Wiener en 1948[32] en France, le journaliste Dominique Dubarle publie dans « Le monde » un article intitulé « *Une nouvelle science : la cybernétique. Vers la machine à gouverner…La manipulation mécanique des réactions humaines créera-t-elle un jour « le meilleur des mondes »* ? »[33]. Le numérique est alors très rapidement associé au pouvoir, et aux incidences qu'il est susceptible d'exercer, y compris pour régir les comportements de la vie en société. Ces réflexions demeurent cependant abstraites et théoriques tant l'informatique n'en est qu'à ses balbutiements.

22. Comme nous l'avons vu, les progrès menés en la matière ont abouti à des ordinateurs de plus en plus performants, mais aussi à des usages plus grand public et à des prix attractifs, ce qui assurera leur démocratisation. Très rapidement, il apparait que le numérique peut

[30] CARDON D., « Le pouvoir des algorithmes », *op. cit.*, p. 63.
[31] Norbert WIENER voyait en la cybernétique une société de l'information transparente au service de la démocratie puisque par nature « *la communication effacerait le secret, qui seul rendit possible le génocide nazi, Hiroshima et le Goulag* », Voir en ce sens, LACROIX G., « Cybernétique et société : Norbert Wiener ou les déboires d'une pensée subversive », *Terminal*, n° 61, 1993.
[32] WIENER N., *La cybernétique, information et régulation dans le vivant et la machine, Seuil*, 2014 [1948].
[33] DUBARLE P., Une nouvelle science : la cybernétique. Vers la machine à gouverner…La manipulation mécanique des réactions humaines créera-t-elle un jour le « meilleur des mondes » ? Les premiers grands relais du cerveau humain - le dépassement du système nerveux – Les processus de la pensée probabiliste – Un prodigieux « jeu de l'homme » - Vers le bonheur (?) statistique des masses, *Le Monde* [en ligne]. 28 décembre 1948. [Consulté le 17 septembre 2020]. Disponible à l'adresse : http://www.nanomonde.org/IMG/pdf/Dubarle_1948.pdf

menacer les libertés du fait de son déploiement. Car la tentation d'automatiser certaines tâches, tout en recoupant toujours plus informations dépassent les capacités humaines sur certains points, et intéressent les gouvernants. L'Etat étant classiquement vu comme une potentielle menace pour les libertés, du fait de la force qu'il peut exercer sur les individus, la modernisation de l'administration par la voie de l'informatique est dans un premier temps observée avec inquiétude. Il s'agit également d'un contexte dans lequel l'action administrative exerce son activité avec une relative opacité[34], ce qui engendre d'importantes suspicions. Cette prise de conscience aboutit assez rapidement à ce que les démocraties libérales se dotent d'un régime juridique pour accompagner cette révolution. Les années soixante-dix marquent cette prise de conscience par le public, notamment en France par l'émoi suscité par l'affaire SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus*)* en 1974[35]. C'est après de nombreuses propositions législatives[36], lors de la décennie soixante-dix, que le gouvernement présentera par la suite un projet de loi aboutissant à la LIL de 1978[37]. Mais l'intelligence du texte est qu'il appréhende et soumet à son régime juridique les traitements de données nominatives mis en œuvre ou allant l'être, aussi bien par la puissance publique que par les acteurs privés. Sa neutralité technique, par le qualificatif de « traitement », permet de saisir les algorithmes informatiques au sens large, sans faire l'erreur de désigner une technologie particulière.

23. L'invention d'internet dans les années soixante, qui n'est qu'un pan du cyberespace, puis du World Wide Web dans les années quatre-vingt-dix et à son accès à grande échelle ne sont de plus pas étrangères à l'immixtion des algorithmes dans tous les domaines de la société, ce qui marque notamment la prééminence des puissances privées au sein de cette sphère, les Etats s'étant en partie désengagés de l'élaboration des normes du cyberespace. Dès 1999, Lawrence Lessig évoque ce retrait de la puissance publique dans l'édification du cyberespace et considère que le code informatique forme du droit à travers l'adage « *code is law* »[38]. Il constate en effet que ce cyberespace illustre le positionnement des puissances se faisant concurrence. Il va même plus loin en affirmant que les architectures[39] développées par les

[34] CHEVALLIER J., « Le mythe de la transparence administrative », *in Information et transparence administratives, PUF*, 1988, p. 239.
[35] Le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) ambitionnait de créer une base de données centralisée regroupant toutes les informations administratives au sujet de la population française par l'intermédiaire d'un identifiant unique. BOUCHER P., « *Affaire SAFARI ou la chasse aux français »*, in *Le Monde*, 21 mars 1974, p. 9.
[36] *Infra.*, n° 44.
[37] Nous reviendrons plus tardivement sur le régime juridique de la LIL de 1978 et ce qu'elle apporte en matière de transparence des traitements algorithmiques.
[38] LESSIG L., *Code and Other Laws of Cyberespace, op. cit.*
[39] *Ibid.*

acteurs du numérique conditionnent l'exercice des droits et libertés de cet environnement, qui lui-même a une incidence sur le terrain classique. C'est donc parce que l'Etat s'est désengagé de l'élaboration des normes du cyberespace, qu'il peine désormais à le réguler. C'était naturellement avant le 11 septembre 2001, et il évoqua dans la révision de son ouvrage en 2006 une résurgence de l'Etat au sein de cette sphère[40].

24. Pierre Musso illustre par ailleurs très bien les manœuvres s'exerçant au sein de cette sphère :

> *« (…) dans le cyberespace, s'échangent des représentations sociales, se confrontent des « cartes mentales » d'acteurs, s'instituent des hiérarchies et des conflits d'image et de réputation. Dans ce second monde s'ordonnent des points de vue d'acteurs, des projets d'action, des conceptions du monde, des imaginaires et des valeurs ; ils s'y rencontrent, collaborent ou s'affrontent* »[41].

25. L'enjeu de la transparence est alors significatif pour observer ces positionnements, et le cas échéant les réglementer. En revanche, cette opacité empêche tout simplement de constater ce qui est, et engendre également des difformités du droit. Son utilisation est naturelle et relève parfois de la servitude volontaire dans une société d'exposition[42], mais le déploiement des nouvelles technologies s'opère souvent sans que les incidences ne soient anticipées. D'une certaine manière, le recours à l'informatique est inéluctable, mais encore faut-il que ce fait juridique soit correctement appréhendé. Ainsi, lorsque les réseaux sociaux font leur apparition, ils exercent une influence sur la société, toujours par la voie de ces algorithmes et des recommandations qu'ils effectuent. Frank Pasquale les qualifie de « *secrets qui contrôlent l'économie et l'information* »[43]. Leur pouvoir est en réalité au service de ceux qui les conçoivent, et est de ce fait corrélativement tout aussi étendu que leur domaine d'intervention. Ils conditionnent désormais l'exercice de la liberté d'expression, ou encore émettent des ordres d'achat ou de vente sur les marchés financiers. Ils sont même susceptibles de menacer l'intégrité physique lorsque nous leur confions nos vies sans contrôle suffisant[44].

---

[40] *Ibid.*
[41] MUSSO P., « Critique de la notion de « territoires numériques », *Quaderni*, n° 66, printemps 2008, p. 25.
[42] HARCOURT B. E., *La société d'exposition. Désir et désobéissance à l'ère numérique*, *Seuil*, 2020, 336 p.
[43] PASQUALE F., *Black Box Society : Les algorithmes secrets qui contrôlent l'économie et l'information*, *FYP éditions*, 2015, 320 p.
[44] Les deux crashs du Boeing 737 max ayant eu lieu en 2018 et 2019 sont imputables à un problème du système de vol automatisé du fait de négligences lors de la procédure de certification par l'administration fédérale américaine de l'aviation civile, autorisant l'appareil sur le marché. Voir en ce sens, DUTHEIL G., Boeing corrige le logiciel de stabilisation de l'avion 737 MAX après les crashs d'Ethiopian Airlines et de Lion Air, *Le Monde* [en ligne]. 28 mars 2019. [Consulté le 25 mai 2020].

26. Mais jusqu'à lors, ils répondaient principalement à des instructions préalablement établies par les développeurs de ces codes informatiques, ce que chamboule notamment la généralisation de l'IA. Antoinette Rouvroy et Thomas Berns constatent dès le début des années 2010 l'émergence d'un nouveau pouvoir statistique[45] et d'une gouvernementalité algorithmique[46], soit *« l'hypothèse d'un gouvernement du monde social fondé sur le traitement algorithmique (automatique) des données massives proliférant de nos comportements plutôt que sur la politique, le droit, les normes sociales, dans une multitude de secteurs d'activité et de gouvernement »*[47]. De plus, Alain Supiot note que la fascination pour les nombres n'est pas contemporaine, et que l'informatique est l'apanage d'une telle tentation, d'une gouvernance par les nombres[48].

27. C'est également parce qu'il est mathématique que l'algorithme bénéficie d'une présomption de rationalité, et donc d'une certaine « scientificité » le rendant difficilement contestable. Ce sentiment est par ailleurs renforcé par la confiance que nous lui attribuons, car le numérique facilite de nombreuses tâches de la vie quotidienne. Comme le fait remarquer le regretté philosophe Bernard Stiegler, « *Aujourd'hui, la prolétarisation, c'est la standardisation des comportements à travers le marketing et les services et la mécanisation des esprits par l'extériorisation des savoirs dans des systèmes tels que ces « esprits » ne savent plus rien de ces appareils de traitement de l'information qu'ils ne font plus que paramétrer : c'est précisément ce que montre la mathématisation électronique de la décision financière. Or cela affecte tout le monde : employés, médecins, concepteurs, intellectuels, dirigeants. De plus en*

Disponible à l'adresse : https://www.lemonde.fr/economie/article/2019/03/28/boeing-a-modifie-le-logiciel-de-stabilisation-de-son-737-max_5442598_3234.html

[45] ROUVROY A., BERNS T., « Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps « numériques »… », *Multitudes*, n° 40, 2010/1, p. 88 à 103.

[46] Comme l'indiquent Antoinette Rouvroy et Thomas Berns « *Le propre de ce qu'on appelle le machine learning est somme toute de rendre directement possible la production d'hypothèse à partir des données elles-mêmes. De la sorte, nous nous trouvons à nouveau face à l'idée d'un savoir dont l'objectivité pourrait paraître absolue, puisqu'il serait éloigné de toute intervention subjective (de toute formulation d'hypothèse, de tout tri entre ce qui est pertinent et ce qui ne serait que du « bruit », etc.). Les normes semblent émerger directement du réel lui-même. Ces normes ou ces « savoirs » ne sont cependant constitués « que » de corrélations, ce qui n'est pas en soi un problème, si l'on n'oublie pas, c'est la condition même d'un ethos scientifique et d'un ethos politique, de conserver un doute, d'entretenir une méfiance par rapport à la suffisance des corrélations, de maintenir la distinction entre corrélation et cause, de se méfier des « effets » autoperformatifs des corrélations (leur capacité rétroactive), d'éviter que des décisions produisant des effets juridiques à l'égard de personnes ou les affectant de manière significative ne soient prises sur le seul fondement d'un traitement de données automatisé, et de considérer que le propre de la politique (notamment le souci d'une mutualisation des risques) est de refuser d'agir sur la seule base de corrélations. Il semble important de rappeler ceci face à l'évolution vers un monde qui paraît de plus en plus fonctionner comme s'il était constitué lui-même de corrélations, comme si celles-ci étaient ce qu'il suffit d'établir pour en assurer le bon fonctionnement* », ROUVROY A., BERNS T., « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux*, 2013/1, n° 177, p. 163 à 196.

[47] SALMON C., « « Bojo le clown » et son ingénieur magicien », in *Médiapart*, 26 janvier 2020.

[48] SUPIOT A., *La gouvernance par les nombres*, Cours au Collège de France, Poids et mesures du monde, *Fayard*, 2015, p. 41 et 43.

plus d'ingénieurs participent à des processus techniques dont ils ignorent le fonctionnement »[49].

28. Certains qualifient même le recours aux traitements algorithmiques de « *coup de data permanent* »[50], car ces derniers produiraient notamment des effets normatifs imperceptibles[51]. Même si nous nous focaliserons essentiellement sur la problématique de l'intelligibilité des algorithmes qui parfois peuvent se mouvoir en norme, lorsque leurs utilisations répondent parfaitement à ce pourquoi ils ont été conçus, c'est leur déploiement qui modifie sans que nous nous en rendions nécessairement compte notre tradition juridique et engendre des difformités du droit[52]. Une surveillance toute particulière doit donc leur être apportée pour anticiper et constater ces changements. L'avènement de grandes plateformes numériques, dont certaines sont en situation quasi monopolistique notamment car les services proposés peuvent pour certains paraître aujourd'hui indispensables à bien des égards dans notre vie quotidienne, façonnent également le monde par l'intermédiaire de ces nouveaux outils. Les conditions générales d'utilisation de ces plateformes constituent un droit alternatif de nature autre qu'étatique[53], et dont l'algorithme se retrouve être la norme d'application. L'efficacité des algorithmes offre de nouvelles perspectives pour influencer le plus possible les consommateurs dans leurs achats par le truchement de profilages très sophistiqués. Shoshana Zuboff qualifie même ce phénomène de nouvelle étape du capitalisme par la surveillance privée à des fins économiques[54].

29. Il existe également un phénomène à ne pas négliger : le fait que dans certains cas, l'Etat et les intérêts privés convergent. Au-delà des relations contractuelles, l'Etat incite un rôle actif des entreprises privées. La crise sanitaire due à la pandémie de Covid-19 que nous traversons a

---

[49] JOIGNOT F., Le Philosophe Bernard Stiegler est mort. Deux grands entretiens pour rappeler sa pensée sur la technique, l'urgence écologique, le « care », le « psycho-pouvoir », la perte du sens de nos vies, *Blog Le Monde* [en ligne]. 21 février 2011. [Consulté le 23 novembre 2019]. Disponible à l'adresse : http://fredericjoignot.blog.lemonde.fr/2011/02/21/nous-vivons-un-extreme-desenchantement-un-entretien-avec-le-philosophe-bernard-stiegler/

[50] « *Si la loi des algorithmes semble constituer une réalité, cette réalité appelle déjà la méfiance en raison du fait que seule une faible partie de ceux dont les conduites sont régies par cette « loi » en ont conscience et, par suite, peuvent poser sur elle un regard critique et sur leurs choix et comportements un regard réflexif. (…). La loi des algorithmes, ensemble de normes tacites, inexprimées, formalisées seulement dans du code, est donc associée à une opacité peu satisfaisante, quel que soit le contenu et la portée des normes en cause. (…) Cela aboutit à des boîtes « noires » qui enregistrent des données et les traitent, dont on peut observer et subir les effets, mais sans en comprendre le fonctionnement* », BARRAUD B., « Le coup de data permanent : la loi des algorithmes », *Revue des droits et des libertés fondamentaux*, Chron. n° 35, 2017, [en ligne]. [Consulté le 3 mars 2020]. Disponible à l'adresse : http://www.revuedlf.com/droit-fondamentaux/le-coup-de-data-permanent-la-loi-des-algorithmes/

[51] *Ibid*.

[52] Voir notamment en ce sens, DUCLERCQ J-B., « Les effets de la multiplication des algorithmes informatiques sur l'ordonnancement juridique », *Communication Commerce Electronique*, n° 11, étude 20, 2015 ; DUCLERCQ J-B., « Les algorithmes en procès », *RFDA*, 2018, p. 131.

[53] ITEANU O., *Quand le digital défie l'Etat de droit*, *Eyrolles*, 2016.

[54] ZUBOFF S., *L'âge du capitalisme de surveillance. Le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, *Zulma*, 2020, 864 p.

par ailleurs renforcé ce processus[55] en ce que des technologies privées se sont de plus substituées à l'incapacité des gouvernants et de l'administration à utiliser leurs propres outils, ce qui n'est pas sans risque également sur le contrôle qu'effectue l'Etat sur ces technologies.

30. Cette féodalité moderne[56], pour notamment y faire respecter le droit, soumet l'application des normes et l'exercice des libertés à des prestataires privés qui recourent pour ce faire à des traitements algorithmiques comme sur les réseaux sociaux par exemple, avec des obligations de suppressions de certains contenus dans des délais imposant toujours plus d'automatisation. Une telle allégeance opère un transfert de l'effectivité du droit par des arbitrages algorithmiques effectués par ces géants transnationaux, alors que la sphère publique n'a nullement procédé à leur élaboration. L'Etat n'est pas en reste puisqu'en recourant massivement aux algorithmes informatiques, y compris à des fins de modernisation, en particulier à travers des doctrines de *new public management*[57], ce sont les administrés qui subissent l'opacité, sans que l'administration ne se soucie toujours d'expliquer les processus menant à ses décisions comme l'a parfaitement démontré l'affaire « *Admission Post Bac* » (APB)[58].

31. La corrélation de tous ces phénomènes nous amène à ce que les algorithmes constituent sur bien des sujets de véritables bombes à retardement[59]. Mais pour pouvoir rattacher un fait juridique au régime qui lui serait applicable, ou le cas échéant à de nouvelles règles, encore faut-il pouvoir observer le comportement de ces algorithmes et que le droit le permette. A défaut, nous risquerions même un ordre juridique inopérant, qui est pourtant l'émanation de l'autonomie des citoyens en démocratie[60], et qui serait concurrencé par des normes algorithmiques produites par d'autres acteurs et appliquées de manière opaque. Qu'il s'agisse de la surveillance effectuée pour le compte d'Etat par la voie des géants du numérique[61] ou les fraudes à des normes environnementales comme dans l'affaire du *dieselgate*[62], les incidences

[55] CLUZEL-METAYER L., « La datasurveillance de la Covid-19 », *RDSS*, 2020, p. 918.
[56] Selon Alain Supiot il existe actuellement un processus d'inféodation des personnes. SUPIOT A., *La gouvernance par les nombres*, *op. cit*., p. 310.
[57] CHEVALIER J., « Le droit administratif vu de la science administrative », *AJDA*, 2013, p. 401 à 403.
[58] *Infra*., n° 437 et s.
[59] O'NEIL C., *Algorithmes. La bombe à retardement*, *Les arènes*, 2016, 340 p.
[60] *Infra*., n° 634.
[61] ERTZSCHEID O., *L'appétit des géants. Pouvoir des algorithmes, ambitions des plateformes*, *C&F éditions*, 2017, 384 p.
[62] A titre d'exemple, l'affaire du *dieselgate* a mis au jour un programme informatique modifié implanté dans un véhicule automobile afin de faire paraître une conformité aux réglementations européennes et américaines lors des essais d'homologation. Le logiciel était capable de déceler lorsque le véhicule se retrouvait en phase d'évaluation de ses émanations Nox[62], afin qu'il les réduise par rapport à un usage classique. Voir en ce sens, MANDARD, S., Cinq ans après le « Dieselgate », les constructeurs bénéficient toujours d'une « clause de confidentialité », *Le Monde.fr* [en ligne]. 18 septembre 2020 [Consulté le 14 décembre 2020] : https://www.lemonde.fr/planete/article/2020/09/18/dieselgate-cinq-ans-apres-la-transparence-fait-toujours-defaut-sur-les-emissions-de-gaz-polluants_6052649_3244.html

de l'informatique nous parviennent essentiellement par les révélations obtenues par la voie de presse, illustrant à quel point le numérique est pernicieux, y compris parce qu'il est difficilement observable.

II - Vers un principe de transparence des traitements algorithmiques

32. L'objet de la présente thèse n'est pas de répertorier les avantages induits par le numérique, mais en quoi un principe de transparence des traitements algorithmiques permettrait de cartographier les puissances s'opposant au sein du cyberespace en vue d'une meilleure effectivité des droits et libertés ainsi qu'une plus grande efficacité de l'ordre juridique, aujourd'hui menacés. Pour ce faire, c'est l'étude des techniques juridiques concourant à la transparence des traitements algorithmiques qui attire notre attention (A), et en quoi il convient qu'un tel principe bénéficie d'une unité conceptuelle permettant sa reconnaissance (B).

A - Etude des techniques juridiques participant à la transparence des traitements algorithmiques

33. Il existe une ambivalence concernant les nouvelles technologies de l'information et de la communication (NTIC) puisqu'elles sont porteuses d'espoir dans l'accès et la diffusion de l'information, offrant un meilleur contrôle de l'action publique. Elles sont donc susceptibles par nature de poursuivre la transparence de nombreux processus décisionnels[63]. Certains prêtent même au numérique une nouvelle façon de participer à la démocratie[64]. Pourtant, il s'avère que son déploiement implique comme nous l'avons vu de l'opacité qui mérite d'être corrigée par des ajustements juridiques.

34. D'importants travaux ont été menés sur le concept même de transparence. L'objectif de la présente thèse est alors essentiellement d'en évaluer le périmètre, la nature et le degré tels que les régimes juridiques l'ont institué, mais aussi comment il convient d'améliorer les techniques juridiques censées la réaliser dans l'environnement numérique. Jean-François Kerléo le notait déjà

> « *la transparence sera identifiée comme un terme du discours juridique : il ne peut y avoir de transparence sans la présence du mot dans le discours. On verra que le*

[63] *Supra*., n° 20.
[64] Certains auteurs pensent en effet que les nouveaux outils numériques peuvent modifier la nature de la participation citoyenne, ce que nous ne nions pas, mais cela n'est pas l'objet de l'actuelle démonstration.

mot sert le plus souvent à désigner d'autres objets juridiques tels que le droit à l'information, l'obligation de motivation des actes administratifs ou encore les règles de publicité qui les régissent »[65].

35. Pour rendre compte au mieux de ce qu'est la transparence des traitements algorithmiques, nous avons envisagé une approche essentiellement chronologique des régimes juridiques traitant de cette question puisqu'ils répondent, à une réaction à un fait juridique particulier qui suit l'histoire et les incidences de l'informatique, et le plus souvent la rencontre avec la culture juridique de la transparence existante (Partie I). Il apparaît donc parfois que les techniques juridiques servant cette transparence sont dans le prolongement de la branche du droit concernée ou de son secteur d'application en suivant la communication de documents traditionnels papiers par exemple. La transparence n'est pas toujours utilisée dans le discours juridique, raison pour laquelle nous avons tout de même choisi ce terme car il est le plus englobant possible pour faire état de l'ensemble des techniques utilisées, et ce quand bien même elle est au service d'objectifs différents comme la publicité, l'intelligibilité, pour le droit public, ou bien de la bonne foi et la loyauté pour les rapports contractuels. En ce sens, il n'existe pas encore un principe général de transparence des traitements algorithmiques, ce que nous regrettons par ailleurs, mais l'ensemble des règles juridiques étudiées illustrent une réaction de plus en plus forte de l'Etat afin de recouvrer sa puissance originelle, sa plus grande force[66], concurrencée par des opérateurs économiques, car il s'agit surtout d'un enjeu de souveraineté et de respect des libertés.

36. Retenons de la transparence qu'il s'agit de « *la qualité de ce qui est psychologiquement ou intellectuellement facilement pénétrable* »[67]. Elle est en droit public associée à la démocratie administrative[68] et constitutionnelle, et elle participe de ce fait à un « *processus de*

---

[65] KERLEO J-F., *La transparence en droit, Recherche sur la formation d'une culture juridique*, Bibliothèque des thèses, *Mare & Martin*, 2015, p. 26.
[66] HERAUD G., « La validité juridique », *in Mélanges Maury*, *Dalloz*, 1960, p. 479 à 480.
[67] JEGOUZO Y., « Le droit à la transparence administrative », *Etudes et documents du Conseil d'Etat*, n° 43, *La Documentation française*, p. 199.
[68] Comme l'indique Julie Arroyo, « *la transparence constitue une condition de réalisation de la démocratie administrative. Sa promotion répond à la crise du système démocratique fondé sur le système représentatif. La légitimité de l'administration apparaît désormais moins fondée sur le principe de séparation des pouvoirs, l'élection et le « mythe » de la représentation reposant sur la concordance des volontés des gouvernés et des gouvernants que sur le pluralisme et le contrôle exercé directement par les citoyens sur le processus politique et administratif. Cette vision renouvelée de la démocratie impose de substituer au modèle administratif classique reposant sur la hiérarchie, le secret et l'assujettissement de l'administré, un modèle d'administration plus ouvert, rééquilibré au profit de l'administré, fondé sur l'information, le dialogue et sa participation. La mise en place de la transparence administrative participe à la réalisation de ces nouvelles exigences démocratiques en assurant l'information des administrés, cette information leur permettant de se livrer à une forme de contrôle du pouvoir ainsi que, dans une certaine mesure, d'y participer.* », ARROYO J., Un droit à l'oubli dans le champ des documents administratifs ?, *in* DECHENAUD D. (dir.), *Le droit à l'oubli numérique. Données nominatives - approche comparée*, *Larcier*, 2015, [en ligne]. [Consulté le 21 décembre 2020]. Disponible à l'adresse : http://www.revuedlf.com/droit-administratif/un-droit-a-loubli-dans-le-champ-des-documents-administratifs/#return-note-6120-111

décomposition de l'action publique »[69]. Elle est donc aussi un important principe support au service de l'effectivité d'autres principes ou droits et libertés[70].

37. A cet égard, il est toutefois intéressant de noter que le numérique a des incidences sur l'Etat de droit. Cet Etat de droit est appréhendé de différentes manières. D'un point de vue formel cette notion renvoie, comme l'avait indiqué Raymond Carré de Malberg, à cet « *État qui, dans ses rapports avec ses sujets et pour la garantie de leur statut individuel, se soumet lui-même à un régime de droit, et cela en tant qu'il enchaine son action sur eux par des règles, dont les unes déterminent les droits réservés aux citoyens, dont les autres fixent par avance les voies et moyens qui pourront être employés en vue de réaliser les buts étatiques : deux sortes de règles qui ont pour effet commun de limiter la puissance de l'État, en la subordonnant à l'ordre juridique qu'elles consacrent* »[71].

38. A cet « *Etat lié par le droit* »[72] se pose naturellement la question de son contenu. C'est par le respect du formalisme de l'Etat que la protection des droits et libertés est rendue possible. Ainsi, Jacques Chevallier précise que « *le perfectionnement de l'architecture formelle n'a pas de signification en soi, mais seulement si elle est mise au service de certaines fins, à savoir la protection des droits et libertés, qui constituent en fin de compte la valeur suprême* »[73].

39. Qu'il s'agisse de l'Etat de droit dans son acception formelle ou matérielle, l'intervention étatique n'est pas absolue. D'une part, par l'intermédiaire de la Constitution et par les habilitations qu'elle confère, les pouvoirs constitués sont encadrés dans le but de limiter leurs actions, ce qui peut être effectué notamment par les individus par la voie juridictionnelle. Il s'agit de poursuivre un intérêt de lutte contre l'arbitraire vis-à-vis des personnes, et dont le risque est inhérent à la puissance de l'Etat. Lorsque l'Etat recourt aux traitements algorithmiques à des fins d'une plus grande efficacité du droit, c'est une nouvelle norme utilisée dont la publicité n'est pas toujours assurée pouvant être constitutive d'un arbitraire dont la transparence de ces nouveaux outils participe à l'amoindrissement de ce risque. D'autre part, dans la philosophie libérale de l'Etat de droit, l'interventionnisme étatique est limité notamment pour protéger les droits et libertés du marché, à moins que celui-ci n'engendre des troubles à

[69] CHEVALLIER J., « Les fondements du droit administratif à l'épreuve de l'Europe », *in* RAIMBAULT P. (dir.), *La puissance publique à l'heure européenne*, *Dalloz*, 2006, p. 47.
[70] Comme l'indique Jennifer Marchand la transparence est un « *principe support des droits fondamentaux* ». Voir en ce sens, MARCHAND J., « Réflexion sur le principe de transparence », *RDP*, n° 3, 2014, p. 677.
[71] CARRE DE MALBERG R., *Contribution à la théorie générale de l'Etat*, *Sirey*, 1920, t. 1, p. 489.
[72] REDOR-FICHOT M.-J., *De l'Etat légal à l'Etat de droit. L'évolution des Conceptions de la Doctrine Publiciste Française, 1879-1914, Presses Universitaires d'Aix-Marseille*, 1992, p. 294.
[73] CHEVALLIER J., *L'Etat de droit*, *LGDJ*, 2017, p. 109.

l'ordre public, y compris de nature économique. En effet, l'Etat est une institution au service des citoyens de par la titularité de la souveraineté, raison pour laquelle la transparence publique permet un contrôle de l'action des gouvernants par les gouvernés dans le cadre de la sphère politique, principe inhérent à la démocratie représentative. Ainsi, comme l'indique Jean-François Kerléo, « *la transparence est réflexion de l'Etat sur lui-même. Dès lors l'idée de transparence s'intercale dans les grandes constructions justificatrices du pouvoir, puisqu'on la retrouve associée à l'architecture du droit et à ses représentations (Nation, Etat de droit, publicité, etc)* »[74].

40. Puis, c'est également un enjeu de transparence de l'action administrative mettant en œuvre les politiques publiques afin qu'elle ne détourne pas le cas échéant l'exorbitance à d'autres fins que l'intérêt général[75]. La puissance de l'Etat elle doit aussi être mise au service d'une régulation du marché[76] par l'intermédiaire d'obligations positives lorsque celui menace l'autonomie des citoyens en démocratie. Or, ce sont aussi les opérateurs économiques qui aujourd'hui concurrencent cette plus grande force par leurs algorithmes, nécessitant une intervention étatique, notamment pour réguler la manière dont ils conditionnent par exemple l'exercice des droits civils et politiques telle que la liberté d'expression sur les réseaux sociaux par exemple. C'est également cette ambivalence que nous serons amenés à traiter et à résoudre afin que la transparence de l'environnement numérique puisse être assurée par l'Etat tout en permettant la protection des droits et libertés.

41. C'est donc l'observation de leur comportement qui empêche la saisie des faits juridiques induits par le numérique, et par là même leur régulation. Au même titre que les individus, ce sont aussi parfois les Etats[77] qui apparaissent vulnérables[78], et particulièrement ceux n'élaborant pas les technologies qu'ils utilisent.

42. Toutefois, et c'est l'intérêt même de cette thèse, la démarche est de déduire des principaux régimes juridiques traitant des traitements algorithmiques, ce qu'ils nous disent de cette notion afin de connaître ce qui la compose, et si l'approche est suffisante au regard des

---

[74] KERLEO J-F., *La transparence en droit, Recherche sur la formation d'une culture juridique*, *op. cit.*, p. 159-160.
[75] En ce sens, l'article 15 de la DDHC de 1789 précise que « *La Société a le droit de demander compte à tout Agent public de son administration* ».
[76] A cet égard, même les théoriciens du libéralisme économique tel que Adam Smith considèrent que le marché se doit d'être transparent afin qu'il se réalise par une concurrence pure et parfaite.
[77] CHASSIN C-A., KORSAKOFF A., MAUGER-VIELPEAU L., « La vulnérabilité des migrants », *Les Cahiers de la Recherche sur les Droits Fondamentaux*, n°18, 2018, p. 55.
[78] Nous l'entendons comme « *toute fragilité morale ou matérielle, individuelle ou sociale à laquelle une personne se trouve exposée* » induite par les techniques informatiques dans notre espèce. Voir en ce sens, ROUX-DEMARE F.-X., « La notion de vulnérabilité, approche juridique d'un concept polymorphe », *Les cahiers de la justice, Vulnérabilités*, n° 4, 2019, p. 619 à 630.

objectifs poursuivis. Sans suspens, il est possible de dupliquer les réflexions de Jean-François Kerléo à la matière algorithmique, considérant qu'elle « *constitue un ensemble de techniques juridiques contenant aussi bien des normes juridiques que des représentations idéales fondées sur une réévaluation du rapport savoir/pouvoir en renvoyant à un processus unilatéral ou multilatéral de communication d'informations dans un but d'efficacité ou de légitimation* »[79].

43. Bien que cette thèse soit avant tout publiciste, le fondement des règles de transparence implique également l'étude de certaines règles juridiques générales du droit privé. Cette transparence repose aujourd'hui sur des obligations d'information et de contrôle, dont le degré et la nature diffèrent cependant d'un régime juridique à l'autre, notamment car les objectifs poursuivis ne sont pas toujours identiques. Nous avons fait le choix d'apporter une réflexion particulière sur le droit national bien que ce dernier soit directement influencé par le droit européen et implique également son étude. En attendant l'adoption des nouvelles propositions de règlement en droit de l'Union européenne traitant spécifiquement de la transparence des traitements algorithmiques, participant par ailleurs à une plus grande autonomie de ce principe du fait d'une prise en considération de l'environnement numérique, force est de constater que pour l'heure le droit français est celui le plus développé en la matière, raison pour laquelle il nous semble opportun d'étudier les techniques juridiques concourant à cette transparence.

44. Les premières discussions parlementaires relatives à la régulation de l'informatique en France remontent à Michel Poniatowski lorsque celui-ci dépose en 1970 une proposition de loi à l'Assemblée nationale en vue de la création d'un tribunal et d'un comité de surveillance de l'informatique[80]. C'est la première réaction politique au fait juridique constaté nationalement[81]. S'en suivront tout le long de cette décennie des discussions amenant à la LIL de 1978. En tant qu'œuvre libérale, l'objectif de cette loi est avant tout d'assurer à la fois le respect de la vie privée, mais aussi de participer à la réalisation d'une démocratie administrative. Pour ce faire, et nous y reviendrons en détail dans le cadre de ces travaux, « *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* »[82], ce qui fonde un droit à l'information. De nombreuses informations doivent également être communiquées par le responsable de

[79] KERLEO J-F., *La transparence en droit, Recherche sur la formation d'une culture juridique*, *op. cit.*, p. 895.
[80] PONIATOWSKI M., proposition de loi tendant à la création d'un comité de surveillance et d'un tribunal de l'informatique n° 1454, 4eme législature, enregistré à la Présidence de l'Assemblée nationale le 25 novembre 1970.
[81] Bien que nous fassions référence au droit régional et international, nous ne le ferons toutefois pas dans une approche comparatiste.
[82] Art. 3 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

traitement à la personne concernée lors de la collecte de ses données nominatives[83]. Enfin, un droit d'accès à ses informations nominatives[84] dans un « *langage clair* » conditionnera également le cas échéant le droit d'opposition à un traitement[85] ou leur rectification[86].

45. Puis, au-delà des différentes modifications de la LIL qui s'en suivirent, le droit de l'Union européenne, par la directive 95/46/CE comportait une occurrence à la transparence, dans son préambule[87], qui n'avait certes qu'une valeur interprétative, ce qui laissait à penser que ce principe n'était pas central, et qui contraste aujourd'hui avec le caractère désormais incontournable de la transparence du Règlement Général sur la Protection des Données (RGPD)[88] qui a abrogé cette dernière. Le groupe de travail « article 29 » (G29)[89] rappelle dans ses lignes directrices[90] que le principe de transparence est un dérivé du principe d'équité se trouvant à l'article 8 de la Charte des droits fondamentaux de l'Union européenne[91]. Il concourt donc à l'intelligibilité de ce qui est « *applicables aux citoyens en leur permettant de comprendre et, au besoin, de contester lesdits processus* »[92]. Toutefois, à défaut d'obtenir une définition précise de la transparence, parce qu'elle n'est nullement définie par le RGPD[93], il convient d'étudier au regard des dispositions du RGPD quelle est sa nature et son degré. C'est donc un principe de transparence en droit des données personnelles qui se retrouvera notamment au cœur d'un changement de paradigme important apporté par cette règlementation puisqu'il

[83] *Ibid*., art. 27.
[84] *Ibid*., art. 34.
[85] *Ibid*., art. 26.
[86] *Ibid*., art. 36.
[87] 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 63 : « *considérant que ces autorités doivent être dotées des moyens nécessaires à l'exécution de leurs tâches, qu'il s'agisse des pouvoirs d'investigation et d'intervention, en particulier lorsque les autorités sont saisies de réclamations, ou du pouvoir d'ester en justice; qu'elles doivent contribuer à la transparence du traitement de données effectué dans l'État membre dont elles relèvent;* ».
[88] 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) dit RGPD.
[89] Le groupe de travail « article 29 » est un organe consultatif indépendant dont les missions sont relatives à la protection des données à caractère personnel. Il a été instauré par la 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. Il réunit les autorités de contrôle, comme la CNIL, des Etats membres de l'Union européenne. Avec l'entrée en application du RGPD en 2018, il a depuis été remplacé par le Comité Européen de la Protection des Données (CEPD).
[90] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018, p. 5.
[91] En effet, l'article 8 de la Charte des droits fondamentaux de l'Union européenne n'évoque pas le principe de transparence, mais la loyauté des traitements, c'est-à-dire la notion d'équité. Nous aborderons la notion de loyauté spécifiquement dans le chapitre II de ce titre.
[92] G29, lignes directrices au sens du RGPD du 11 avril 2018, p. 5.
[93] Selon le considérant 39 du RGPD qui n'a qu'une valeur interprétative, « *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. Ce principe vaut, notamment, pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement.* ».

conditionnera le consentement d'une personne physique à un traitement[94]. Pour ce faire, et sauf exceptions[95], le responsable de traitement devra communiquer de nombreuses informations[96] « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* »[97], et un droit d'accès à ses données personnelles[98] afin que la personne concernée y apporte le cas échéant son adhésion, son droit d'opposition ou de rectification ou d'effacement, en plus d'un droit à l'explicabilité pour les décisions exclusivement fondées sur un traitement de données personnelles[99]. Un protocole additionnel à la Convention européenne des droits de l'homme reprendra également un tel principe[100].

46. Malgré ces avancées, bien qu'imparfaites à certains égards toutefois, les limites de la LIL se faisaient ressentir, et ce même si elles étaient applicables aux responsables de traitement privés qui ont été amenés à prendre une part de plus en plus importante par rapport à l'Etat. Et alors que l'informatique prenait une ampleur conséquente dans la société, et que de nombreuses décisions étaient prises par ou sur le fondement de traitements algorithmiques à l'encontre de personnes morales, et sans que des données personnelles ne soient par ailleurs toujours manipulées, de nouvelles dispositions s'imposaient. Ainsi, la LRN[101] de 2016 marque une étape importante en ce qu'elle appréhende l'introduction de nouvelles règles relatives à la transparence des algorithmes aussi bien du secteur public que privé. Un droit spécial privé des algorithmes a alors également fait son apparition pour saisir la problématique des plateformes numériques, tout en prenant en compte des règles particulières pour toute personne faisant l'objet d'une décision administrative individuelle prise sur le fondement d'un traitement algorithmique.

47. Dans le premier cas, les techniques juridiques déployées pour parvenir à la transparence de ces traitements repose sur le fait que les plateformes en ligne[102] ont pour obligation de délivrer une information pré-contractuelle « *loyale, claire et transparente* » aux consommateurs[103]. La loyauté en en ce sens est régulièrement combinée à la transparence

[94] NETTER E., « A quoi sert le principe de transparence en droit des données personnelles ? », *Dalloz IP/IT*, 2020, p. 611.
[95] *Infra*., n° 93 et s.
[96] Art. 13 et 14 du RGPD. Pour plus de précisions, *Infra.*, n° 93 et s.
[97] Art. 12 du RGPD.
[98] Art. 15 du RGPD.
[99] Art. 22 du RGPD.
[100] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 18 mai 2018. Ce protocole modernise la convention n° 108 du 18 janvier 1981 du Conseil de l'Europe du même nom.
[101] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
[102] Il s'agit des plateformes en ligne mentionnées à l'article L. 111-7 I du Code de la consommation. *Infra.*, n° 266 et s.
[103] Le droit de l'Union est aussi intervenu de même entre professionnels compte tenu du rôle de plus en plus monopolistique des plateformes en ligne par une plus grande information. Voir en ce sens le Règlement UE 2019/1150 du Parlement Européen

puisqu'en effet, et comme l'indique le Conseil National du numérique (CNn), « *pour la plateforme, ce principe implique premièrement et d'une manière générale la transparence du comportement de la plateforme, condition pour s'assurer de la conformité entre la promesse affichée du service et les pratiques réelles* »[104].

48. De l'autre, et dans la continuité de la doctrine de la CADA[105] reprise par la jurisprudence des juridictions administratives[106], le code source des logiciels utilisé par l'administration était assimilé à un document administratif communicable. Il s'agit de la continuité du droit d'accès aux documents administratifs telle que prévue par la loi n° 78-753 du 17 juillet 1978. Le recours d'une mention explicite dans les décisions administratives individuelles prises sur le fondement d'un traitement algorithmique[107] a été ajouté et marque également la possibilité pour l'administré, qu'il soit une personne physique ou non, de prendre connaissance des principales caractéristiques du traitement[108]. Ainsi, ces techniques juridiques, ces obligations de la part de l'administration, concourt notamment de fait à des impératifs de transparence de l'action administrative instituée par les exigences de motivation des actes administratifs[109]. Il apparaît alors que ce mouvement de prise en considération des algorithmes déploie de nouvelles obligations juridiques pour servir la transparence administrative[110]. Parallèlement l'administration est aussi tenue de publier « *en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles* »[111].

49. L'Etat n'est toutefois pas en reste puisque craignant le recours aux traitements algorithmiques parce qu'il est concurrencé par de nombreux opérateurs économiques ayant des incidences sur les personnes et la société, si ce n'est sur son existence même, il exige en retour à leur encontre des obligations afin de préserver l'ordre public. Tel est par exemple le cas de la lutte contre la manipulation de l'information diffusée sur les plateformes pouvant menacer la

et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne.

[104] CONSEIL NATIONAL DU NUMERIQUE, Projet de loi pour une République numérique au sujet de la loyauté des plateformes, CNNumérique.fr [en ligne]. 2015. [Consulté le 23 avril 2020]. Disponible à l'adresse : https://cnnumerique.fr/files/uploads/2015/11/CNNum_Fiche_Loyaute-des-plateformes.pdf

[105] CADA, avis n° 20144578 du 8 janvier 2015.

[106] TA de Paris, 10 mars 2016, M. X, n° 1508951.

[107] L. 311-3-1 du Code des relations entre le public et l'administration (CRPA).

[108] *Ibid*.

[109] Loi n° 79-587 du 11 juillet 1979 relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public.

[110] Les lois de 1978 et 1979 évoquées constituent « une communauté d'inspiration : ces trois lois ont pour objet d'améliorer et de rénover les rapports de l'administration et des citoyens en donnant à ceux-ci des droits nouveaux d'accès l'information ; elles visent à assurer plus d'ouverture et de transparence aux services publics », LASSERE B., LENOIR N, STIRN B, *La transparence administrative*, *PUF*, 1987, p. 3 à 4.

[111] Art. L. 312-1-3 du CRPA.

sincérité de scrutins[112] ou en matière de lutte contre les contenus à caractère terroriste en ligne[113]. L'économie est aussi susceptible de vaciller par une importante immixtion des algorithmes dans le secteur financier induisant des manipulations ou des erreurs[114], raison pour laquelle il exige des informations particulières de la part de ces acteurs concernant le recours aux algorithmes.

50. Il existe également des domaines dans lesquels des techniques juridiques de transparence sont utilisées plus sporadiquement comme en médecine dans la mesure où les algorithmes sont amenés à jouer un rôle de plus en plus important dans la prévention, le diagnostic et les soins par des techniques auto-apprenantes. Un droit à l'information des patients est alors étendu[115] à ces dispositifs. Mais surtout, les concepteurs de ces technologies doivent expliquer le fonctionnement du traitement aux professionnels de santé les utilisant[116]. Il en est de même en droit social lorsque l'évaluation des candidatures ou d'un salarié fait intervenir un traitement algorithmique[117].

51. Il apparait donc que la transparence des algorithmes vient servir une culture juridique déjà existante, allant de la protection des droits et libertés, et de l'ordre juridique, y compris pour la sauvegarde de l'Etat. Mais toutes les dimensions ne sont toujours pas appréhendées par le droit tel que la gouvernementalité algorithmique[118], et il existe d'un point de vue juridique d'importants îlots d'opacité empêchant d'observer les incidences de nombreux traitements algorithmiques. Cela est parfois compréhensible puisqu'il ne sera pas possible d'exiger une transparence pour tout, et notamment car la transparence, y compris en démocratie, n'offre pas que des bénéfices car d'autres droits et libertés, et principes, doivent être conciliés avec cet impératif[119].

52. Néanmoins, même dans les régimes juridiques identifiés, le secret y est culturel et protège bien trop souvent le libéralisme économique, et ce parfois au détriment de l'effectivité

[112] Loi n° 2018-1202 du 22 décembre 2018 *relative à la lutte contre la manipulation de l'information.*
[113] Voir par exemple en ce sens, Règlement (UE) du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion de contenus à caractère terroriste en ligne. *Infra*., n° 347 et s.
[114] Règlement (UE) No 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission.
[115] Art. L. 4001-3 du Code de la santé publique crée par la loi n° 2021-1017 du 2 août 2021, *Infra.*, n° 381 et s.
[116] *Ibid*.
[117] Art. L. 1222-4 et L. 1221-9 du Code du travail *Infra.*, n° 360 et s.
[118] *Infra*., n° 647 et s.
[119] CARCASSONNE G., « Le trouble de la transparence », *Pouvoirs*, n° 97, 2001, p. 17 à 23. ; LEQUESNE ROTH C., « La transparence : vice ou vertu de la démocratie ? », in RIDEAU J. (dir.), *La transparence dans l'Union européenne, Mythe ou principe juridique*, 1998, *LGDJ*, p. 11.

d'autres libertés. Lorsqu'il s'agit de l'Etat, la transparence se heurte classiquement aux intérêts de la Nation, et le droit d'accès à ses données personnelles, s'il est prévu, va pouvoir s'effectuer que par un tiers de confiance. Et dans d'autres hypothèses, le secret y fait totalement écran, y compris lorsqu'il s'agit des acteurs économiques, la communication d'informations au sujet des traitements devient difficile si ce n'est inexistante.

53. De plus, et nous le verrons, la nature et le degré de la transparence exigée ne semblent pas toujours être les plus opportunes avec l'objectif qui est poursuivi par les corps constitués de l'Etat. A titre d'exemple, sous couvert de la communication de certains documents portant sur ces algorithmes, rien ne prouve qu'il s'agît dudit algorithme en fonctionnement.

54. Il est toutefois à noter que de nombreux régimes juridiques ont été adoptés sur cette question lors de la précédente décennie et que des propositions, y compris de règlements européens, viendront nourrir ces réflexions.

B - Un principe en manque d'unité conceptuelle

55. Guy Braibant notait que le droit à la transparence, en ce qu'il concourt à la démocratie administrative, y compris par le droit à l'information, était constitutif d'un droit de l'homme de troisième génération[120]. Bien que Jean Rivero le considérait en revanche « trop vague »[121], nous soutenons qu'il en a désormais la consistance pour y prétendre sous forme d'un principe pouvant le cas échéant se mettre en œuvre par une pluralité de techniques juridiques, y compris de droits. Une telle reconnaissance impliquerait une juridicité dont l'invocation devant les juridictions serait certaine puisqu'un « *principe s'analyse comme une contrainte, ce qui est le propre de toute norme juridique et comme la manifestation d'une volonté, celle d'un objectif à atteindre, en l'occurrence la transparence* »[122].

56. L'hyper spécialisation du droit nuit néanmoins à notre sens de plus en plus à la reconnaissance de principes généraux, raison pour laquelle nous avons par ailleurs souhaité appréhender la transparence du fait juridique algorithme dans sa globalité. Une approche globale du fait juridique étudié afin de l'aborder de la manière la plus pertinente possible et proposer une approche fonctionnelle de mise en œuvre d'un tel principe général de transparence

[120] Voir en ce sens, BRAIBANT G., « Droit d'accès et droit à l'information », in *Service public et libertés, Mélanges offerts au Professeur Robert-Édouard Charlier*, Éditions de l'université et de l'enseignement moderne, 1981, p. 704.
[121] RIVERO J., « La transparence administrative en Europe », rapport de synthèse « Transparence, je n'aime pas les mots flous…il y a malfaçon, opacité de la transparence », *Annuaire européen d'administration publique*, 1990, p. 307.
[122] MARCHAND J., « Réflexion sur le principe de transparence », *op. cit.*, p. 677.

des traitements algorithmiques. Il est général en ce qu'il permettrait d'observer le cyberespace dans un but de respect des droits et libertés, et plus largement de l'ordre juridique. Ce qui légitime surtout un tel principe est en lien avec la théorie générale de l'Etat dans sa philosophie libérale, à savoir rendre observable l'action de l'administration pour qu'elle puisse rendre compte, mais aussi la connaissance du positionnement des autres acteurs amenés à concurrencer son ordre juridique, émanation de l'autonomie des citoyens. Ce principe n'empêcherait pas par ailleurs d'agir de manière plus traditionnelle en relais d'autres régimes juridiques comme en matière contractuelle pour assurer le consentement des personnes.

57. Il arrive que saisir un fait nouveau en le rattachant à des régimes juridiques déjà existants ne peut être suffisant, et il convient à ce titre de consacrer un principe général de transparence des traitements algorithmiques, qu'ils soient publics ou privés, mais cela implique des ajustements significatifs. La réorientation des objectifs pour que la transparence soit propre au numérique sur le fondement de la transparence classique est insuffisante à assurer juridiquement la lisibilité des traitements. L'émergence d'une nouvelle source s'impose et sa mise en œuvre implique par ailleurs d'importants ajustements tant du point de vue constitutionnel que législatif.

58. Cette transparence n'a pas pour but de lever totalement l'opacité qui résulterait de ces traitements en réétudiant toutes les étapes des processus pour chaque personne et pour chaque usage, mais elle servirait à ce que l'ordre juridique continue d'être globalement efficace. Nous ne pouvons que tendre vers cet objectif car les moyens alloués ne sont pas sans limite[123] et parce que l'informatique connait également des contraintes observationnelles que le juridique ne saurait lever. Les tentatives de compréhension de ces systèmes ne doivent pas avoir pour obstacle le droit.

59. Même si des principes font parfois leur émergence à la suite de révisions constitutionnelles[124], ils sont souvent

> « *des règles de fond, habituellement très importantes (les droits de la défense, le principe de non-rétroactivité, etc.), que le juge met au monde lui-même en*

[123] A cet égard, le doyen Carbonnier ne considérait-il pas que la transparence « *a une substance, comme la vitre, c'est un bien, comme la vitre ; elle a donc un prix* ». Elle a donc un coût pour la société et les opérateurs économiques. Voir en ce sens, « Propos introductifs » in colloque *La transparence, RJ com.*, 1993, n° spécial, p. 11.
[124] Comme l'indique Didier Truchet, « *le principe de précaution a migré du droit international vers le droit communautaire, puis vers le droit français (art. 5 de la charte de l'environnement adoptée par la loi constitutionnelle du 1er mars 2005)* », TRUCHET D., *Le droit public*, *PUF*, 2014, spec. p. 58.

justifiant cette attitude théoriquement illicite au moyen d'une rhétorique subtile, mais pas forcément convaincante. En fait, et quoi qu'il en dise, cela revient toujours à apporter une norme générale nouvelle dans le système (même si l'opération ne prend presque jamais la forme d'une pure création ex nihilo, le juge ne pouvant donner l'impression de se comporter comme le ferait le législateur). Il faut voir là l'expression la plus manifeste du pouvoir normatif du juge, ou plus précisément de son pouvoir de créer des normes générales »[125].

60. Mais bien que le Conseil constitutionnel[126] ait récemment rattaché le droit d'accès aux documents administratifs à l'article 15 de la DDHC[127] lorsqu'il a été confronté aux algorithmes locaux de « *Parcoursup* »[128], ce qui est assez rare pour être souligné[129], il a également validé que le secret était opposable à leur communication. Malgré cette relative avancée, la reconnaissance d'un principe de transparence de la vie publique[130] apparaît encore lointaine, et il serait encore plus déraisonnable d'attendre du juge constitutionnel qu'il découvre un principe général de transparence des traitements algorithmiques répondant également à la concurrence de l'Etat par les opérateurs économiques, notamment car certaines valeurs du libéralisme politique qui se sont forgées contre l'ingérence de l'Etat dans la vie des acteurs privés seraient susceptibles de l'empêcher parce que les sources constitutionnelles manquent à cette fin[131]. Et quand bien même une loi poserait un tel principe, elle se heurterait donc à de nombreuses sources constitutionnelles. La fin des règles générales constitue également un émiettement du droit qui ne permet plus toujours d'appréhender l'entièreté d'un phénomène[132]. C'est la raison pour laquelle nous sommes favorables à ce qu'un tel principe figure dans une révision constitutionnelle. Il aurait toute sa place dans une charte des droits fondamentaux numériques[133].

61. Pourtant, comme nous l'avons constaté, les premières techniques juridiques concourant à une plus grande compréhension des algorithmes informatiques servent l'application de règles juridiques déjà existantes et assurent une dimension de principe support aux droits et libertés, et ce au même titre qu'un principe classique de transparence qui ne serait pas propre à la sphère

[125] DE BECHILLON D., *Qu'est-ce qu'une règle de Droit ?*, *Odile Jacob*, 1997, p. 30.
[126] CC, décision n° 2020-834 QPC, 3 avril 2020.
[127] Art. 15 DDHC 1789, « *La société a le droit de demander compte à tout agent public de son administration* ».
[128] *Infra*., n° 650.
[129] KERLEO J-F., « La constitutionnalisation d'un principe de transparence de la vie publique », *ADJA*, 2020, p. 1137.
[130] *Ibid*.
[131] *Infra* n° 647 et s.
[132] Ce mouvement était déjà pressenti. Voir en ce sens, DE BECHILLON D., *Qu'est-ce qu'une règle de Droit ?*, *op. cit.*
[133] LATIL A., « En attendant la Déclaration de droits fondamentaux du numérique », *Dalloz IP/IT*, 2021, p. 593 à 597.

numérique[134]. Nous n'y voyons donc pas plus qu'un principe relais indispensable, ce qui n'exclut pas pour autant qu'il soit bien plus au fur et à mesure de la découverte de nouvelles incidences de l'informatique sur la société. Qu'il s'agisse du droit privé ou du droit public, les sources ne sont pas toujours les mêmes, ce qui explique que la réalisation de la transparence s'opère par des techniques juridiques particulières. Il est important que l'objet étudié bénéficie d'une unité conceptuelle, reposant sur la justification de l'observation des faits juridiques du cyberespace, afin de garantir l'effectivité de l'ordre juridique lorsque leur immixtion le menace, ce qui n'est pas pour l'heure le cas.

62. Le recours au numérique exige une régulation au regard d'autres enjeux qui commencent à être cernés, notamment par la nouvelle proposition de règlement européen relative à l'IA[135]. Elle tend à reconnaître l'autonomie d'un principe de transparence propre à l'observation de l'environnement numérique pour la protection des droits fondamentaux[136]. Ces nouvelles obligations visent non pas à se substituer aux obligations et objectifs que nous étudierons tout le long de ces travaux, mais bien à se cumuler par l'intermédiaire d'une approche par les risques. Toutefois, le déploiement des techniques juridiques qu'elle souhaite opérer nous semble encore insuffisant pour parvenir convenablement à cet objectif.

63. L'enjeu de la transparence est éminemment démocratique. Un principe ne répondant qu'à des impératifs de transparence de l'action publique, c'est-à-dire dans une acception purement libérale est lacunaire. Ce sont aujourd'hui les puissances privées qui sont aussi une menace pour l'Etat et les libertés collectives et individuelles. La transparence en droit privé, qui repose par ailleurs essentiellement sur des obligations d'information contractuelles ou précontractuelles, ne saurait parvenir à elle seule à cet objectif. De plus, il convient désormais d'appréhender le numérique comme le disait Lawrence Lessig en tant que sphère à part entière susceptible de menacer la démocratie[137] et que seule une nouvelle organisation de l'Etat serait

[134] Comme l'indique Jennifer Marchand, le principe de transparence *« constitue la modalité substantielle de l'exercice effectif de droits essentiels tels que l'égalité de traitement, le droit à l'information, l'accès aux documents administratifs, la sécurité juridique, et l'intelligibilité de la loi. La transparence est une technique administrative et procédurale et ou un outil de légitimation politique. La transparence est une règle sanctionnable qui caractérise la norme intelligible et fonde un nouveau rapport à l'information politique, économique, administrative, contractuelle* », MARCHAND J., « Réflexion sur le principe de transparence », *op. cit.*, p. 677.

[135] Proposition n° 2021/0106 (COD) 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, du 21 avril 2021.

[136] *Infra.*, n° 946 et s.

[137] LESSIG L., *Code Is Law: on liberty in cyberspace*, *op. cit.*

à même de combattre pour se prémunir de la déviance des gouvernants et des opérateurs économiques[138] (Partie 2).

64. La reconnaissance d'un tel principe, qui se composerait en une pluralité d'autres principes et se déclinerait par ailleurs en une multitude de techniques juridiques, y compris sous forme de droits, offrirait la possibilité d'effectuer une conciliation juridique propre à la matière numérique et non seulement en fonction d'une conciliation du terrain classique, ce qui pourrait être l'occasion, d'un point de vue constitutionnel de hiérarchiser certaines valeurs entre elles au sein de cet environnement. Ainsi, les secrets protégés par la loi, la liberté d'entreprendre et le secret des affaires doivent-ils prévaloir sur la transparence des traitements algorithmiques alors qu'ils sont susceptibles de menacer les droits et libertés par l'inobservation de ces nouveaux outils, également vis-à-vis de l'Etat, pourtant nécessaires à la sanction des normes juridiques ? Il s'agit en réalité de rectifier un déséquilibre permettant de lever les freins à la réalisation juridique de la transparence. Mais pour ce faire, et dans le respect du droit des tiers issus du libéralisme économique, qui est aussi partie prenante de l'Etat de droit dans nos actuelles démocraties libérales, la transparence devrait avoir lieu *a minima* de manière indirecte, c'est-à-dire par l'intermédiaire d'un tiers de confiance. Cet apport ne peut provenir d'un droit souple, d'un éventuel principe de responsabilité des acteurs tel que prévu par le RGPD[139], mais il nécessite l'édiction d'un droit dur qui s'épanouirait par l'intermédiaire d'une nouvelle organisation des pouvoirs constitués qu'il conviendrait de repenser. L'Etat est l'échelon le plus à même de remplir cette tâche dès lors qu'il en donnerait les garanties pour qu'une telle transparence puisse être opérée en toute indépendance. C'est en effet grâce à sa force, institution au service de l'autonomie des citoyens en démocratie, qu'il serait possible de protéger les libertés menacées aussi bien par les gouvernants et l'administration, ainsi que par les géants du numérique. En effet, le libéralisme politique ne s'est pas construit face aux opérateurs privés, mais à l'encontre de la puissance publique. Face au retour d'éventuelles féodalités, ce qui a par ailleurs été au fondement de la naissance de l'Etat moderne, ce dernier est tout désigné pour remplir cette mission. Se pose naturellement la façon d'y parvenir, car la puissance publique constitue également une menace pour les libertés.

65. C'est au cœur de la notion de contre-pouvoirs institutionnels qu'il conviendrait de rétablir un équilibre. Ainsi, lorsque la Commission Nationale de l'Informatique et des Libertés

[138] *« Liberty in cyberspace will not come from the absence of the state. Liberty there, as anywhere, will come from a state of a certain kind », ibid.*, p. 4. Nous traduisons « La liberté dans le cyberespace ne viendra pas de l'absence de l'Etat. La liberté dans le cyberespace, comme partout ailleurs, viendra d'une certaine organisation de l'Etat ».
[139] *Infra.*, n° 209 et s.

(CNIL) est instituée comme première autorité administrative indépendante (AAI) désignée en tant que tel par une loi dès 1978[140] pour assurer la conformité des traitements automatisé ou non de données nominatives au droit par l'intermédiaire de plusieurs techniques que nous étudierons, elle opère aussi en contre-pouvoir technique pour certains traitements intéressant l'Etat par la voie d'un avis conforme qui lui sera par ailleurs plus tard retiré[141]. Nous avons identifié dans le cadre de ces travaux que l'approche par branche ou sectorielle du droit du fait numérique a engendré une pluralité d'autorités de contrôle étatiques, parfois indépendantes ou non, se faisant concurrence et à travers des moyens matériels et humains très faibles. A titre d'exemple, la CADA est compétente pour se prononcer sur les demandes de communication de documents administratifs, alors qu'elle ne vérifie pas que les documents transmis par l'administration sont véridiques, ce qui ne participe pas à lutter contre une asymétrie informationnelle au détriment des administrés. Une autorité de contrôle dédiée, la Commission Nationale de Contrôle des Techniques de Renseignement[142] (CNCTR), est chargée de contrôler les algorithmes utilisés dans le cadre de la surveillance étatique à des fins de prévention des troubles à l'ordre public. Lorsque les algorithmes font une immixtion dans le droit de la consommation, la Direction Générale de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF) est compétente[143]. Il en est de même en matière de santé avec la Haute Autorité de Santé (HAS) ou avec l'autorité de la concurrence pour apprécier les algorithmes des géants du numérique susceptibles d'effectuer des distorsions de concurrence.

66. Cette erreur remonte à notre sens à la genèse de la LIL. En effet, d'une part, le décret du gouvernement de Jacques Chirac instituant la « *Commission informatique et libertés* » afin qu'elle propose un régime juridique applicable aux traitements, ne souhaite pas cantonner un tel régime juridique aux données nominatives, puisqu'il est question de « *garantir que le développement de l'informatique, dans les secteurs public, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques* »[144]. Et d'autre part, le premier rapport de cette commission rendu public en 1975, et qui inspirera ensuite en partie la LIL, retient dans un chapitre X intitulé « *Informatique et démocratie* » la nécessité de prendre en compte les données qui gouvernent les aides à la prise de décision quand bien même celles-ci ne seraient pas nominatives. L'esprit du rapport est simple :

[140] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[141] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1).
[142] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.
[143] Voir notamment en ce sens, loi n ° 2016-1321 du 7 octobre 2016 pour une République numérique. Pour plus de précisions, *Infra.*, n° 292 et s.
[144] Décret n° 74-938 du 8 novembre 1974 portant création de la commission Informatique et libertés.

« (…) *Le véritable responsable, généralement incapable de démontrer tous mécanismes du modèle, ne dispose que de son bon sens pour s'opposer à une mobilisation considérable de moyens d'apparence scientifique. Il existe donc bien un danger de substitution du pouvoir ; les spécialistes du modèle tendent de facto à jouer un rôle majeur dans les processus de décision. Si, à l'insu du responsable en dernier ressort, le modèle a été façonné de manière à favoriser abusivement certaines orientations, notamment en agissant au niveau du programme, ce transfert de pouvoir peut se transformer en abus de pouvoir* »[145].

67. L'informatique devait y être saisie dans son entièreté, permettant à l'autorité administrative de référence d'avoir une emprise sur ces faits juridiques nouveaux. Il est d'ailleurs troublant de remarquer que de nombreuses incidences du numérique sur les droits et libertés que nous pensons découvrir aujourd'hui étaient autrefois déjà globalement observées. En revanche, l'informatique ayant majoritairement à cette époque des incidences sur le respect de la vie privée et une opacité sur les intentions de l'action publique, le régime juridique certes général qui en en a découlé s'est retrouvé limité à la question des données nominatives, puis personnelles.

68. Cela explique notamment en partie pourquoi la CNIL est limitée dans son action et se retrouve elle-même concurrencée par d'autres autorités publiques, ce qui suscite un éparpillement de la force de l'Etat[146] pour saisir ce phénomène. Il nous a semblé opportun de nous prononcer en faveur d'une autorité unique de contrôle des traitements algorithmiques qu'ils soient publics ou privés, et qui serait amenée à collaborer avec le cas échéant d'autres régulateurs. Il est nécessaire qu'un seul lieu réunisse les compétences et les efforts pour la compréhension de la sphère numérique afin de communiquer, dans le respect du droit des tiers et des secrets protégés par la loi, sur le comportement de ces outils. Il s'agirait donc d'un tiers de confiance étatique indépendant du pouvoir politique qui exercerait une transparence indirecte lorsqu'elle ne peut s'effectuer directement. La spécialisation des institutions pour

[145] Rapport de la commission informatique et libertés, *La Documentation française*, 1975, p. 82 à 83.

[146] Selon Guy HERAUD « *un ordre normatif est juridique, c'est-à-dire valable, au sens de la validité globale, lorsqu'il est soutenu par la plus grande force. Cette « plus grande force » est la force matérielle : économique, financière, et, finalement policière et militaire. Parce qu'il dispose de la plus grande force, l'ordre juridique a le pouvoir de faire respecter les normes qu'il édicte. La sanction matérielle organisée est le propre de l'ordre juridique, bien qu'on ne puisse dire de chaque règle qu'elle est effectivement sanctionnée, ni même qu'elle bénéficie d'une possibilité de sanction. La sanction, comme « la plus grande force », est le caractère de l'ordre in globo et non de ses éléments ut singuli. Le concept de « plus grande force » revêt avec le phénomène un caractère tranché : on peut dire, en effet, de l'Etat (et de l'Etat seul, à l'exclusion des pouvoirs féodaux), qu'il détient une puissance matérielle irrésistible. L'Etat peut, en effet, plier à volonté toute manifestation de force rebelle qui se dresserait contre lui au sein de l'ordre interne. L'imperium, le pouvoir de décision unilatérale, caractère l'Etat, et l'oppose aux ordres de coordination fondés sur les relations de type contractuel, telles la société féodale et la société d'individus* », HERAUD G., « *La validité juridique* », *op. cit.*, p. 479.

saisir les particularités de l'environnement numérique implique des corps constitués dédiés au sens large, y compris de la justice puisqu'elle doit participer davantage à la transparence de ces traitements, mais aussi du Parlement afin notamment de préciser le principe général constitutionnel souhaité.

69. Parallèlement, le rôle de la société civile n'est pas à négliger. Qu'elle intervienne en tant que justiciable, par la voie d'associations par exemple, ou des lanceurs d'alertes, elle concourt à une plus grande compréhension de ces systèmes. Un écosystème juridique doit donc encourager cette forme de transparence qui est au service de l'intérêt général. Il est à noter qu'il convient de s'intéresser au rôle que les architectes du cyberespace seraient amenés à avoir pour une plus grande transparence des systèmes qu'ils conçoivent. L'éthique joue une place de plus en plus présente dans la société, qu'elle soit d'ailleurs d'inspiration étatique ou privée, y compris par les acteurs du numérique eux-mêmes, mais bien qu'elle agisse comme l' « antichambre » du droit, elle ne saurait se substituer à un droit dur, raison pour laquelle certaines obligations particulières de transparence pourraient être imposées par la déontologie pour les grands projets ayant des incidences sur la société, et indépendamment de la manipulation de données personnelles. Nous envisageons sur le modèle du délégué à la protection des données[147] (DPD), l'élargissement d'une profession à des grands projets ne portant pas que sur les données à caractère personnel.

70. Enfin, un nouveau régime juridique législatif et réglementaire général nous semble opportun afin de mettre en œuvre cette transparence. Il convient d'y établir le degré et la nature des obligations relatives à transparence devant s'opérer, notamment en fonction des usages, mais également de la légitimité de l'acteur régulé. Les nouvelles propositions de règlement européen[148] allant en partie en ce sens avec son approche par les risques en fonction des usages algorithmiques est une source indéniable d'inspiration.

71. Mais nous ne voudrions pas que la reconnaissance d'un tel principe soit considérée comme une fin en soi. Bien que la transparence soit indispensable pour les raisons évoquées, elle ne peut se suffire à elle-même. La transparence juridique, même si elle devait aboutir à une transparence technique totale, lorsque cela est possible, ne veut pas dire que l'usage qui en est

[147] Le délégué à la protection des données à caractère personnel est une profession garante du respect de la réglementation des données personnelles au sein des organismes publics et privés. Il est régi par l'article 37 et suivants du RGPD.
[148] Proposition n° 2021/0106 (COD) 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, du 21 avril 2021.

fait est acceptable. Cette perspective nous conduirait à autoriser à tort des usages attentatoires aux libertés. Dans notre démonstration l'objet de transparence n'a aucun objectif de légitimation de l'usage. Certains usages algorithmiques doivent être exclus, et c'est pour cette raison aussi que la transparence est censée éclairer les citoyens et la représentation parlementaire sur les incidences de l'informatique sur la société. D'ailleurs, et nous le verrons, quand bien même le droit ne se heurterait pas à une transparence de ces traitements, certaines technologies demeurent opaques. Afin de compléter la démocratie représentative, et un peu à l'instar de la démocratie administrative, mais dans une acception plus générale pour prendre en considération certains projets privés ayant des incidences sur la société, il serait judicieux de compléter le principe de transparence par un principe de participation du public à la démocratie numérique. En effet, comme l'affirmait Christian Lequesne, la transparence « *ne suffit nullement à rendre une démocratie vivante dans la mesure où la démocratie ne saurait être réduite à un problème de visibilité des décisions* »[149].

[149] LEQUESNE ROTH C., « La transparence : vice ou vertu de la démocratie ? », *op. cit.*, p. 18.

PARTIE I - LES PRINCIPAUX REGIMES JURIDIQUES CONCOURANT A LA TRANSPARENCE DES TRAITEMENTS ALGORITHMIQUES

72. Notre génération ne découvre pas les incidences de l'informatique sur les droits et libertés. Un important régime juridique en matière de NTIC s'est construit depuis les années soixante-dix en France. Une règlementation générale a d'abord été créée afin de notamment concourir à la compréhension des traitements algorithmiques, aussi bien vis-à-vis des acteurs privés que publics par l'intermédiaire d'un droit à l'information, à la condition qu'ils traitent des données nominatives[150]. Sous l'impulsion du droit européen son approche a été modifiée. Une nouvelle règlementation issue du RGPD[151] et notamment de la directive l'accompagnant[152], ont complété des obligations de transparence en matière de données personnelles (Titre I). L'objectif poursuivi correspond d'une part au respect de la vie privée, mais aussi à la transparence de l'action administrative. Dès le départ, cette logique générale a été pensée pour être accompagnée de règles particulières[153].

73. Ainsi, parallèlement à ce droit général, un droit sectoriel, s'est construit. Des régimes juridiques sont par ailleurs apparus ou ont été récemment complétés afin de répondre à l'accentuation de ces nouveaux enjeux. Il est désormais possible d'affirmer qu'il existe un droit particulier relatif aux algorithmes privés et publics (Titre II) se superposant aux obligations générales précitées.

74. Bien que d'autres dispositions soient susceptibles de parvenir à la transparence de ces traitements, ce que nous serons amenés à constater de manière occasionnelle, c'est l'étude des techniques juridiques du droit positif apportées en réaction à ce nouveau fait juridique qui a notre attention, notamment pour évaluer leur effectivité et leurs éventuelles incohérences. Nous ferons par ailleurs état d'importants changements susceptibles d'intervenir par l'intermédiaire du droit européen[154].

---

[150] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[151] 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), *op. cit*.

[152] Directive (UE) 2016/680 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, dite « Police-Justice ».

[153] BRAIBANT G., « La protection des droits individuels au regard du développement », *Revue internationale de droit comparé*, 1971, p. 801.

[154] En effet, d'importantes et récentes propositions de la Commission européenne sont amenées à venir modifier ou compléter les régimes juridiques étudiés.

TITRE I - LE DROIT DES INDIVIDUS A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL : LE PRINCIPE DE TRANSPARENCE DES TRAITEMENTS

75. Attribuée trop souvent à l'affaire SAFARI[155], la LIL de 1978 est en réalité le fruit d'un long cheminement opéré en France dès le début des années soixante-dix. Dès 1970 le Conseil d'Etat consacre une étude sur « *les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives* »[156]. Il est toutefois important de souligner que dans la genèse de la LIL, l'atteinte potentielle aux droits et libertés engendrée par l'avènement de l'informatique est surtout l'émanation de la puissance publique, ce que la polémique SAFARI confirmera, et moins des opérateurs économiques, dans la mesure où les géants du numérique que nous connaissons aujourd'hui n'existaient pas encore, raison pour laquelle elle est qualifiée d'œuvre libérale[157] et concourant à l'accomplissement du mouvement de démocratie administrative de cette époque. Cela s'explique également par le fait que la couverture informatique dans les foyers est marginale, et l'internet civil n'a pas encore été déployé.

76. Assez vite, l'idée est alors d'aboutir à un régime juridique général pouvant ensuite être complété le cas échéant par des règlements particuliers[158]. Tout au long de cette décennie, les propositions de loi s'enchaînent, puis, il convient d'attendre 1974 pour qu'enfin la Commission informatique et libertés soit désignée[159] pour penser un nouveau régime juridique, dont la grande partie des propositions seront par ailleurs retenues dans un projet de loi qui donnera ensuite naissance à la LIL de 1978[160].

77. La LIL est un texte général, c'est-à-dire qui s'adapte à toutes les technologies de traitement de données à caractère personnel par l'intermédiaire de sa neutralité technique en soumettant les responsables de traitement à des obligations. Les personnes physiques concernées par ces traitements de données personnelles bénéficient désormais de droits leur

[155] A la suite d'un article publié dans le journal *Le Monde* en 1974, la France découvre que l'informatique peut être utilisée à des fins de fichage Le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) ambitionnait de créer une base de données centralisée regroupant toutes les informations administratives au sujet de la population française par l'intermédiaire d'un identifiant unique. Ce projet a finalement été abandonné.
[156] CONSEIL D'ETAT, Rapport, « Les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives : notes, comptes-rendus d'entretiens, notes manuscrites, projet de plan, projets intermédiaires », 20050574/18, n° 2, Archives nationales, 1970.
[157] Rapport de la commission informatique et libertés, *La Documentation française*, 1975.
[158] *Supra*., n° 72.
[159] Décret n° 74-938 du 8 novembre 1974 portant création de la commission informatique et libertés.
[160] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

permettant d'être informés, et d'accéder à leurs données personnelles, ce qui conditionne le cas échéant un droit de rectification, d'opposition ou d'effacement. C'est la généralité des dispositions de cette loi qui fait sa force. Elle ne se destine pas à des acteurs particuliers, ce qui en aurait exclu certains de son champ d'application, mais vise à l'époque tout traitement automatisé ou non d'informations nominatives[161]. L'automation à laquelle fait référence cette loi correspondent à des traitements algorithmiques[162].

78. Dorénavant, cette règlementation, sous l'impulsion du droit européen, concourt explicitement à la transparence des traitements algorithmiques, il ne s'agira pas dans le cadre de cette démonstration d'étudier le régime juridique des données personnelles dans son entièreté, mais la pluralité de principes ou de mécanismes juridiques œuvrant à la transparence de ces traitements. En ce sens, surtout à la lecture du RGPD, il est possible d'identifier que parmi les droits des personnes concernées par le traitement, certaines dispositions participent à la transparence de ce dernier (Chapitre I). Toutefois, l'information n'est rien si elle ne peut être vérifiée au moins par un tiers de confiance afin de mettre fin à toute asymétrie informationnelle. Ainsi, des autorités de contrôle participent au respect de la transparence, mais de nouveaux mécanismes tendent également désormais à responsabiliser les acteurs, et ce dans le but qu'ils démontrent par eux-mêmes leur conformité (Chapitre II). Cette logique diffère quelque peu de l'esprit originel de la LIL de 1978, ce qui n'est pas sans incidence sur le respect des droits et libertés.

79. En ce qui concerne les obligations relatives au RGPD que nous allons étudier, elles s'appliquent « *au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* »[163]. Enfin, conformément à son champ d'application matériel, des obligations particulières de transparence sont prévues pour les traitements de telles données en matière de « Police-Justice », ce que nous serons amenés à aborder[164]. Tandis que dans d'autres

[161] *Ibid*., art. 4 : *« Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale. ».* Depuis, la LIL ne fait plus référence aux informations nominatives mais à la notion de données à caractère personnel.

[162] *Ibid*., art. 5 : « *est dénommé traitement automatisé d'informations nominatives au sens de la présente loi tout ensemble d'opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives* ».

[163] Art. 2 §1 du RGPD.

[164] Indépendamment de ce domaine, concernant les traitements de données à caractère personnel des institutions, organes et organismes de l'Union, il existe une harmonisation des obligations avec le RGPD. Voir en ce sens, 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

hypothèses, le RGPD ne s'applique pas par exemple aux données personnelles traitées par les personnes physiques dans un cadre strictement personnel ou domestique[165]. Quant au champ d'application territorial de cette règlementation, tout traitement saisi par ce régime juridique s'applique dès lors qu' « *il est effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union* »[166].

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.

[165] Art. 2 §2 du RGPD.

[166] Art. 3 du RGPD.

CHAPITRE I - TRANSPARENCE ET DROITS DES PERSONNES CONCERNEES PAR LE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

80. Les règles faisant l'objet d'une étude dans le cadre de ce chapitre nous éclairent sur le fonctionnement des traitements algorithmiques de données à caractère personnel. Elles n'étaient toutefois pas initialement qualifiées en tant que telles de techniques juridiques œuvrant ou concourant à la transparence des traitements, puisque cette notion était encore assez peu présente dans le discours politique et juridique au tout début des années soixante-dix, période à laquelle l'informatique, comme fait juridique, a nécessité une réaction juridique à des fins de régulation.

81. Nous le verrons, la transparence a surtout été associée au numérique par l'intermédiaire du droit international, puis régional. C'est d'ailleurs essentiellement le droit de l'Union qui agrégera le droit à l'information et le droit d'accès à ses données personnelles, par ailleurs déjà présents dans la version initiale de la LIL de 1978, comme constitutif d'un principe de transparence. La directive 95/46/CE, abrogée depuis par le RGPD, comportait une seule occurrence à la transparence, dans son préambule[167], qui n'a qu'une valeur interprétative, ce qui laissait à penser que ce principe n'était pas central, et contraste aujourd'hui avec le caractère désormais incontournable de la transparence dans cette réglementation. Ce principe sert toutefois des objectifs différents, à savoir d'une part la démocratie administrative puisqu'il s'agit de contrôler l'action de l'Etat qui recourait à des traitements algorithmiques de données personnelles, puis de l'autre essentiellement le consentement à des fins de loyauté contractuelle.

82. Il convient donc à notre sens de distinguer d'une part entre les règles relatives à la communication par le responsable du traitement aux personnes physiques des informations sur leurs droits, parmi lesquels certaines portent sur celles relatives au traitement (Section 1), et d'autre part, l'étude des dispositions propres à la transparence du traitement (Section 2). Ces deux acceptions concourent effectivement à la transparence du traitement mais d'une manière différente. La première comporte des informations sur la façon dont le traitement sera mis en œuvre, tandis que l'autre évoque le traitement lui-même.

83. C'est l'analyse des règles de transparence, en l'occurrence de régulation, à l'aune du droit européen et national, qui va faire l'objet d'une étude particulière dans ce chapitre. Il n'est

[167] 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 63.

donc pas question d'évoquer la règlementation dans son entièreté. Toutefois, il apparaît que cette transparence revêt plusieurs acceptions et limites. Son degré et sa nature sont donc variables en fonction des situations rencontrées.

SECTION 1 - LES REGLES RELATIVES A LA COMMUNICATION PAR LE RESPONSABLE DU TRAITEMENT AUX PERSONNES PHYSIQUES DES INFORMATIONS SUR LEURS DROITS : LE DROIT A L'INFORMATION

84. Le G29 rappelle dans ses lignes directrices[168] que le principe de transparence est un dérivé du principe d'équité se trouvant à l'article 8 de la Charte des droits fondamentaux de l'Union européenne[169]. Il concourt donc à l'intelligibilité de ce qui est « *applicables aux citoyens en leur permettant de comprendre et, au besoin, de contester lesdits processus* »[170]. Toutefois, à défaut d'obtenir une définition précise de la transparence, parce qu'elle n'est nullement définie par le RGPD[171], il convient d'étudier au regard des dispositions de cette règlementation quelle est sa nature et son degré.

85. Il est intéressant de noter qu'il existe plusieurs dimensions dans la transparence des traitements de données à caractère personnel. L'article 12 du RGPD précise les modalités de transparence relatives à la collecte de données à caractère personnel. C'est donc au titre des droits de la personne physique concernée par la collecte de telles données que le responsable de traitement[172] doit procéder à un certain formalisme (Paragraphe 1) ainsi qu'à la communication d'informations particulières à ce sujet (Paragraphe 2).

[168] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018, p. 5.
[169] En effet, l'article 8 de la Charte des droits fondamentaux de l'Union européenne n'évoque pas le principe de transparence, mais la loyauté des traitements, c'est-à-dire la notion d'équité. Nous aborderons la notion de loyauté spécifiquement dans le cadre du chapitre I titre II de la première partie de cette thèse.
[170] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018, p. 5.
[171] Selon le considérant 39 du RGPD qui n'a qu'une valeur interprétative, « *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. Ce principe vaut, notamment, pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement.* ».
[172] Conformément au RGPD, il faut entendre par responsable du traitement *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre*; », art. 4 § 7.

PARAGRAPHE 1 - Transparence et modalité des communications

86. Il nous semble opportun d'évoquer en premier lieu la genèse de la transparence en matière de données à caractère personnel, car elle permet de comprendre l'esprit de cette règlementation au regard des objectifs qu'elle poursuit (A). Enfin, nous nous intéresserons au formalisme auquel sont soumis les responsables de traitement de la mise en œuvre du principe de transparence (B).

A - Genèse du principe de transparence en matière de données à caractère personnel

87. Dès 1974, le gouvernement de Jacques Chirac charge la *« Commission informatique et libertés* » de proposer un nouveau régime juridique permettant de « *garantir que le développement de l'informatique, dans les secteurs public, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques* »[173]. Les réflexions sont larges et ne se cantonnent pas qu'aux traitements de données nominatives. La transparence n'est pas désignée comme telle dans le rapport de la Commission en 1975[174], mais de nombreuses propositions seront reprises par le Rapport « Foyer »[175], puis dans un projet de loi qui donnera ensuite lieu à la LIL de 1978[176]. La menace pour la vie privée et les autres libertés sont identifiées comme étant essentiellement l'émanation de la puissance publique, bien qu'il soit tout de même question d'encadrer les opérateurs économiques. Il s'agit donc aussi d'une « *œuvre libérale* », socle de la démocratie administrative[177]. Ainsi, l'article 3 de la LIL évoquait déjà que « *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* », ce qui fonde un droit à l'information. A ce titre, de nombreuses informations doivent être communiquées par le responsable de traitement à la personne physique concernée lors de la collecte de ses données nominatives. Enfin, sauf exception, il est possible d'interroger l'entité chargée d'une telle manipulation de données *« en vue de savoir si ces traitements portent sur des informations nominatives la concernant, et le cas échéant, d'en obtenir communication* »[178]. Ces informations doivent être communiquées dans un « *langage clair* »,

[173] Décret n° 74-938 du 8 novembre 1974 portant création de la commission Informatique et libertés.
[174] COMMISSION INFORMATIQUE ET LIBERTES, Rapport, *La Documentation Française*, 1975.
[175] FOYER M., Rapport n° 3125 sur le projet de loi relatif à l'informatique et aux libertés de l'Assemblée nationale, 5e législature, fait au nom de la commission des Lois, enregistré à la Présidence de l'Assemblée nationale le 4 octobre 1977.
[176] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[177] OCHOA N., *Le droit des données personnelles, une police administrative spéciale*, thèse de doctorat soutenue le 8 décembre 2014 à l'Université Paris I – Panthéon-Sorbonne, p. 497.
[178] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 34.

et conditionnera également le cas échéant le droit d'opposition à un traitement[179] ou leur rectification[180], puisqu'en effet, comme le notait le « rapport Tricot », « *le droit d'accès demeurerait fictif si la personne ignorait jusqu'à l'existence du fichier qui la concerne* »[181].

88. Il s'agit toutefois d'un droit de savoir qui ne se limite pas aux responsables de traitement public. Cette forme de transparence ne poursuit donc pas que la transparence de l'action administrative puisqu'elle est plus large. Au-delà des enjeux de respect de la vie privée et de la protection des autres libertés, c'est la notion d'auto-détermination informationnelle, c'est-à-dire la possibilité de garder la maitrise de ses données, par le droit à l'information, qui semble désormais l'emporter et justifier cette transparence. Ainsi, le RGPD précise désormais que « *Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant* »[182].

89. Paradoxalement, il s'agit d'une avancée et d'un recul. D'une part, cette transparence joue un rôle fondamental dans le cadre de l'autonomie de la volonté afin que les individus consentent aux traitements de données personnelles de la manière la plus libre et éclairée possible. D'autre part, cette approche contractualiste nuit considérablement à la protection des libertés, laissant le cas échéant l'individu face à ses propres turpitudes sous couvert de son consentement, alors que « *l'émancipation individuelle par le libre choix est souvent une illusion* »[183].

90. Dès 1980, un principe de transparence fait son apparition très rapidement dans les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE. Il est présenté comme corolaire au principe de la participation individuelle et consiste à ce 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 de ses activités* »[184]. Puis, furtivement, la directive 95/46/CE a fait entrer la notion de transparence dans le régime juridique des données personnelles[185]. Il n'avait cependant qu'une

[179] *Ibid*., art. 26.
[180] *Ibid*., art. 36.
[181] Rapport de la commission informatique et libertés, *La Documentation française*, 1975, p. 37.
[182] Considérant 7 du RGPD.
[183] NETTER E., « A quoi sert le principe de transparence en droit des données personnelles ? », *Dalloz IP/IT*, 2020, p. 611.
[184] OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel en date du 23 septembre 1980, cons. 12.
[185] 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 63 : « *considérant que ces autorités doivent être dotées des moyens nécessaires à l'exécution de leurs tâches, qu'il s'agisse des pouvoirs*

valeur interprétative, ce qui laissait à penser que ce principe n'était pas central, et contraste aujourd'hui avec le caractère désormais incontournable de la transparence tel que prévu par le RGPD[186] qui a abrogé cette dernière. Nous le retrouvons à l'article 5 du RGPD aux côtés de la licéité et de la loyauté. Les données à caractère personnel doivent « *être traitées de manière licite, loyale et transparente au regard de la personne concernée* »[187].

91. Le G29 rappelle dans ses lignes directrices[188] que le principe de transparence est un dérivé du principe d'équité se trouvant à l'article 8 de la Charte des droits fondamentaux de l'Union européenne[189]. Il concourt donc à l'intelligibilité de ce qui est « *applicables aux citoyens en leur permettant de comprendre et, au besoin, de contester lesdits processus* »[190]. Il est également précisé que la transparence revêt trois principaux domaines, à savoir

> « *la communication aux personnes concernées d'informations relatives au traitement équitable de leurs données; 2) la façon dont les responsables du traitement communiquent avec les personnes concernées sur leurs droits au titre du RGPD; et 3) la façon dont les responsables du traitement facilitent l'exercice par les personnes concernées de leurs droits* »[191].

92. Toutefois, à défaut d'obtenir une définition précise de la transparence, parce qu'elle n'est nullement définie par le RGPD[192], il convient d'étudier au regard des dispositions de cette règlementation quelle est sa nature et son degré.

---

d'investigation et d'intervention, en particulier lorsque les autorités sont saisies de réclamations, ou du pouvoir d'ester en justice; qu'elles doivent contribuer à la transparence du traitement de données effectué dans l'État membre dont elles relèvent ».

[186] 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).

[187] Art. 5 § 1 a) du RGPD.

[188] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018, p. 5.

[189] En effet, l'article 8 de la Charte des droits fondamentaux de l'Union européenne n'évoque pas le principe de transparence, mais la loyauté des traitements, c'est-à-dire la notion d'équité.

[190] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018, p. 5.

[191] *Ibid*., p. 4.

[192] Selon le considérant 39 du RGPD qui n'a qu'une valeur interprétative, « *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. Ce principe vaut, notamment, pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement.* ».

B - Le formalisme de la transparence en droit européen

93. Qu'il s'agisse des articles 13[193],14[194], 15[195] ou 22[196] du RGPD que nous allons étudier[197], parce qu'ils concourent à la transparence des traitements de données à caractère personnel, ces obligations doivent respecter un certain formalisme afin d'assurer cette dernière. En effet, parmi les droits de la personne visés par le chapitre III du RGPD, nous retrouvons une section dédiée à la transparence et ses modalités de mise en œuvre. Mais elle ne contient expressément qu'une seule disposition : l'article 12 de ce texte.

94. La communication des informations doit être opérée « *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* »[198]. Il est à noter que pour ce faire, le responsable du traitement « *prend des mesures appropriées pour fournir toute information* ». La nature de cette information rassure, surtout lorsqu'on sait que la transparence est parfois réalisée par la communication d'innombrables documents visant à induire en erreur les personnes[199].

95. Le RGPD règle également la question du support de la communication. Elle peut s'effectuer par écrit, mais aussi par d'autres moyens comme la voie électronique[200]. Il est notamment envisageable que, sur demande de la personne, la communication s'effectue à l'oral à la seule condition que « *l'identité de la personne concernée soit démontrée par d'autres moyens* »[201]. L'objectif de cette disposition est de ne pas effectuer cette communication à un

---

[193] L'article 13 du RGPD porte sur les informations que le responsable de traitement doit immédiatement communiquer à la personne concernée si la collecte a lieu de manière directe.
[194] L'article 14 du RGPD porte sur les informations que le responsable de traitement doit communiquer dans un délai raisonnable si la collecte a lieu de manière indirecte.
[195] L'article 15 du RGPD est relatif au droit d'accès des personnes physiques à leurs données personnelles.
[196] Quant à l'article 22 du RGPD, il s'agit d'un droit à l'information concernant la logique des décisions individuelles automatisées.
[197] *Infra*., n° 104 et s.
[198] Art 12 § 1 du RGPD. En ce sens, le considérant 58 du préambule du RGPD qui a vocation interpretative, precise encore davantage cette disposition : « *Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels. Ces informations pourraient être fournies sous forme électronique, par exemple via un site internet lorsqu'elles s'adressent au public. Ceci vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne. 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* ».
[199] PASQUALE F., *Black Box Society : Les algorithmes secrets qui contrôlent l'économie et l'information*, *op. cit.*
[200] Art. 12 § 1 du RGPD.
[201] *Ibid*.

tiers malveillant qui pourrait ensuite bénéficier d'informations sensibles sur une personne par exemple.

96. Concernant désormais les articles 15 et 22 du RGPD, qui nous intéressent particulièrement au titre du principe de transparence, le responsable du traitement doit faciliter la mise en œuvre des droits garantis auprès de la personne physique concernée. Toutefois, s'il n'est pas en mesure d'identifier la personne faisant l'objet d'un tel traitement, il n'est logiquement pas tenu de produire ces renseignements[202].

97. La communication des informations à fournir cette fois-ci au titre des articles 13 et 14 du RGPD s'effectue auprès de la personne, et ce gratuitement de la part du responsable du traitement. Dans l'hypothèse où les demandes seraient « *manifestement* » infondées, voire excessives, ce que le responsable du traitement doit être en capacité de prouver, il peut facturer des frais raisonnables afin de prendre en compte ces coûts ou tout simplement ne pas traiter cette demande[203]. L'esprit du texte semble alors dirigé vers le souhait de prévenir l'entrave de l'innovation par des efforts déraisonnables et difficilement tenables économiquement. Il est à noter que les informations visées par les articles 13 et 14 du RGPD « *peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu* »[204]. Dans l'hypothèse où ces informations sont communiquées par la voie électronique, ces icônes doivent pouvoir être lues par la machine.

98. Les informations qui devront être communiquées au titre du droit des personnes concernées sont à transmettre par le responsable du traitement dans un délai d'un mois à compter de la réception de la demande[205]. Néanmoins, si l'opération s'avère complexe ou parce que les demandes seraient trop nombreuses à traiter, ce délai peut être prolongé de deux mois[206] à la condition de notifier aux demandeurs l'allongement du délai ainsi que les motifs de ce report dans un délai d'un mois.

99. Si le responsable du traitement « *ne donne pas suite à la demande formulée par la personne concernée* », il est tenu d'informer les demandeurs, dans un délai d'un mois à compter

[202] Art. 12 § 2 du RGPD.
[203] Art. 12 § 5 du RGPD.
[204] Art. 12 § 7 du RGPD.
[205] Les informations à communiquer sont celles prévues aux articles 15 à 22 selon l'article 12 § 3 du RGPD.
[206] *Ibid*.

de la réception de la demande, des motifs tout en les informant des voies de recours, c'est-à-dire de la possibilité d'introduire « *une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel.* »[207].

100. Quant au protocole d'amendement à la Convention européenne des droits de l'homme, appelée convention 108+[208], il existe également un formalisme relatif aux modalités de communication des informations du traitement. L'article 9 du protocole fait référence à une communication sous une forme intelligible ainsi qu' *« à intervalle raisonnable et sans délai ou frais excessifs* »[209]. Contrairement au RGPD, la convention ne prévoit pas le format des informations devant être fournies, ce qui peut malheureusement nuire à une uniformisation de ces obligations au sein des Etats partis à la convention.

101. Toutefois, le principe de transparence et les règles que nous avons abordées dans le cadre des modalités de la communication des informations, ne s'appliquent pas dans certaines circonstances[210]. Nous retrouvons donc les exceptions prévues par le texte tels que par exemple les traitements de données personnelles opérés dans le cadre de la sécurité publique ou juridictionnels au titre de la directive « *Police-Justice* »[211].

---

[207] Art. 12 § 4 du RGPD.

[208] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 18 mai 2018. Ce protocole modernise la convention n° 108 du 18 janvier 1981 du Conseil de l'Europe du même nom.

[209] *Ibid*., Art. 9 b).

[210] En ce sens, art. 23 du RGPD, « *1. Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir :*
c) la sécurité publique ;
d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale
f) la protection de l'indépendance de la justice et des procédures judiciaires ;
h) une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g) ;
i) la protection de la personne concernée ou des droits et libertés d'autrui ;
2) En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant :
a) aux finalités du traitement ou des catégories de traitement ;
b) aux catégories de données à caractère personnel ;
c) à l'étendue des limitations introduites ;
d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;
e) à la détermination du responsable du traitement ou des catégories de responsables du traitement ;
f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ;
g) aux risques pour les droits et libertés des personnes concernées ; et
h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation. »

[211] Directive (UE) 2016/680 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,

102. Compte tenu de la vulnérabilité des personnes physiques dans certaines circonstances, c'est-à-dire si la collecte de données à caractère personnel n'a pas lieu auprès de la personne physique concernée, le responsable de traitement doit lui communiquer certaines informations, œuvrant notamment à une meilleure transparence, dans un délai raisonnable n'excédant un mois après l'obtention de ces données[212].

103. Notons qu'il conviendrait d'imposer au responsable de traitement qu'il soit d'avantage imposé de s'adapter à son destinataire, ce qui empêcherait par ailleurs l'envoi d'informations trop stéréotypées. En effet, entre un destinataire expert ou un profane en informatique, le niveau d'information ne devrait pas être identique.

PARAGRAPHE 2 - Les informations à communiquer au titre du droit européen

104. Le droit à l'information est défini par les obligations incombant au responsable du traitement. Ainsi, son étude nous indique que les informations à communiquer à la personne concernée au titre du droit européen renseigne dès la collecte des données sur le traitement futur (A). Ce droit à l'information est toutefois à concilier avec de nombreux impératifs qui limitent très fortement ce droit, et donc la compréhension du traitement à venir (B).

A - Les dispositions communes pour un traitement équitable et transparent

105. Dès lors que nous avons étudié le formalisme des informations à communiquer, il convient de s'intéresser au contenu, c'est-à-dire aux informations que le responsable du traitement est amené à fournir aux personnes concernées. Ces règles s'appliquent du début du cycle de vie du traitement, à savoir de la phase de l'obtention des données jusqu'à son traitement ultérieur[213] . Le responsable de traitement est donc contraint par certaines obligations dès la collecte de données afin d'informer la personne physique du traitement la concernant. A cet égard, la transparence porte sur les données et non sur le traitement en lui-même, ce qui explique pourquoi les articles 13 et 14 du RGPD se situent dans une section s'intitulant « *information et accès aux données à caractère personnel* »[214].

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.
[212] Art. 14 § 3 a) du RGPD.
[213] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018, p. 35.
[214] Section 2 du RGPD.

106. Concernant les obligations à fournir au titre du RGPD, il convient cependant de distinguer les informations devant être fournies lorsque la collecte a lieu directement auprès de la personne concernée (article 13 du RGPD), alors que d'autres informations sont spécifiquement communiquées lorsque les données ne sont pas obtenues auprès de la personne concernée (article 14 du RGPD). En effet, le régime juridique applicable n'est pas exactement similaire. Bien entendu, comme nous l'avons vu précédemment[215], la communication de ces informations doit être effectuée « *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* »[216].

1 - Les dispositions communes aux articles 13 et 14 du RGPD et à la convention 108+

107. Sur ce point, il est à noter que le RGPD et la convention 108+ offrent une étonnante symétrie dans son contenu, sans doute pour aligner le droit de la convention sur le droit de l'Union, et ce malgré des intitulés différents puisque selon le nouveau protocole de la convention 108, les informations que nous allons étudier sont à communiquer afin d'assurer un traitement transparent.

108. Qu'il s'agisse d'une collecte de données à caractère personnel effectuée auprès de la personne concernée (c'est-à-dire au moment où les données sont obtenues) ou directement auprès d'elle, certaines informations à fournir par le responsable du traitement sont communes à ces deux situations. En ce sens, le responsable du traitement doit communiquer son identité, ses coordonnées ainsi que celles du représentant du responsable du traitement[217] ou du DPD[218]. La base juridique et les finalités de ce traitement doivent également être connues de la personne dont les données ont été collectées[219]. Il en est de même concernant « *les destinataires ou les catégories de destinataires* » de ces données dans les hypothèses où ils existeraient[220]. Enfin, si le responsable de traitement « *a l'intention d'effectuer un transfert de données vers un pays tiers ou une organisation internationale* », la personne physique doit bénéficier de certaines informations telles que son fondement ou non sur une décision d'adéquation de la

[215] *Supra*, n° 94.
[216] Art. 12 du RGPD.
[217] Art. 13 § 1 a) et Art 14 § 1 a) du RGPD et art. 8 § 1 a) de la convention 108+.
[218] Art. 13 § 1 b) et Art 14 § 1 b) du RGPD et art. 8 § 1 b) de la convention 108+.
[219] Art. 13 § 1 c) et Art 14 § 1 c) du RGPD.
[220] Art. 13 § 1 e) et Art 14 § 1 e) du RGPD et art. 8 § 1 d) de la convention 108+.

Commission[221]. En l'absence d'une telle décision, les garanties appropriées doivent lui être communiquées afin qu'elle puisse le cas échéant en obtenir une copie, ou l'endroit où il sera possible d'en prendre connaissance[222].

2 - La garantie d'un traitement équitable et transparent

109. Bien que les dispositions communes évoquées participent à la transparence, les articles 13 et 14 du RGPD évoquent également la communication d'informations spécifiques « *nécessaires pour garantir un traitement équitable et transparent* »[223]. Deux notions sont donc combinées dans ce cas de figure : le principe d'équité et de transparence malgré une absence de définition.

110. Les articles 13 et 14 du RGPD énumèrent à ce titre certaines informations qui doivent être communiquées telles que la durée de conservation des données, ou si le responsable du traitement est dans cette impossibilité, « *les critères utilisés pour déterminer cette durée* »[224]. La mention selon laquelle la personne dispose de droits tels que le droit d'accès à ses données personnelles, mais aussi le droit de les rectifier ou encore de les effacer ainsi que le droit de s'opposer au traitement, sans oublier le droit à la portabilité doivent être fournies[225]. Si le traitement a été consenti pour une ou plusieurs finalités, voire si ce dernier repose sur un consentement explicite de données sensibles[226], la personne concernée doit être informée qu'elle peut « *retirer son consentement à tout moment* »[227]. La personne physique faisant l'objet d'un traitement est par ailleurs tenue informée qu'elle dispose d'un droit de recours auprès de l'autorité de contrôle[228].

111. Dans l'hypothèse où le traitement est fondé sur des intérêts légitimes[229], la personne concernée en prend connaissance[230]. Toutefois, il est surprenant que lorsque la collecte n'a pas

[221] Art. 13 § 1 f) et Art. 14 § 1 f) du RGPD.
[222] *Ibid*.
[223] Art. 13 § 2 et Art. 14 § 2 du RGPD.
[224] Art. 13 § 2 a) et Art. 14 § 2 a) du RGPD
[225] Art. 13 § 2 b) et Art. 14 § 2 c) du RGPD et art. 8 § 1 e) de la convention 108+.
[226] Il convient d'entendre par donnée personnelle sensible au regard de la LIL, les données qui « *(…) révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* », art. 6 de la LIL modifiée.
[227] Art. 13 § 2 c) et Art. 14 § 2 d) du RGPD.
[228] Art. 13 § 2 d) et art. 14 § 2 e) du RGPD.
[229] Au titre de l'article 6 § 1 f) du RGPD.
[230] Art. 13 § 1 d) et art. 14 § 2 b) du RGPD.

eu lieu directement auprès de la personne concernée, la communication de cette formalité ne figure non pas dans le paragraphe relatif aux informations générales, mais dans celui relatif à la garantie d'un traitement équitable et transparent.

112. Toutes ces informations relèvent davantage de la transparence et de la compréhension du cadre réglementaire, c'est-à-dire d'une information relative aux droits de la personne concernée par le traitement. Elles participent naturellement à la transparence du traitement en orientant le cas échéant la personne physique sur la manière dont le traitement est opéré, mais il ne s'agit nullement de dispositions qui sont propres à la compréhension ; la façon dont le traitement algorithmique est mis en œuvre dans les faits, sachant qu'il peut toujours exister un décalage entre la réalité technique et les considérations découlant des obligations juridiques du responsable du traitement.

113. En toute logique, si le responsable du traitement a l'intention d'effectuer, après collecte, un autre traitement de données à caractère personnel fondé sur une autre finalité que celle prévue initialement, il doit fournir à la personne physique concernée des informations au sujet de cette nouvelle finalité. Néanmoins, « *toute autre information pertinente* » parmi la liste que nous venons d'étudier[231], et ce afin de garantir un traitement équitable et transparent[232], est également à transmettre. Le G29 a précisé dans ses lignes directrices qu'à la lumière du considérant 61 du RGPD, représentatif de l'esprit du texte, il existait un risque d'interprétation contradictoire à ce sujet. En effet, la disposition pouvait laisser entendre que dans le cadre des traitements prévus à l'article 13 § 3 et 14 § 4 du même texte, les renseignements à fournir étaient à l'appréciation du responsable du traitement parmi les informations listées. Finalement, selon le G29, le considérant 61 laisserait à penser que *« la position par défaut est que toutes les informations énoncées dans ce paragraphe devraient être fournies à la personne concernée à moins qu'une ou plusieurs catégories d'informations n'existe(nt) pas ou ne soi(en)t pas applicable(s)* »[233]. Cette prise de position démontre qu'entre les dispositions et ses considérants, le RGPD est extrêmement mal rédigé en plus d'être complexe.

[231] Il s'agit des informations à communiquer au titre de l'article 13 § 2 et 14 § 2 du RGPD, *Supra*., n° 109 et s.
[232] Art. 13 § 3 et art. 14 § 4 et considérant 61 du RGPD.
[233] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018, p. 28.

a - Les informations spécifiques à communiquer au titre d'une collecte auprès de la personne concernée

114. La personne physique concernée doit être informée lors de la collecte (si elle est effectuée auprès d'elle) du fondement juridique de la fourniture des données, c'est-à-dire si elle a lieu au titre d'une exigence réglementaire ou contractuelle. Ladite personne doit être tenue informée au sujet de la collecte dès lors que la fourniture de ses données personnelles est nécessaire à la conclusion du contrat, voire des conséquences « *éventuelles* » si elles ne pouvaient être fournies[234].

b - Les informations spécifiques à communiquer au titre d'une collecte non opérée auprès de la personne concernée

115. Le responsable de traitement communique de plus à la personne concernée par une collecte non opérée auprès d'elle, la provenance des informations collectées et mentionne si « *elles sont issues ou non de sources accessibles au public* »[235]. De plus, lorsque les données personnelles sont utilisées *« aux fins de la communication avec la personne concernée* », les renseignements sont à transmettre « *au plus tard au moment de la première communication à ladite personne* »[236], ou « *s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois* »[237].

B - Dérogations à la communication des informations et limites

116. Lorsque la collecte des données a lieu directement auprès de la personne concernée ou non, dès lors qu'elle dispose déjà de ces informations, le responsable de traitement n'est pas tenu de les communiquer ou de les transmettre de nouveau[238].

117. Dans l'hypothèse où la collecte n'a pas été effectuée auprès de la personne physique, le responsable de traitement n'est pas dans l'obligation de communiquer les informations étudiées dès lors que *« la fourniture de telles informations se révèle impossible ou exigerait des efforts*

[234] Art. 13 § 2 e) du RGPD.
[235] Art. 14 § 2 f) du RGPD.
[236] Art. 14 § 3 b) du RGPD.
[237] Art. 14 § 3 c) du RGPD.
[238] Art. 13 § 4 et art. 14 § 5 a) du RGPD, et art. 8 § 2 de la convention 108+.

disproportionnés »[239] ou parce que *« les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel* »[240]. Il en est de même si le droit de l'Union ou un Etat membre impose la fourniture d'informations particulières pour certains traitements[241].

118. Du coté des lignes directrices édictées par le G29, il est rappelé que le RGPD contient un conflit entre l'exigence de communication d'informations « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* » et une information qui serait complète[242], sachant que le responsable du traitement est le plus à même d'analyser quelles sont les informations qui rempliraient cette exigence. C'est d'ailleurs ce qui abonde dans le sens que le RGPD n'offre du point de vue de ces dispositions qu'un niveau très modéré d'explication ne permettant pas, même pour les plus aguerris en informatique, de vérifier la conformité du traitement mis en œuvre. A cet égard, l'information n'est pas de même degré, ni de même nature que celle concernant les algorithmes publics, qui demeure à ce jour, le régime juridique le plus précis en la matière, notamment car l'action administrative répond à des exigences supérieures de transparence[243].

119. Quant à la convention modernisée 108 du Conseil de l'Europe[244], elle stipule que « *les données à caractère personnel faisant l'objet d'un traitement sont : traitées loyalement et de manière transparente* ». Ce n'est que dans l'article 9 du protocole intitulé « droits des personnes concernées » que figure l'obligation d'explicabilité, et d'intelligibilité[245] que nous étudierons au titre du droit d'accès des données traitées. Selon le protocole, en plus de ce qui est prévu à l'article 9, doit être communiqué à la personne concernée « *toute autre information complémentaire nécessaire pour garantir un traitement loyal et transparent des données à caractère personnel* »[246], alors qu'en revanche le RGPD lui préfère sur ce point la notion d'équité ainsi qu'une liste limitative d'informations à communiquer[247], bien que le Comité

[239] Art 14 § 5 b) du RGPD et art 8 § 3 de la convention 108+.
[240] Art 14 § 5 d) du RGPD.
[241] Art 14 § 5 c) du RGPD et art 8 § 3 de la convention 108+.
[242] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018, p. 21.
[243] *Infra.*, chapitre II titre 2 de la première partie de cette thèse.
[244] Art. 5 § 2 a) du protocole.
[245] En ce sens, art. 9 (b) du protocole : « *la communication sous une forme intelligible des données traitées, et toute information disponible sur leur origine, sur la durée de leur conservation ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements conformément à l'article 8, paragraphe 1 »* ainsi que « *d'obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués ».*
[246] Art. 8 §1 (e) de la convention 108+.
[247] Art. 13 § 2 et 14 § 3 du RGPD.

Européen de la Protection des Données (CEPD) considère pourtant qu'il s'agisse d'une liste non exhaustive[248].

120. Toutefois, ce droit à l'information n'est pas absolu puisqu'il est également restreint par certains impératifs au titre d'une conciliation avec d'autres droits et libertés. Les droits de l'article 8 §1 et 9 que nous venons d'énoncer sont exclus par l'article 11 dans certains cas. Nous y retrouvons des impératifs classiques comme la sécurité nationale, mais également plus nébuleux comme les intérêts économiques et financiers de l'Etat[249]. Le secret des affaires n'est pas directement cité, mais il est inclus de fait dans les dispositions de l'article 11 § 1 (b) qui évoquent la conciliation avec la protection « *de la personne concernée ou des droits et libertés fondamentales d'autrui* ». Le choix a donc été fait de hiérarchiser ces principes à celui de la transparence et non de les intégrer au sein de ces principes afin d'obtenir une transparence par l'intermédiaire d'un tiers de confiance par exemple.

121. Ces dispositions sont essentielles, (bien qu'insuffisantes, comme nous le verrons plus loin), puisqu'en l'absence de cette obligation d'information, la personne ayant fait l'objet d'une collecte de données à caractère personnel, ne pourrait connaître l'existence d'un tel traitement. Pourtant, c'est bien l'une des problématiques de la transparence : sans information préalable, il n'est pas possible de contester un traitement, notamment parce qu'il est ignoré de l'individu et l'autorité de contrôle n'a pas compte tenu de ses budgets, la faculté d'opérer des contrôles massifs. L'information est un principe primordial en ce qu'il va, par exemple, permettre de saisir le responsable du traitement d'une contestation ou une autorité de contrôle, voire un juge afin que le droit existant soit effectif. C'est donc une pierre angulaire au bon respect des droits et libertés. Et nous savons très bien que les algorithmes, du fait qu'ils ne sont pas directement observables par un individu, peuvent recueillir des données en toute impunité. En effet, si la personne faisant l'objet d'une telle collecte n'est pas informée, elle ne peut connaître le statut de ses données et donc l'usage qui peut en être fait.

[248] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018, p. 26.
[249] Art. 11 de la convention modernisée, « 1. *Aucune exception aux dispositions énoncées au présent chapitre n'est admise, sauf au regard des dispositions de l'article 5 paragraphe 4, de l'article 7 paragraphe 2, de l'article 8 paragraphe 1 et de l'article 9, dès lors qu'une telle exception est prévue par une loi, qu'elle respecte l'essence des droits et libertés fondamentales, et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique :*
a. à la protection de la sécurité nationale, à la défense, à la sûreté publique, à des intérêts économiques et financiers importants de l'État, à l'impartialité et à l'indépendance de la justice ou à la prévention, à l'investigation et à la répression des infractions pénales et à l'exécution des sanctions pénales, ainsi qu'à d'autres objectifs essentiels d'intérêt public général ;
b. à la protection de la personne concernée ou des droits et libertés fondamentales d'autrui, notamment la liberté d'expression ».

122. Les responsables du traitement qui ne respecteraient pas ces obligations mettent en péril l'esprit du RGPD qui vise à *« ce que les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant »*[250]. Nous considérons que ces règles de transparence ne sont que constitutives d'une transparence théorique et non effective. En effet, la transparence effective ne peut être opérée que par une autorité de contrôle[251], à travers son pouvoir d'investigation, en vérifiant que les informations communiquées à l'utilisateur sont véridiques.

123. Cette approche de transparence théorique, reposant sur la communication d'un certain nombre d'informations, est toutefois intéressante car elle est fondée sur le risque et non sur la violation directe de droits fondamentaux. Nous pouvons imaginer une absence de transparence et un respect des droits fondamentaux de la part du responsable du traitement qui se ferait dans l'opacité. Mais ce principe de transparence, dans la dimension étudiée, permet de sanctionner cette opacité puisque c'est cette dernière qui empêche de constater aisément la violation. Il est donc tout à fait possible de condamner le responsable du traitement uniquement sur le fondement de cette carence intermédiaire qui ne porte pas sur la transparence du traitement lui-même, mais sur l'absence d'informations susceptibles de constater les autres manquements au RGPD, à savoir aux autres droits de la personne concernée.

124. En revanche dans le droit de la convention, il est question de la communication de tout document attestant du caractère loyal et transparent[252]. Il convient néanmoins d'attendre les exigences du juge de Strasbourg en la matière.

SECTION 2 - LA TRANSPARENCE PROPRE AU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

125. Après avoir étudié le régime juridique applicable aux informations à communiquer lors de la collecte des données, il convient de se consacrer à l'analyse du droit d'accès aux données traitées puisque ce dernier est susceptible de renseigner sur le traitement effectivement en cours de fonctionnement, dans la mesure où nous nous situons plus tardivement dans le cycle de vie des données, censé aboutir à la communication d'informations plus détaillées (Paragraphe 1).

[250] Cons. 7 du RGPD.
[251] *Infra.*, n° 171 et s.
[252] Art. 8 e) de la Convention 108+.

126. Un approfondissement sera également réservé aux prises de décisions individuelles automatisées et de profilage, parce qu'elles peuvent exercer une incidence significative sur la situation des intéressés et des effets juridiques, ce qui ouvre spécifiquement un droit à l'information sur la logique sous-jacente du traitement ainsi qu'une intervention humaine, qui n'est toutefois pas constitutive d'un droit supplémentaire à l'explicabilité du traitement (Paragraphe 2). Toutefois, bien qu'il existe des débats sur ce point dans la doctrine, certaines juridictions pourraient être susceptibles de solliciter un degré de transparence supérieur à ce que recommande les lignes directrices du G29 à ce sujet.

PARAGRAPHE 1 - Le droit d'accès aux données personnelles traitées

127. Le droit d'accès aux données personnelles traitées était déjà l'un des piliers de la LIL de 1978. Elle peut s'exercer de différente manière, c'est-à-dire de façon directe auprès du responsable du traitement (A), et dans d'autres situations, que de façon indirecte (B). Le degré du niveau d'information n'est pas identique et dépend également du droit des tiers. Alors que ce droit intervient lorsque le cycle de la donnée est déjà bien avancé, car la personne fait déjà l'objet d'un traitement, il s'avère que cette information n'est pas toujours plus précise qu'au titre du droit à l'information général s'opérant lors de la collecte des données personnelles.

A - Le droit d'accès direct

128. Avant l'entrée en application du RGPD, la LIL de 1978[253] ainsi que la directive 95/46/CE[254] contenaient déjà une disposition relative au droit d'accès des personnes physiques à leurs données personnelles. On retrouve également la présence de ce droit dans la Charte des droits fondamentaux de l'Union européenne[255]. Il est également présent dans la convention 108[256] et 108+[257] du Conseil de l'Europe.

L'article 15 §1 du RGPD dispose que

[253] Art. 39 LIL de 1978.
[254] Art. 12 directive 95/46/CE.
[255] Art. 8 § 2 de la Charte des droits fondamentaux de l'Union Européenne.
[256] Art. 8 b) de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.
[257] Art. 9 § 1 b) du protocole 108 +.

« La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel (…) ».

129. Et comme nous l'avons vu précédemment[258], l'article 12 du RGPD précise que cette communication doit être effectuée de « *façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* », tandis que la convention 108 et modernisée lui préfèrent une communication « *des données traitées sous une forme intelligible* ».

130. Contrairement aux informations communiquées lors de la collecte des données de la personne concernée au titre des articles 13 et 14 du RGPD[259], le droit d'accès permet dans ce cas de figure d'obtenir des informations sur le traitement lorsque celui-ci est déjà mis en œuvre. En théorie, on pourrait raisonnablement penser que cela est censé favoriser l'accès à des informations encore plus précises sur le traitement des données puisque nous sommes à ce stade dans une phase plus avancée du cycle de vie des données. Dès lors, si la personne concernée par le traitement n'a par exemple pas été informée au titre des articles 13 et 14 du RGPD, elle peut donc formuler une demande auprès de l'organisme dont elle pense que ses données sont traitées.

131. Dans l'hypothèse où des données à caractère personnel sont traitées par l'organisme sollicité, alors la personne concernée pourra y obtenir l'accès[260]. Alors que la transparence est désignée par le RGPD comme un principe, l'accès au traitement est quant à lui un droit, c'est-à-dire que sa mise en œuvre y est précisée et des obligations particulières incombent au responsable de traitement[261]. Il est intéressant en ce qu'il subordonne en théorie l'effectivité des autres droits ou dispositions du RGPD participant à la transparence des traitements. Le considérant 63 du RGPD précise à cet égard que la personne concernée « *devrait avoir le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet et d'exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité* (…) ». C'est donc parce que l'un des volets de ce droit concourt à une

[258] *Supra*, n° 93 et s.
[259] *Ibid.*
[260] Art. 15 § 1 du RGPD et art. 49 de la LIL modifiée ainsi que art. 9 § 1 (b) du protocole 108+.
[261] L'article 15 du RGPD est intitulé « *droit d'accès de la personne concernée* ».

plus grande transparence des données traitées que le traitement peut être apprécié par la personne concernée.

132. Cette disposition permet de vérifier quelles sont les données traitées afin de prendre connaissance de leur exactitude, ce qui, le cas échéant, conditionnera l'exercice du droit d'opposition[262], de rectification[263] ou d'effacement des données[264] par exemple. Mais faut-il encore que l'information soit véritable, ce qui peut seulement être apporté par la conformité[265] afin de pallier toute asymétrie informationnelle. En effet, le responsable du traitement reste dans une position de supériorité par rapport à l'individu faisant l'objet d'un traitement.

133. S'ajoutent à cela des informations complémentaires qui doivent lui être transmises, reprenant par ailleurs les informations à communiquer au titre des articles 13 et 14 du RGPD que nous avons étudiées[266], telles que

> « *a) les finalités du traitement;*
>
> *b) les catégories de données à caractère personnel concernées ;*
>
> *c) les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales ;*
>
> *d) lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;*
>
> *e) l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement ;*
>
> *f) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;*
>
> *g) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source* »[267] .

[262] Art. 21 du RGPD.
[263] Art. 16 du RGPD.
[264] Art. 17 du RGPD.
[265] *Infra*., n° 169 et s.
[266] *Supra.*, n° 107 et s.
[267] Art. 15 § 1 du RGPD.

134. Il y a d'ailleurs fort à parier qu'en fonction du responsable du traitement, les informations fournies au titre de l'article 15 soient finalement identiques à celles communiquées en vertu des obligations de l'article 13 et 14 du RGPD, alors qu'en théorie elles devraient être plus pertinentes puisque nous ne sommes plus dans la phase de la collecte des données, mais de leur exploitation. Mais dans l'hypothèse où la personne n'avait pas connaissance de ce traitement, cela permet tout de même de garantir la communication de ces informations ainsi que la prise de connaissance du cadre réglementaire.

135. Il est à noter que cet accès au traitement s'effectue également par la faculté de demander une copie des données à caractère personnel traitées[268]. Dans ce cas de figure, cette communication porte uniquement sur les données personnelles relatives à la personne concernée, et non sur les autres données personnelles afférentes aux tiers, ce qui est compréhensible car elle ne doit pas nuire aux droits et libertés d'autrui[269]. Cela permet toutefois de prendre connaissance posément des informations détenues par le responsable du traitement. A titre d'exemple, lorsque la personne physique sollicite auprès du responsable du traitement un accès à ses données personnelles traitées, les informations obtenues sont censées lui procurer des renseignements sur le respect des autres obligations de cette règlementation. En ce sens, c'est ainsi que Max Schrems a obtenu la copie de ses données personnelles détenues par Facebook, ce qui lui permis de réaliser l'ampleur de la non-conformité de cette société au droit européen, comme le non-effacement de certaines données qu'il avait sollicité[270].

136. Toutefois, comme ce droit implique de pouvoir l'exercer à intervalle régulier afin de vérifier la licéité du traitement, il est prévu que des « frais raisonnables » puissent être exigés pour les copies supplémentaires sur les coûts imposés au responsable du traitement[271].

---

[268] Art. 15 § 3 du RGPD.

[269] Art. 15 § 4 du RGPD. Au regard du considérant 63 du RGPD, les droits et libertés d'autrui comprennent notamment le « *secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel.* ».

[270] BRANDY G., Maximilian Schrems : « Les termes de Facebook ne sont pas valides selon les lois européennes », *Le Monde* [en ligne], 04 août 2014, mis à jour le 14 août 2014. [Consulté le 04 octobre 2020]. Disponible à l'adresse : https://www.lemonde.fr/pixels/article/2014/08/07/maximilian-schrems-le-but-est-de-faire-respecter-a-facebook-la-legislation-europeenne_4468090_4408996.html. Lorsque Max Schrems demanda le droit d'accès à ses données personnelles, Facebook les lui transmettra manuellement sur un CD. En effet, en 2011, le média social n'avait pas implanté l'option permettant d'accéder automatiquement à ses données comme c'est aujourd'hui le cas. Il n'est donc pas exclu que Facebook ait communiqué malencontreusement des informations s'auto-incriminant, ce qui peut être résolu par l'automatisation de cette communication au strict nécessaire, c'est-à-dire à ce qui est conforme à la réglementation. En effet, rien ne peut garantir à la personne concernée par le traitement que les informations communiquées par le responsable du traitement correspondent à la réalité du traitement. Ce droit d'accès servit donc de fondement à Max Schrems pour ensuite introduire des plaintes, ce qui aboutira notamment à l'annulation du *Safe harbor en* 2015.

[271] Art. 15 § 3 du RGPD.

137. Dans le cadre de ce droit d'accès, cette communication ne concerne pas davantage les données qui contribuent au fonctionnent du traitement. Il est donc difficile, sur le fondement de ce droit, de connaître le fonctionnement du traitement global.

138. Cela démontre que le RGPD est essentiellement fondé autour des personnes physiques et ne prend pas en considération le fait que des associations puissent prendre connaissance du fonctionnement des algorithmes utilisés par les responsables du traitement, alors que ces derniers, du moins pour les plus grandes organisations, ont une large incidence sur la société.

B - Le droit d'accès indirect et autres limitations

139. Le RGPD a toutefois permis des limitations au droit d'accès de la personne concernée à travers d'importantes marges d'appréciation laissées à la convenance des Etats membres de l'Union européenne, ce qui atténue la transparence de cette règlementation, bien qu'elle ne puisse être absolue juridiquement à raison d'une exigence de conciliation avec un intérêt général ou d'autres droits et libertés.

140. Les données personnelles traitées à des fins de recherche scientifique, historique ou statistiques peuvent limiter ce droit de savoir puisque la communication de ces informations serait de nature à entraver, voire rendre impossible de telles finalités[272]. Il en est de même si des données à caractère personnel font l'objet d'un traitement archivistique dans un intérêt public et que ce droit d'accès nuirait également à cette finalité[273]. Toutefois, les limitations évoquées ne peuvent s'opérer sans garanties « *techniques et organisationnelles* » telles que la minimisation des données, ou encore, lorsque cela est possible, au recours à la pseudonymisation, voire à l'anonymisation des données[274]. La loi n° 2018-493 du 20 juin 2018, transposant ledit règlement[275], est venue modifier l'article 49 alinéa 3 de la LIL. Dès lors, compte tenu du droit national, « *lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée et à la protection des données des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de réalisation de recherche scientifique ou historique* », le droit d'accès de la personne concernée n'est pas applicable.

[272] Art. 89 § 2 du RGPD.
[273] *Ibid*., § 3 du RGPD.
[274] *Ibid*., § 1 du RGPD.
[275] Voir en ce sens l'article 15 et 89 § 2 du RGPD.

141. Comme nous l'avons abordé précédemment, l'article 23 du RGPD prévoit notamment plusieurs limitations relatives à la communication d'informations, ce qui n'est pas sans incidence sur le droit d'accès puisqu'il n'est pas absolu et doit être concilié avec d'autres impératifs tels que la sûreté de l'Etat et la défense nationale[276]. Dans cette hypothèse, il s'agit d'un accès indirect qui va être opéré par un tiers de confiance, en l'occurrence la CNIL, afin d'effectuer des vérifications[277]. Au lieu de solliciter le responsable du traitement, la personne concernée sollicitera donc la CNIL, qui à son tour désignera un de ses membres « *appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes* » afin de procéder aux investigations, et le cas échéant aux modifications nécessaires[278]. L'autorité en question informera ensuite l'intéressé que ces vérifications ont bien été effectuées, ainsi que sa possibilité de former un recours juridictionnel. Toutefois, une copie des données est susceptible d'être communiquée à la personne concernée à la seule condition que cette dernière ne remette pas en cause les « *finalités, la sûreté de l'Etat, la défense ou la sécurité publique* »[279]. Il ne s'agit cependant pas d'une obligation, et cela reste à l'appréciation de la commission en accord avec le responsable du traitement. Sous l'empire de la précédente version de la LIL, le Conseil d'Etat a eu à juger dans un arrêt du 24 octobre 2019 qu'il n'existait pas un tel droit si le fichier était relatif à la sureté de l'Etat, et qu'une consultation des données sur place pouvait être opérée en lieu et place de la transmission d'une copie des données[280]. Enfin, dans le cadre d'un tel système d'informations, le droit d'accès direct peut être rétabli par acte réglementaire si « *la communication ne mettrait pas en cause les fins qui lui sont assignées* »[281]. Dans ce cas de figure, la transparence directe est donc laissée à l'appréciation du responsable du traitement.

142. Les traitements de données en matière pénale font également l'objet de dispositions particulières dérogeant au RGPD. Ainsi, le droit d'accès est plus restrictif que celui prévu par la règlementation européenne en ce qu'il permet d'obtenir la communication non pas de la totalité des données détenues par le responsable de traitement, mais uniquement celles faisant l'objet du traitement[282]. Le principe du droit d'accès indirect, bien qu'il existe encore pour de nombreux autres fichiers, a cependant été aménagé. A titre d'exemple, depuis le décret n° 2018-687 du 1er août 2018, il est désormais possible pour la personne concernée d'obtenir un droit

[276] Conformément à la directive « Police-Justice » et sa transposition à l'art. 118 de la LIL modifiée.
[277] Art. 118 § 1 de LIL modifiée.
[278] *Ibid*.
[279] *Ibid*.
[280] CE, 24 octobre 2019, req. n° 427204.
[281] Art. 119 de la LIL modifiée.
[282] Art. 105 de la LIL modifiée.

d'accès direct au traitement d'antécédents judiciaires (TAJ)[283], ce qui conditionnera le cas échéant la rectification ou l'effacement des données[284]. A défaut d'une réponse du ministère de l'Intérieur dans un délai de deux mois, ou d'un refus, un droit d'accès indirect pourra être effectué auprès de la CNIL qui sollicitera le procureur de la République afin qu'il se prononce sur cette demande[285].

143. Compte tenu de l'existence de prérogatives de puissance publique justifiant ces traitements, un texte peut facilement exclure ce droit d'accès et mettre à mal cette technique de transparence juridique participant à la compréhension des traitements algorithmiques. Nous notons de manière générale que de nombreux fichiers demeurent encore inaccessibles directement par les personnes concernées. La tentation est même parfois au renforcement de la culture du secret. Le projet de de loi relatif à la prévention d'actes de terrorisme et au renseignement en date du 28 avril 2021[286] comportait une limitation supplémentaire au droit d'accès à ses données personnelles concernant les échanges de données entre autorités administratives et services de renseignement tel que prévu par l'article L.863-2 du Code de la sécurité intérieure au motif que cela constituerait un risque opérationnel.

144. Au-delà des fichiers intéressant la sûreté de l'Etat et de la défense nationale, ou relatifs à la matière pénale, d'autres traitements ayant une incidence significative sur les personnes ne sont par exemple toujours pas consultables dans leur intégralité comme en matière fiscale et bancaire. Le responsable du traitement du fichier national des comptes bancaires et assimilés[287] (FICOBA) est la Direction générale des finances publiques, alors que les données sont collectées par des opérateurs économiques, puisqu'il recense tous les comptes ainsi que les données afférentes à celui-ci, tels que les noms et adresses par exemple, mais il ne contient toutefois pas d'informations sur les opérations bancaires. Le droit d'accès direct n'est possible que par la personne physique concernée par le traitement qu'au regard des données d'identification[288] auprès du centre des finances publiques du domicile du requérant, tandis que l'accès aux données relatives à la nature et à l'identification du compte ne peut s'effectuer que de manière indirecte auprès de la CNIL en vertu des articles 52 et 118 de la LIL[289]. Ce droit d'accès est alors considéré comme mixte par certains auteurs[290].

---

[283] Il en est de même concernant le système d'information Schengen et le fichier des personnes recherchées.
[284] Art. R40-33 II du Code de procédure pénale.
[285] *Ibid*., III.
[286] Projet de loi n° 4104 relatif à la prévention d'actes de terrorisme et au renseignement du 28 avril 2021.
[287] Art. 164 FC du Code général des impôts.
[288] Art. 164 FE du Code général des impôts.
[289] *Supra*., n° 141.
[290] Voir en ce sens, FERAL-SCHUHL C., *Cyberdroit. Le droit à l'épreuve de l'internet*, *Dalloz*, 2020, p. 50.

145. Les ayants droits, comme dans le cadre du FICOBA, sont susceptibles d'accéder aux informations relatives aux comptes bancaires de la personne défunte[291], et ce alors même que le droit d'accès et d'information s'éteignent par principe à l'extinction de la personnalité juridique physique[292].

146. Enfin, quant aux données de santé, la LIL[293] prévoit que les données soient communiquées directement auprès de la personne concernée ou bien consultée le cas échéant par un médecin désigné par elle[294].

PARAGRAPHE 2 - Le cas spécifique des décisions individuelles automatisées

147. Les décisions individuelles exclusivement automatisées, c'est-à-dire n'impliquant pas d'intervention humaine, sont amenées à connaître un essor croissant. Elles nécessitent une attention toute particulière puisqu'elles sont susceptibles d'avoir des effets juridiques ou d'impacter de manière significative les personnes concernées, voire des groupes sociaux. C'est à ce titre qu'une information particulière doit être apportée à la personne concernée par le responsable du traitement au sujet de la logique sous-jacente (A). Dans certains cas, une intervention humaine est même exigée *a posteriori* par le RGPD, mais il ne peut totalement s'agir en l'état d'un droit à l'explicabilité de la décision. Cette information est de plus soumise à des limitations (B).

A - La logique sous-jacente du traitement de données : le droit à l'explicabilité

148. La loi n° 78-17 du 6 janvier 1978 abordait déjà en réalité une approche de protection par le risque, ce que n'a pas découvert la Commission européenne par l'intermédiaire de sa proposition de règlement visant à réguler l'IA[295], puisqu'elle interdisait aussi bien les décisions de justice ou les décisions individuelles privées ou publiques ayant « *pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de*

[291] Art. L. 151 B du livre des procédures fiscales.
[292] Voir en ce sens, CE, 10 et 9e chambres réunies, n° 386525, du 8 juin 2016, *« (…) qu'il résulte de ces dispositions qu'elles ne prévoient la communication des données à caractère personnel qu'à la personne concernée par ces données ; qu'il suit de là que c'est à bon droit que la présidente de la CNIL, qui avait reçu délégation pour prendre la décision attaquée, a confirmé le refus opposé par la Banque de France à Mme et MMD..., qui ne pouvaient, en leur seule qualité d'ayants droit, être regardés comme des "personnes concernées"* ».
[293] Art. 64 de la LIL modifiée.
[294] Et ce conformément à l'article L.1111-7 du CSP.
[295] *Infra*., n° 946 et s.

l'intéressé »[296]. En dehors de ces interdictions, elle disposait également d'un droit de connaître les informations et le raisonnement des traitements dont les résultats étaient opposés à un individu à des fins de contestation[297].

149. Pourtant, quelle que soit la nature des décisions individuelles automatisées, cette interdiction n'était qu'assez peu respectée par les acteurs. En effet, même si nous y reviendrons spécifiquement concernant les décisions administratives individuelles[298], de telles décisions étaient bien automatisées, et ce même avant que ne le permette la transposition du RGPD et de sa directive. Perica Sucevic avait reconnu, en tant que conseiller juridique à la Direction interministérielle du numérique et du système d'information et de communication de l'Etat (DINSIC)[299], lors de son audition au Sénat le 12 juin 2018, que certaines décisions administratives individuelles ne faisaient déjà plus intervenir depuis de nombreuses années le moindre humain, comme pour le calcul des impôts sur le revenu notamment[300]. Le législateur européen et national a donc sans doute souhaité dans un élan de pragmatisme encadré et contrôlé de telles décisions.

150. Il ne s'agit pas de nier que certaines activités sont chronophages et que la machine présente des performances supérieures aux humains dans les domaines déniés de sens commun justifiant de ce fait son recours. Cette forme de transparence a également plusieurs acceptions. D'une part elle sert à informer les personnes concernées, et d'autre part, il s'agit également pour le responsable du traitement de s'assurer de la maitrise de l'outil utilisé[301], alors que ce dernier est susceptible de prendre des décisions contraires à ce qu'il souhaite. Il en va de la maîtrise du traitement et de ses effets juridiques.

151. Dès lors, lorsque l'informatique s'immisce au point de fonder exclusivement des décisions individuelles, la transparence doit être renforcée par rapport aux autres usages. Il s'agit notamment de la logique reprise par le RGPD. L'article 22 du RGPD porte sur les décisions individuelles exclusivement automatisées, c'est-à-dire sans intervention humaine, y

[296] Art. 2 de la LIL de 1978.
[297] Art. 3 de la LIL de 1978.
[298] *Infra*., n° 435 et s.
[299] La DINSIC est depuis devenue la Direction Interministérielle du Numérique (Dinum).
[300] BERNE X., Transparence des algorithmes publics : l'avertissement du Conseil constitutionnel, *Nextinpact* [en ligne]. 18 juin 2018. [Consulté le 12 avril 2020]. Disponible à l'adresse : https://www.nextinpact.com/article/28508/106743-transparence-algorithmes-publics-lavertissement-conseil-constitutionnel
[301] Les lignes directrices du G29 relatives à la prise de décision individuelle précisent en effet « que la communication de ces informations aidera également les responsables du traitement à s'assurer qu'ils respectent certaines garanties requises visées par l'article 22, paragraphe 3, et au considérant 71 », G29, lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 du 3 octobre 2017, version révisée le 6 février 2018, p. 28.

compris de profilage[302] « *produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* »[303].

152. Aux informations communiquées au titre du droit à l'information générale, s'ajoute une information spécifique concernant la logique sous-jacente des décisions individuelles automatisées[304]. Elle est quant à elle prévue par les articles 13§2 (f) et 14 §2 (g) et 15 §1 (h) du RGPD, rédigées par ailleurs dans les mêmes termes, et combinant l'impératif d'équité et de transparence en précisant que concernant ces usages, le responsable du traitement doit mentionner les *« informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée* ». La loyauté du traitement en dépend[305]. A la lecture de ces premières dispositions, il s'agirait donc davantage de dispositions relatives à l'intelligibilité, ce qui au mieux offre à la personne concernée une information générale au risque qu'elle soit stéréotypée. Pour autant, cette information ne permet pas de lever le voile sur tous les mystères qui entourent les décisions automatisées.

153. Il est donc à noter que cette logique « *sous-jacente* » du traitement est censée être communiquée aussi bien lors de la collecte des données que dans le cadre du droit d'accès vu précédemment[306]. La convention 108+ reprend également comme « droit de la personne concernée » le fait pour cette dernière *« d'obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués »*[307].

154. Le profilage est également concerné par l'article 22 du RGPD et illustre parfaitement la problématique de la transparence du traitement des données dans la mesure où la personne concernée ignore le plus souvent l'existence de ces données, ne serait-ce car il s'agit de données inférées. Le profilage nécessite de plus la réalisation d'une pluralité de procédés techniques que les profanes en informatique ne sont pas susceptibles de comprendre à l'état brut quand bien même il existerait une transmission de ces informations, d'où l'exigence de l'article 12 du

[302] Selon l'article 4 4) du RGPD, il convient d'entendre par profilage *« toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;* ».
[303] Art. 22 § 1 du RGPD.
[304] *Supra.*, n° 93 et s.
[305] G29, lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 du 3 octobre 2017, version révisée le 6 février 2018, p. 26.
[306] *Supra.*, n° 128 et s.
[307] Art. 9 § 1 c) de la convention 108+.

RGPD précisant que cette dernière s'effectue « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* ».

155. Les lignes directrices du G29 relatives à la prise de décision individuelles automatisées précisent à cet égard que « *Le RGPD exige que le responsable du traitement fournisse des informations utiles sur la logique sous-jacente, mais pas nécessairement une explication complexe des algorithmes utilisés ou la divulgation de l'algorithme complet. Les informations fournies doivent toutefois être suffisamment complètes pour que la personne concernée comprenne les raisons de la décision* »[308]. Et c'est justement parce que la technologie est parfois trouble qu'elle nécessite par ailleurs la fourniture d'informations[309] et des exigences accrues de compréhension.

156. Par principe, les personnes physiques peuvent s'opposer à un tel traitement[310]. Mais compte tenu des exceptions à ce droit d'opposition[311], le responsable du traitement doit prévoir « *des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée* » ainsi qu'une intervention humaine dans certains cas[312]. Il semblerait toutefois qu'en fonction des Etats membres de l'Union européenne, des exigences supérieures de transparence soit exigée au titre de l'article 22 du RGPD.

157. En application du RGPD, il a par exemple été jugé en Italie que sous peine d'illicéité, lorsque le consentement de la personne physique concernée est la base légale d'une telle décision, le responsable du traitement est tenu de transmettre les éléments sur lesquels fonctionnent l'algorithme[313]. Une telle interprétation, si elle se généralisait, serait susceptible d'aboutir à l'obtention d'informations plus précises sur l'algorithme contrairement à ce qu'exige le G29. Dans l'attente d'un éclaircissement à ce sujet de la Cour de justice de l'Union européenne, le degré de cette transparence est donc de plus variable en fonction de la culture

[308] G29, lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 du 3 octobre 2017, version révisée le 6 février 2018, p. 28.
[309] Voir en ce sens considérant 58 du RGPD.
[310] Art. 22 § 1 du RGPD.
[311] Les personnes physiques ne peuvent s'opposer à une décision individuelle automatisée, ou à un profilage lorsque la décision *« a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ; b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou*
c) est fondée sur le consentement explicite de la personne concernée ». Voir en ce sens, art 22 §2 du RGPD.
[312] Parmi les exceptions au droit d'opposition à une décision individuelle automatisée évoquées précédemment au titre de l'article 22 § 2, *« une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision* » n'est toutefois pas prévue en cas d'application de l'article 22 § 2 b) du RGPD. Pour plus de précisions, *Infra.*, n° 160 et s.
[313] Cour de cassation Italienne, chambre civile 1, n° 14381 du 25 mai 2021.

des juridictions, et de l'espèce, ainsi que le cas échéant des Etats membres sous réserve du respect des droits des tiers pouvant s'opposer à une telle communication[314].

158. Lors de la transposition du RGPD et de sa directive dans notre droit national, le législateur n'a pas souhaité reprendre la terminologie de « logique sous-jacente », mais de « principales caractéristiques »[315]. Il semblerait que cette particularité ne soit qu'un alignement avec l'explicabilité des décisions administratives individuelles fondées sur un traitement algorithmique dont le régime juridique est antérieur à l'entrée en application du RGPD, puisqu'issu de la LRN de 2016. Il ne s'agit donc pas d'une transparence de nature différente, si ce n'est que son degré a légèrement été altérée car le législateur a tout de même exclu une telle communication dans l'hypothèse de secrets protégés par la loi[316]. Au même titre que Thibault Douville[317], nous ne comprenons pas en quoi le secret devrait empêcher une information relative aux principales caractéristiques du traitement puisque ces éléments demeurent généraux, et ne sont pas donc pas susceptibles de décrire le processus dans son intégralité.

159. De plus, la règlementation des données personnelles ne permet pas de bénéficier d'un droit à l'information au sujet des outils de recommandation pouvant influencer la prise de décision finale. En d'autres termes, le risque est que l'humain fasse écran alors que sa pensée a pu être construite, même de manière inconsciente, par un ou une pluralité d'outils algorithmiques puisque comme nous l'avons évoqué, l'informatique jouit en apparence d'une certaine « s*cientificité* »[318]. Comme le note le Thibault Douville, « *on pourrait regretter que, sans que le droit d'opposition soit étendu à toute prise de décision fondée même partiellement sur un traitement de données, une information particulière des personnes concernées ne soit pas généralisée à l'hypothèse de l'utilisation d'un outil d'aide à la décision* »[319], et ce contrairement à ce qui est prévu en droit public[320].

[314] Il convient de rappeler à cet égard que dans certaines hypothèses les obligations de transparence prévues par les articles 13, 14, 15 et 22 du RGPD connaissant des exceptions. En ce sens, *Supra.*, n° 120 et 141.
[315] Art. 47 §1 de la LIL de 1978 modifiée.
[316] *Ibid*.
[317] DOUVILLE T., *Droit des données à caractère personnel : droit de l'Union européenne, droit Français*, *Lextenso*, 2021, p. 285.
[318] *Supra.*, n° 27.
[319] DOUVILLE T., *Droit des données à caractère personnel : droit de l'Union européenne, droit Français, op. cit.*, p. 281.
[320] *Infra*., n° 438 et s.

B - Intervention humaine et absence de droit à l'explicabilité supplémentaire

160. Lorsqu'une décision individuelle est exclusivement automatisée, et que la personne concernée ne peut s'y opposer[321], le responsable du traitement « *met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée* »[322], parmi lesquelles le droit pour la personne intéressée « *d'obtenir une intervention humaine dans le but d'exprimer son point de vue et de contester la décision* »[323]. Les « *mesures appropriées* » que le responsable du traitement doit mettre en œuvre ne sont pas précisées. Naturellement, certains mécanismes, comme la désignation d'un DPD[324] ne peuvent que y concourir.

161. Du point de vue de la transparence des traitements, l'article 22 du RGPD a été la disposition la plus débattue par la doctrine. En effet, certains auteurs[325] estimaient que cet article reconnaissait un véritable droit à l'explicabilité du traitement, tandis que d'autres[326], au contraire, ont considéré l'inverse. En effet, l'article 22 du RGPD interprété à la lumière du considérant 71 laissait à penser un tel droit en ce qu'il évoque notamment qu'

> *« en tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision. Cette mesure ne devrait pas concerner un enfant ».*

162. Cependant, les lignes directrices du G29 relatives aux décisions automatisées sont venues préciser dès 2017 que cette obligation d'intervention humaine *« de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision »*[327]

---

[321] Il s'agit des exceptions de l'article 22 § 2 du RGPD que nous avons vues précédemment, *Supra*., n° 156.
[322] En ce sens, voir l'article 22 § 3 du RGPD. L'intervention humaine ne s'applique toutefois que pour les exceptions prévues par l'article 22 § 2 a) et c).
[323] *Ibid.*
[324] Nous serons amenés à évoquer plus en détail le rôle du DPD. Voir pour plus de de précisions, *Infra*., n° 237 et s.
[325] Voir en ce sens GOODMAN B., FLAXMAN S., European Union regulations on algorithmic decision-making and a « right to explanation », *AI Magazine*, vol. 38, n° 3, 2017, spec. p. 6 [en ligne] [Consulté le 5 novembre 2020]. Disponible à l'adresse : https://arxiv.org/pdf/1606.08813
[326] WACHTER S., MITTELSTADT B., FLORIDI L., « Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation », *International Data Privacy Law*, vol. 7, issue 2, mai 2017 ; EDWARDS L., VEALE M., Slave to the Algorithm ? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, in *Duke Law & Technology Review*, vol. 18, 2017 [en ligne]. [Consulté le 15 juin 2020]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855
[327] Art 22 § 3 du RGPD.

n'emporte pas une explication détaillée du traitement et encore moins la divulgation de l'algorithme[328]. Cela est d'autant plus regrettable qu'elle considère à propos de l'intervention humaine que « *tout examen doit être effectué par une personne qui a l'autorité et la compétence appropriées pour modifier la décision* »[329]. Quitte à avoir un dialogue avec le représentant du responsable du traitement compétent, il aurait été intéressant que l'échange soit fructueux afin que chaque étape du processus appliquée à sa situation soit expliquée, ce qui reviendrait par ailleurs à pouvoir vérifier que le traitement initial contesté était finalement correct. Toutefois, nous ne pouvons exclure que la CJUE soit amenée un jour à reconnaître un tel droit sur le fondement de cette interprétation[330].

163. Finalement, et nous rejoignons ce point de vue, il s'agirait davantage d'un droit de notification d'une telle prise de décision permettant d'obtenir communication du processus général à la personne concernée afin de permettre le cas échéant de s'y opposer[331]. Cette intervention humaine, comme l'évoque Margot E. Kaminski, constituant un droit d'être informé, elle est centrée sur la personne physique concernée et non sur le traitement en lui-même. Il s'agirait donc d'une transparence garantissant l'exercice des autres droits individuels garantis par le RGPD tels que le droit d'opposition ou encore de rectification, et aucunement d'obtenir un débat technique sur le système[332]. Tout au plus, les droits de la personne concernés par cette réglementation offrent un dialogue avec le responsable de traitement, voire la rectification de certaines erreurs en fonction des informations communiquées, mais elles ne font pas intervenir des tiers, le cas échéant indépendants, dans le contrôle de ces algorithmes[333].

164. Quand bien même un tel droit à l'explication des décisions algorithmiques serait effectif, il ne peut concourir intégralement à la transparence de ces systèmes comme nous le verrons dans la partie 2 de ces travaux. Une logique collective par l'intermédiaire d'autres techniques juridiques nous semblerait en effet plus utile que la manière dont ce droit purement individuel a été construit, puisque dans certaines conditions nous ne pouvons-nous opposer à une

[328] G29, lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 du 3 octobre 2017, version révisée le 6 février 2018, p. 28.
[329] *Ibid*., p. 30.
[330] CASTETS-RENARD C., « Régulation des algorithmes et gouvernance du machine learning : vers une transparence et « explicabilité » des décisions algorithmiques ? », *Revue Droits & Affaires*, n° 15, *Lexisnexis*, 2018, p. 32 à 48, spec. p. 41.
[331] Il est possible de s'y opposer dans les conditions prévues à l'article 21 et 22 du RGPD.
[332] KAMINSKI M, E., « Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability », *Southern California Law Review*, vol. 92, n° 6, 2019, spec, p. 1589 [en ligne] 03 avril 2019, mis à jour le 11 novembre 2019. [Consulté le 15 juin 2020]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351404
[333] *Ibid.*

explication opérée par un tiers de confiance, en l'occurrence une nouvelle institution, de préférence étatique, disposant de la légitimité politique pour l'effectuer[334].

165. Bien que le RGPD institue en son article 22 un droit « *de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé* »[335], il n'en demeure pas moins que la directive du même jour[336] a permis à l'administration d'y déroger en contrepartie d'une transparence plus accrue que celle mise en place par le RGPD[337]. Mais la LRN, sur laquelle nous reviendrons plus en détail, prévoyait déjà quant à elle un véritable droit à l'explicabilité des décisions administratives individuelles fondées sur un traitement algorithmique[338]. En dehors de cette hypothèse, et c'est particulièrement ce qui nous intéresse, c'est-à-dire sur la base du consentement[339] ou lorsque l'exécution ou la conclusion d'un contrat en dépend[340], le RGPD ouvre droit à une certaine explicabilité de ce type de traitement bien que nous craignions qu'elle soit dans les faits stéréotypées. Rien n'empêchait cependant le pouvoir législatif d'offrir un niveau de transparence supérieur par une intervention humaine pour les décisions individuelles privées. Mais l'excès de transparence se heurterait naturellement à d'autres principes juridiques et considérations de nature économique puisque la transparence et son effectivité a un coût dès lors qu'une intervention humaine est exigée pour refaire l'explication d'un processus automatisé[341]. Déjà consultée dans le cadre du projet de décret d'application de la LRN relatif à son volet sur la transparence administrative, la CNIL s'était prononcée en faveur d'une symétrie entre d'une part le régime juridique du droit d'accès permettant d'obtenir de manière générale la logique sous-tendue par le traitement, et d'autre part, une explication propre à la situation de l'intéressé dans le cadre des décisions administratives individuelles fondées sur un traitement algorithmique[342]. Toutefois, la CNIL souhaitait que cette symétrie informationnelle s'effectue au détriment d'une information personnalisée, mais générale, conformément au droit d'accès afin que les deux dispositions n'entrent pas en concurrence dans

[334] Nous formulerons des propositions en ce sens dans la seconde partie de ces travaux. Voir en ce sens, *Infra*., n° 717 et s.
[335] « *y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.* » selon l'article 22 du RGPD.
[336] Directive (UE) 2016/680 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, et art 22 § 2 b) du RGPD, art. 8 de la convention 108 et art. 9 de la convention 108+.
[337] Voir en ce sens le chapitre II titre II de la première partie de cette thèse.
[338] *Infra.*, n° 438 et s.
[339] Art. 22 § 2 a) du RGPD.
[340] Art. 22 § 2 c) du RGPD.
[341] A cet égard, le doyen Carbonnier ne considérait-il pas que la transparence « *elle a une substance, comme la vitre, c'est un bien, comme la vitre ; elle a donc un prix* ». Elle a donc un coût pour la société et les opérateurs économiques. Voir en ce sens, « Propos introductifs », *op. cit.*, p. 11.
[342] CNIL, délibération n° 02017-023 du 16 février 2017 portant avis sur un projet de décret relatif aux modalités de communication des règles et caractéristiques des traitements algorithmiques, p. 5.

les hypothèses où les personnes physiques soumises à des traitements de données à caractère personnel se détournent des dispositions de la LIL. Nous supposons que ce raisonnement pourrait tout à fait être encore tenu sous l'empire de la nouvelle réglementation qui est intervenue depuis. Il nous paraît nécessaire de considérer que c'est au contraire à la nouvelle version de la LIL, qui transpose et précise les dispositions du RGPD, d'opérer cet alignement. Car le fait de pouvoir rejouer les opérations et de se voir expliquer les critères de mise en œuvre du traitement à sa propre situation, est une démonstration de la conformité du traitement. La transparence des traitements algorithmiques de données à caractère personnel ne dispose de plus pas d'un degré équivalent, même lorsqu'ils ont des effets juridiques sur la personne physique concernée, ne serait-ce car il n'est pas possible d'obtenir la communication du code source et la documentation afférente permettant à des éventuels experts d'étudier la logique sous-jacente.

166. Enfin, le texte ne prend pas spécifiquement en considération les techniques d'IA. Comme le rappelle Jean-Marc Deltorn au sujet des difficultés de la transparence des modèles d'IA, « *si le principe de transparence mis en avant dans le Règlement se borne en pratique à une telle dimension « descriptive », « approximative », le risque sera alors grand qu'il ne se réduise qu'à un faux semblant, une illusion de transparence dénuée de tout effet juridique* »[343].

CONCLUSION DU CHAPITRE I

167. Au regard de ces premiers éléments, il apparaît que le principe de transparence des données personnelles se déploie à travers des techniques juridiques dont la nature et le degré sont très variables en fonction des situations, c'est-à-dire à dire qu'il s'agisse des données traitées ou du traitement en lui-même. Il est naturellement centré sur les données de la personne concernée et ne permet pas de connaître l'intégralité du fonctionnement d'un traitement, offrant finalement peu de garanties sur son étendue réelle. Il s'agit que d'une transparence théorique dont l'effectivité est relative. Nous regretterons également que les outils d'aide à la prise de décision ne soient pas appréhendés par une telle réglementation, alors qu'ils sont susceptibles d'influencer les décisions humaines. De la même manière, les droits à l'information évoqués reposent exclusivement sur les individus. Il aurait été préférable que certains groupements

[343] DELTORN J-M., « Le droit des données personnelles face à l'opacité des algorithmes prédictifs : les limites du principe de transparence », *in* NETTER E. (dir.), *Regards sur le nouveau droit des données personnelles*, *LGDJ*, 2019, p. 195.

comme des acteurs de la société civile puissent être titulaire d'un droit à l'information, dans le respect du droit des tiers, afin d'aboutir à une transparence collective.

168. Il convient désormais d'étudier comment le régime juridique des données personnelles opère une transparence nécessaire à la conformité des traitements par l'intermédiaire d'autres mécanismes.

CHAPITRE II - DE L'EFFECTIVITE DE LA TRANSPARENCE DES TRAITEMENTS DE DONNEES PERSONNELLES

169. Dans la sphère numérique, la transparence est le fait de rendre visible l'invisible. C'est tout l'enjeu de la conformité, qui vise à empêcher que les informations communiquées au titre des articles 12, 13, 14, 15 et 22 du RGPD[344], c'est-à-dire du droit à l'information et à l'explicabilité des décisions individuelles automatisées, ne soient erronées, car la personne concernée est *de facto* en situation de vulnérabilité par rapport aux responsables du traitement[345], voire des sous-traitants, à raison notamment d'une asymétrie informationnelle. Le RGPD repose donc sur des pouvoirs traditionnels de conformité par les autorités de contrôle, dont la CNIL au plan national. Ils permettent à la fois d'améliorer la transparence avant que le traitement ne soit mis en œuvre, puis de le contrôler le cas échéant *a posteriori* (Section I).

170. Au-delà de ces considérations, cette réglementation modifie l'approche de la protection sur les données personnelles en ayant fait basculer un régime d'autorisation et de formalités préalables[346] à un régime de responsabilisation des responsables de traitement et de leurs sous-traitants à des fins de simplification. En contrepartie, de nouveaux mécanismes dits de conformité ont été rendus obligatoires. Selon Margot E. Kaminski[347], le RGPD instaure pour certains d'entre-deux une gouvernance collaborative à travers des mécanismes plus novateurs, le plus souvent de droit non contraignant de façon à ce qu'il existe une complémentarité entre la puissance publique, intervenant en tant que régulateur, et les responsables du traitement, leur permettant de prendre part à l'élaboration de la réglementation. Il s'agit donc de la mise en œuvre du principe de responsabilité consistant à ce que les acteurs concernés par les obligations du RGPD démontrent leurs conformités, par eux-mêmes, et qui concourt à l'effectivité de la réglementation, dont celui du principe de transparence en matière de données personnelles, même si celui demeure imparfait (Section 2).

---

[344] S*upra.,* n°80 et s.
[345] Voir en ce sens, DOUVILLE T., HERVOCHON C., NOEL E., PAQUIER Y., « Les vulnérabilités numériques », *Les Cahiers de la Recherche sur les Droit Fondamentaux,* 2020, p. 111.
[346] *Infra*., n° 208 et s.
[347] KAMINSKI M, E., « *Binary Governance : Lessons from the GDPR's Approche to Algorithmic Accountability* », *op. cit*., p. 1609.

SECTION 1 - LES POUVOIRS TRADITIONNELS DES AUTORITES DE CONTROLE

171. La CNIL est la première AAI désignée en tant que tel par le législateur de l'histoire du droit français[348]. Cela démontre que le législateur souhaitait que cette commission soit indépendante du pouvoir politique dans le cadre de sa composition et de son fonctionnement. Compte tenu des nouveaux enjeux, et de l'exacerbation des problématiques relatives au numérique, il n'est pas déraisonnable de penser qu'une telle autorité, avec des compétences élargies, et un budget à la hauteur de ses missions, soit désormais instituée avec un statut qui va au-delà de ce que les autorités administratives indépendantes permettent aujourd'hui. Mais avant d'aborder ce sujet dans la deuxième partie de ces travaux[349], il est nécessaire d'analyser dans leur généralité les prérogatives dont dispose la CNIL pour parvenir à l'effectivité de la transparence des traitements algorithmiques de données à caractère personnel. Il est par ailleurs à noter que la CNIL, depuis l'immixtion du droit de l'Union dans ce domaine, est également sous la supervision du CEPD afin d'uniformiser l'application de ce nouveau droit au sein des Etats membres, mais aussi de la Commission européenne.

172. La CNIL dispose de pouvoirs susceptibles de concourir à la transparence des traitements de données personnelles en amont de leur mise en œuvre. Toutefois, au-delà de la mission préventive de cette institution (Paragraphe 1), qui demeure par ailleurs insuffisante pour les raisons que nous évoquerons, elle jouit d'un important pouvoir coercitif permettant de contrôler les traitements une fois déployés par les responsables du traitement et de leurs sous-traitants (Paragraphe 2).

PARAGRAPHE 1 - Les pouvoirs concourant *ex ante* à la transparence des traitements

173. Au-delà des mécanismes de responsabilité des acteurs que nous aborderons ultérieurement, et à laquelle la CNIL participe, les pouvoirs traditionnels de cette autorité, et susceptibles de concourir *ex ante* à la transparence des traitements algorithmiques de données à caractère personnel, repose davantage sur un droit souple (A) que règlementaire, ce qui aboutit, notamment du fait de la fin du régime d'autorisation de nombreux traitements sous

[348] Art. 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[349] *Infra*., n° 717 et s.

l'empire de l'ancienne règlementation, à un affaiblissement de cette dernière en tant que contre-pouvoir technique (B).

A - Un pouvoir de proposition et de droit souple

174. La CNIL dispose d'un rôle en matière d'informations auprès des personnes physiques afin de les informer au sujet de leurs droits, mais également auprès des responsables du traitement, qu'ils soient privés ou publics dans le but de les renseigner sur leurs obligations, y compris sur le respect des droits des personnes parmi lesquels la transparence des données personnelles traitées bénéficie d'une place centrale[350]. L'article 8 § 1 1° de la LIL dispose en ce sens qu'« *elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations et peut, à cette fin, apporter une information adaptée aux collectivités territoriales, à leurs groupements et aux petites et moyennes entreprises* ». La commission peut aussi être sollicitée par de nombreux acteurs publics auprès desquels elle exerce une mission de conseil[351]. Elle répond également aux demandes d'avis formulés par les pouvoirs publics[352], y compris des autres autorités administratives indépendantes.

175. Au-delà de l'avis obligatoire au titre des articles 31 et 32 de la LIL[353], elle est consultée pour tout projet de loi ou de décret portant sur le traitement de données personnelles ou sur leur protection au sens large[354]. Nous regrettons sur ce point que cette consultation ne porte que sur les projets, qui certes sont importants afin que les parlementaires puissent le cas échéant bénéficier de son expertise lors des débats, alors qu'il serait en revanche plus constructif qu'elle intervienne tout le long du processus parlementaire ou règlementaire en vue de prodiguer les meilleurs conseils possibles. En effet, les projets ressemblent rarement à la version définitive qui pourtant s'imposera. Elle est également susceptible d'être force de proposition concernant l'évolution des régimes juridiques comme cela est le cas au sujet du projet de règlement européen de la Commission européenne relatif à l'IA[355].

176. Elle effectue par ailleurs des actions de médiation. Il s'agit dans ce cas d'un important volet visant à prévenir les violations à la réglementation. Cette institution joue également un

[350] *Supra.,* n° 80 et s.
[351] Art. 57 1 § 1 c) du RGPD.
[352] Art. 8 § 2 2° e) de la LIL modifiée.
[353] *Infra*., n° 183.
[354] Art. 8 § 2 4° a) de la LIL modifiée.
[355] La CNIL ainsi que ses homologues européens ont formulé un avis conjoint à ce sujet. Voir en ce sens, EDPB-EDPS, *Joint opinion 5/2021, on the proposal for a Regulation of the European Parliament and of the Concil laying down harmonised rules on artificial intelligence,* 18 juin 2021.

rôle de sensibilisation et de recueil de doléances auprès de nombreux publics. Elle a par exemple effectué une concertation citoyenne sur les enjeux de l'IA et des algorithmes ayant abouti à un rapport dans lequel figure d'intéressantes recommandations[356], notamment sur la transparence des algorithmes que nous serons amenés à évoquer dans la seconde partie de ces travaux[357]. Son laboratoire d'innovation numérique (LINC)[358] ambitionne de cerner les enjeux prospectifs, ce qui lui permet de s'émanciper de la mission traditionnelle de régulateur tout en étant force de proposition.

177. En plus des avis qu'elle émet à la demande des pouvoirs publics, la LIL[359] permet de plus aux juridictions de solliciter la CNIL à des fins d'expertise. Sur ce dernier point, il est à noter qu'en matière pénale elle doit saisir le procureur de la République dès lors que sont portés à sa connaissance des faits criminels ou délictueux, et ce conformément à l'article 40 du Code de procédure pénale (CPP) et lui formuler un avis sans délai[360]. S'ajoute à cela la possibilité de « *présenter des observations dans les procédures pénales* »[361], mais également devant toute autre juridiction si le contentieux est relatif à la protection des données à caractère personnel[362]. Ainsi, *« la juridiction d'instruction ou de jugement peut appeler le président de la Commission nationale de l'informatique et des libertés ou son représentant à déposer ses observations ou à les développer oralement à l'audience* »[363]. Lorsque de telles procédures interviennent, le traitement de données est certes déjà mis en œuvre, mais la CNIL est susceptible d'exercer une influence par l'intermédiaire d'interprétation du droit en précisant la portée d'une disposition amenée à se pérenniser dans la jurisprudence pour une meilleure effectivité de la transparence et donc des droit et libertés. Elle participe donc d'une certaine manière à l'action juridictionnelle.

[356] CNIL, Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, *www.cnil.fr* [en ligne]. Décembre 2017. [Consulté le 2 décembre 2020]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
[357] *Infra.*, n° XXX.
[358] Site du Laboratoire d'Innovation Numérique de la CNIL [en ligne]. [Consulté le 2 juillet 2021]. Disponible à l'adresse : https://linc.cnil.fr
[359] Art. 8 § 1 4°e) de la LIL modifiée.
[360] Art. 8 § 1 4°f) de la LIL modifiée.
[361] *Ibid*.
[362] Art. 8 § 1 5° de la LIL modifiée.
[363] Art. 41 de la LIL modifiée.

178. La CNIL recourt notamment aux lignes directrices[364] et aux recommandations afin de venir préciser, voire interpréter la réglementation applicable[365]. En tant qu'autorité de contrôle indépendante, elle siège également au sein du CEPD, ce qui lui offre la possibilité de participer à l'interprétation des dispositions au niveau européen. A ce titre, elle a concouru à l'élaboration des lignes directrices sur la transparence[366]. Toutefois, ces actes de droit souple ne peuvent être de portée générale et absolue[367]. Il convient donc d'en déduire que la CNIL ne pourrait pas aboutir à une interprétation particulièrement large des obligations des responsables du traitement en matière de transparence. Ce droit souple est par ailleurs susceptible de recours s'il fait grief, ce qui correspond parfaitement à la nature de ces recommandations qui font droit[368]. Elle peut donc établir des règles en matière de transparence, mais certaines lignes directrices laissent à penser que les droits des personnes concernées font l'objet de régression par rapport à la réglementation afin de favoriser les acteurs économiques dans leurs transitions. En ce sens, le 17 septembre 2020, elle avait encore décidé de repousser de six mois la mise en conformité des acteurs en matière de « cookies et autres traceurs » dans de nouvelles lignes directrices[369], alors pourtant que la règlementation générale et sectorielle relative aux données à caractère personnel est en application et connue depuis de nombreuses années[370].

B - L'affaiblissement du pouvoir de décision de la CNIL

179. Afin notamment de favoriser la circulation des données dans le cadre du libre marché européen, le régime d'autorisation préalable avant la mise en œuvre de nombreux traitements, s'est en grande partie substitué à une logique de responsabilité des acteurs[371]. Nous notons à

[364] Le Comité consultatif de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel élabore également des lignes directrices. A titre d'exemple, il a récemment proposé par cette intermédiaire un régime juridique sur la reconnaissance faciale. Voir en ce sens, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, lignes directrices sur la reconnaissance faciale, 28 janvier 2021.
[365] Art. 8 § 2 2° b) de la LIL modifiée.
[366] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018.
[367] CE, n° 434684, 19 juin 2020.
[368] *« Les documents de portée générale émanant d'autorités publiques, matérialisés ou non, tels que les circulaires, instructions, recommandations, notes, présentations ou interprétations du droit positif peuvent être déférés au juge de l'excès de pouvoir lorsqu'ils sont susceptibles d'avoir des effets notables sur les droits ou la situation d'autres personnes que les agents chargés, le cas échéant, de les mettre en œuvre. Ont notamment de tels effets ceux de ces documents qui ont un caractère impératif ou présentent le caractère de lignes directrices »*, CE, n° 418142, 12 juin 2020.
[369] CNIL, délibération n° 2020-091 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.
[370] En ce sens, le RGPD est en application depuis le 25 mai 2018, tandis que la transposition de la directive 2002/58/CE du 12 juillet 2002, dite « *eprivacy* » modifiée en 2009, a été effectuée par l'ordonnance n° 2018-1125 du 12 décembre 2018.
[371] *Infra.*, n° 208 et s.

regret une tendance à l'affaiblissement des pouvoirs contraignants de la CNIL ayant pourtant participer à la transparence des traitements de données personnelles.

180. Au-delà de son pouvoir règlementaire portant sur l'édiction de son règlement intérieur, la CNIL dispose également d'un tel pouvoir afin d'adopter des règlements types contraignants. Ils ne sont cependant possibles qu'« *en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données biométriques, génétiques et de santé* »[372]. A titre d'exemple, la CNIL a édicté un règlement *« relatif à l'accès par authentification biométrique sur les lieux de travail* ». Il précise la mise en œuvre de l'article 12 et suivants du RGPD dans ce domaine, concourant par cet intermédiaire à la transparence[373].

181. Autrefois obligatoires, le RGPD a mis fin aux autorisations préalables qui portaient sur certaines catégories de données, ce qui à notre sens est regrettable dans la mesure où ce mécanisme permettait indiscutablement de contrôler un traitement avant sa mise en œuvre, et le cas échéant de ne pas l'autoriser si les garanties, notamment de transparence n'étaient pas respectées. Cela explique pourquoi les dispositifs biométriques ne sont désormais plus soumis à une telle autorisation. Toutefois, la CNIL est toujours susceptible de se prononcer sur certains traitements, ne serait-ce car le législateur national[374] les a maintenus pour quelques rares exception dans la LIL. Tel est encore le cas pour certains traitements de données de santé[375]. Mais contrairement à la directive 95/46/CE, le RGPD en a simplifié la tenue.

182. Comme l'indique Christina Koumpli dans sa thèse à propos des formalités préalables à effectuer par le responsable du traitement,

> « *(…) il est important de relever que les processus de simplification ont contribué de manière notable à une moindre transparence. Comme la doctrine l'a noté, « la disparition progressive des formalités pose (...) une difficulté puisqu'elle diminue la capacité de contrôle des personnes concernées sur les traitements ». Or, ce*

[372] Art. 8 § 1 2° c) de la LIL de 1978 modifiée.
[373] Le droit à l'information dans ce domaine, au titre du règlement type de la CNIL, « *doit figurer dans une notice écrite remise par le responsable de traitement à chaque personne concernée préalablement à l'enrôlement des données biométriques de ce dernier* ». Voir en ce sens, délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, art. 9.
[374] Conformément à l'art. 9 § 4 du RGPD.
[375] Lire en ce sens, CLUZEL-METAYER L., FRANCOIS A., « La protection des données personnelles à l'épreuve de la télémédecine », *RDSS*, 2020, p. 51-59.

contrôle est la manifestation même du droit fondamental à la protection des données personnelles selon certains auteurs »[376].

183. De plus, certains « *traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat* »[377], ne pouvaient être mis en service qu'après un avis motivé de la CNIL[378]. Mais il ne s'agit plus d'un avis conforme depuis 2004[379], ce qui affaiblit la mission préventive de protection des libertés et de contre-pouvoir technique de cette institution. Cet avis conforme était pourtant qualifié par certains auteurs, dont Christina Koumpli, de pouvoir règlementaire attribué à la Commission par le législateur originel de la LIL de 1978[380]. Dans le contexte particulier de la Covid-19, les parlementaires avaient adopté, dans une disposition du projet de loi prorogeant l'urgence sanitaire[381], la réintroduction de l'avis conforme de la CNIL au sujet des décrets mettant en œuvre les systèmes d'information en matière de santé. A défaut de l'aval de la CNIL, les traitements de données déployés dans le cadre de l'urgence sanitaire n'auraient pas pu être déployés. Toutefois, le Conseil constitutionnel a déclaré cette disposition inconstitutionnelle dans la mesure où le législateur ne peut « *subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire* »[382].

---

[376] KOUMPLI C., *Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données à caractère personnel : étude comparée : Union européenne, Allemagne, France, Grèce, Royaume-Uni*, Thèse de doctorat, soutenue à l'Université Paris 1 Panthéon-Sorbonne le 18 janvier 2019, spec. p. 455.

[377] Il s'agit des traitements de données à caractère personnel visés par les article 31 et 32 de la LIL tels que « *1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ; 2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. » mais également ceux pris dans le cadre de « l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.* ».

[378] Art. 8 § 1 2° a) de la LIL modifiée.

[379] Avant la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, si la CNIL rendait un avis défavorable pour un traitement de cette nature, seulement un décret pris sur avis conforme du Conseil d'Etat permettait la mise en œuvre de ce dernier (art 15 de la LIL de 1978).

[380] KOUMPLI C., *Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données à caractère personnel : étude comparée : Union européenne, Allemagne, France, Grèce, Royaume-Uni, op. cit.*, spec. p. 32.

[381] Art. 11 § V, Assemblée Nationale, projet de loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, n° 418, en date du 9 mai 2020.

[382] CC, décision n° 2020-800 DC, 11 mai 2020, *Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions*, § 77, « *en vertu de l'article 21 de la Constitution et sous réserve de son article 13, le Premier ministre exerce le pouvoir réglementaire à l'échelon national. Ces dispositions n'autorisent pas le législateur à subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire. Dès lors, le mot « conforme » figurant à la première phrase du paragraphe V de l'article 11 est contraire à la Constitution.* ».

184. La CNIL a pu s'illustrer différemment lors de son avis sur le projet en demandant la transparence du dispositif « *StopCovid* »[383] en allant au-delà des droits garantis par le RGPD et la LIL[384]. En effet, elle a considéré qu'

> « *une transparence renforcée quant au mode de fonctionnement et aux finalités de traitement, est un élément déterminant pour assurer la confiance dans le dispositif et favoriser son adoption par une partie significative de la population* »[385]

185. Concrètement, cette transparence renforcée se caractérise par d'une part la recommandation et la publication d'une analyse d'impact, d'autre part, la recommandation par la CNIL d'un accès aux protocoles et au code source de l'application, et aux paramétrages du serveur gérant les notifications. Le but étant notamment « *de permettre à la communauté scientifique de contribuer à l'amélioration constante du dispositif et à la correction des éventuelles vulnérabilités* », notamment afin que des remarques puissent nourrir le débat au sein de la communauté scientifique et soient prises en compte. Il est à noter que selon la commission, la communication de ces informations n'a pas pour but principal d'assurer la transparence vis-à-vis de l'ensemble des citoyens, ce qui serait sans doute d'un intérêt limité car trop technique, mais de s'assurer de la conformité du traitement par une garantie collective par l'intermédiaire de la société civile.

186. Finalement, dans sa délibération du 25 mai 2020 portant sur le projet de décret instaurant ce traitement[386], le gouvernement ne souhaitait pas transmettre l'intégralité du code source de l'application ainsi que certains paramétrages du serveur central au motif qu'il existerait un danger pour « *l'intégrité et la sécurité de l'application* ». La commission n'a pas hésité à insister sur la nécessité de diffuser ce code conformément aux engagements du secrétaire d'Etat du numérique, Cédric O, lors de ses déclarations. Elle a rappelé que *« même si le paramétrage des logiciels utilisés et le détail des mesures de sécurité n'ont pas vocation à être rendus publics, il est important que l'intégralité du code source soit quant à lui rendu public »*, ce que le décret final repris[387]. Elle a par ailleurs incité à ce que le code source de « *TousAntiCovid*

[383] Selon le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « *StopCovid* » il s'agit d'un traitement « *qui permet à ses utilisateurs d'être informés lorsqu'ils ont été à proximité d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus du covid-19, grâce à la conservation de l'historique de proximité des pseudonymes émis via la technologie Bluetooth* ». Il est désormais appelé « *TousAntiCovid* ».
[384] *Supra.*, n° 80 et s.
[385] CNIL, délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « *StopCovid* ».
[386] Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « *StopCovid* ».
[387] Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « *StopCovid* ».

Vérif », application utilisée afin d'assurer la validité du passe sanitaire, soit rendu public mais « *expurgé, le cas échéant, des secrets permettant de sécuriser les transmissions de données avec les serveurs centraux* »[388].

187. La CNIL peut également publier certains avis consultatifs, notamment afin qu'ils soient repris par la presse, ce qui exerce par cet intermédiaire une influence sur les autres acteurs. Néanmoins, ce rôle de proposition, de droit souple, demeure faible, car il ne s'agit plus d'un avis conforme, et elle ne peut donc s'opposer à la mise en œuvre d'un tel traitement quand bien même il serait liberticide, alors que cette institution était pourtant initialement pensée pour être un contre-pouvoir de nature technique[389] par le législateur originel.

PARAGRAPHE 2 - Les pouvoirs permettant l'observation du traitement

188. Initialement, lors des débats parlementaires, la CNIL ne devait pas être une AAI, mais un Comité de surveillance muni d'un pouvoir d'investigation permettant d'une part de recueillir les plaintes des personnes physiques, et d'autre part d'enquêter sur ces éventuelles violations à la législation de la LIL. Ce comité ne disposant pas quant à lui d'une compétence juridictionnelle, il avait la faculté de saisir une section du Tribunal administratif de Paris agissant en qualité de Tribunal de l'informatique[390].

189. Dans ce cas de figure, l'observation du traitement s'effectue *a posteriori*, c'est-à-dire lorsque le traitement est mis en œuvre dans les faits. Ces pouvoirs consistent donc en leur observation, afin, le cas échéant, de remédier aux manquements du responsable du traitement ou de leur sous-traitant.

190. De manière générale, les autorités de contrôle indépendante, dont la CNIL, disposent aussi bien d'un pouvoir d'enquête (A) que de coercition (B). Et eu égard à ce pouvoir de

[388] CNIL, délibération n° 2021-067 du 7 juin 2021 portant avis sur le projet de décret portant application du II de l'article 1er de la loi n° 2021-689 du 31 mai 2021 relative à la gestion de la sortie de crise sanitaire, p.8.
[389] *Supra.*, n° 183.
[390] FOYER M., Rapport n° 3125 sur le projet de loi relatif à l'informatique et aux libertés de l'Assemblée nationale, 5e législature, fait au nom de la commission des Lois, enregistré à la Présidence de l'Assemblée nationale le 4 octobre 1977 relatant la proposition de loi n° 1454 par M. Poniatowski. Une proposition de loi sénatoriale (n° 144-1973-74 déposée par M. Caillavet) visait également à la création non pas d'un comité de surveillance, mais d'un directoire de l'informatique bénéficiant toutefois des mêmes compétences.

coercition, la CNIL dispose d'un pouvoir juridictionnel au sens d'un pouvoir de sanction comme de nombreuses autres AAI[391].

A - Le pouvoir d'investigation

191. Dès lors qu'une autorité de contrôle dispose des compétences et de la confiance des citoyens, ce qui n'est pas par ailleurs sans poser la question de la transparence de l'action de cette institution, il n'est pas inconsidéré d'attendre que l'information soit médiée par cette autorité à l'utilisateur s'il s'agit de procédés sensibles remettant en cause les droits fondamentaux d'autrui. Mais cela implique qu'elle bénéficie de tous les pouvoirs permettant de s'assurer de la conformité effective des traitements. En effet, la crainte légitime est que les responsables du traitement utilisent les secrets protégés par la loi pour pérenniser l'opacité de ces systèmes.

192. Les plaintes et réclamations[392] des personnes concernées, voire d'autres acteurs, auprès de la CNIL, jouent un rôle majeur en matière de transparence dans la mesure où elles vont éveiller les soupçons sur certains manquements. En effet, lorsque les griefs sont corroborés par des éléments probants, elles engendreront des enquêtes pouvant déboucher sur des constatations de violation. C'est donc un rôle d'alerte indispensable sur les traitements opérés, et ce d'autant plus que la société civile œuvre également au signalement des mauvaises pratiques. A titre d'exemple, de nombreux utilisateurs signalent sur Twitter à la CNIL les manquements qu'ils découvrent au quotidien. Les autres autorités de contrôle indépendantes des Etats membres de l'Union peuvent également lui adresser des signalements[393]. La Commission peut de plus se saisir de sa propre initiative.

193. Toutefois, ces dernières années, la CNIL ne semble pas avoir la capacité de faire face à l'afflux de plaintes, notamment car les traitements de données personnelles se sont immiscés dans d'innombrable domaines et de nombreux acteurs sont encore dans la méconnaissance de la nouvelle réglementation, alors que les moyens matériels et humains de cette institution

[391] En ce sens, lire BRUNET F., « De la procédure au procès : le pouvoir de sanction des autorités administratives indépendantes », *RFDA*, 2013, p. 113-126.
[392] Art. 8 § I 2° b) de la LIL modifiée et art 57 § 1 f) du RGPD.
[393] Art. 57 § 1 f), g) et h) du RGPD.

demeurent minces au regard de l'enjeu. A ce titre, certains justiciables se désintéressent des autorités de régulation en intentant directement des actions en justice[394].

194. Le pouvoir d'investigation des autorités de contrôle est essentiel puisqu'il permet de constater ou non la conformité effective des traitements algorithmiques à la réglementation. A cette fin, le RGPD et le droit national prévoient certaines compétences en matière d'enquête. Toutefois, au sens de la directive « Police-Justice »[395], la CNIL est exclue du contrôle des traitements opérés par les juridictions dans le cadre de leurs missions, logiquement pour des raisons de séparation des pouvoirs[396].

195. L'autorité de contrôle bénéficie du pouvoir de se faire communiquer « *toute information dont elle a besoin pour l'accomplissement de ses missions* » aussi bien de la part du responsable du traitement que du sous-traitant[397]. Elle peut également mener des audits afin de constater ou non la conformité des algorithmes au RGPD, ce qui nécessite d'accéder au traitement, assurant une transparence de ces derniers auprès de l'autorité de contrôle[398]. Un comité d'audit du système national des données de santé a par ailleurs été institué par la LIL[399].

196. Dans le cadre de ce pouvoir d'enquête, le contrôleur est susceptible d'accéder aux locaux du responsable de traitement, et le cas échéant du sous-traitant, ainsi qu'à « *toute installation et à tout moyen de traitement* »[400]. Plus généralement, le contrôleur peut accéder à toutes les données à caractère personnel, ainsi qu'à toutes les informations afférentes, dans le cadre de ses prérogatives[401]. Le recours à des experts par la Commission est de plus précieux notamment pour effectuer des audits et bénéficier du plus d'éléments possibles sur le traitement

---

[394] MANANCOURT V., Have a GDPR complaint ? Skip the regulator and take it to court, *Politico.eu*. 30 août 2020, mis à jour le 1er septembre 2020. [Consulté le 04 octobre 2020]. Disponible à l'adresse : https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/

[395] Directive (UE) 2016/680 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.

[396] Art. 55 § 3 du RGPD.

[397] Art. 58 § 1 a) du RGPD.

[398] Art. 58 § 1 b) du RGPD.

[399] Art. 77 de la LIL modifiée.

[400] Art. 58 §1 f) du RGPD. L'article 19 III de la LIL modifiée précise par ailleurs que *« les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 10 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel. Le procureur de la République territorialement compétent en est préalablement informé* ».
En cas de refus du responsable du traitement ou de son sous-traitant, le juge des libertés et de la détention peut néanmoins autoriser lesdites vérifications, y compris dans un lieu privé. Voir en ce sens, art. 25 à 32 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[401] Art. 58 § 1 e) du RGPD et dans les conditions prévues à l'art. 19 de la LIL modifiée.

mis en œuvre[402]. Toutefois, l'article 19 III de la LIL précise que « *le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous réserve du deuxième alinéa du présent III, par le secret médical* ». Des contrôles en ligne[403] et des auditions[404] sont par ailleurs susceptibles d'être effectués.

197. Au-delà de ces pouvoirs de contrôle des traitements mis en œuvre, force est de constater que la CNIL demeure une AAI pourvue de seulement 225 agents en 2020, dont le département de la conformité ne représente que 24% de l'effectif, ce qui n'a permis d'aboutir seulement à 74 contrôles sur pièce sur ladite année[405]. Cette faible performance en matière de contrôle n'est pas due aux circonstances exceptionnelles de la pandémie de SARS-CoV-2 puisqu'en 2019 ce chiffre n'était que de 45[406]. Elle s'explique surtout par son faible budget annuel de 20,1 millions d'euros[407].

198. En matière d'enquête, il convient de noter que les transferts de données vers les Etats tiers à l'Union européenne sont un défi majeur. Or, à titre d'exemple, en vertu du principe de compétence territoriale, l'autorité de contrôle irlandaise se retrouve être en première ligne car le siège social européen de nombreux géants du numérique s'y trouve, ce qui a pour incidence qu'elle exerce ce pouvoir d'enquête à l'encontre de ces sociétés en tant que chef de file[408]. C'est donc en grande partie elle qui est la garante de l'effectivité du RGPD, y compris pour les requêtes formulées à l'encontre de ces géants dans d'autres Etats de l'Union. Même si les autorités de contrôle européenne coopèrent mutuellement[409], des enjeux politiques et économiques nationaux sont susceptibles de nuire à l'effectivité de la réglementation européenne sur les données personnelles. Une résolution du Parlement européen met en exergue ce risque au sujet de cette autorité irlandaise. Les parlementaires notent que le commissaire irlandais a laissé en suspens de nombreuses réclamations et plaintes relatives à des suspicions de violations du RGPD par ces grands groupes. Les députés remettent par ailleurs en cause la

[402] Art. 35 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[403] *Ibid*., art. 33.
[404] *Ibid*., art. 34.
[405] CNIL, Rapport d'activité 2020 de la Commission Nationale de l'Informatique et des Libertés, p. 7, *www.cnil.fr* [en ligne]. Juin 2020. [Consulté le 27 août 2021]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_41e_rapport_annuel_-_2020.pdf.
[406] CNIL, Rapport d'activité 2019 de la Commission Nationale de l'Informatique et des Libertés, p. 3, *www.cnil.fr* [en ligne]. Juin 2020. [Consulté le 27 août 2021]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf
[407] CNIL, Rapport d'activité 2020 de la Commission Nationale de l'Informatique et des Libertés, *op. cit.*
[408] Art. 56 du RGPD.
[409] Art. 60 du RGPD.

compétence de l'institution qui ne serait pas suffisamment dotée en moyen humain pour saisir les enjeux technologiques. Ainsi, et au regard des risques pour l'effectivité des droits des personnes, le législateur européen demande à la Commission européenne « *d'engager une procédure en manquement à l'encontre de l'Irlande pour absence de contrôle satisfaisant de l'application du RGPD* »[410].

199. Lorsque l'on constate l'impossibilité d'enquêter sur place afin de constater le véritable fonctionnement des traitements algorithmiques de ces sociétés, il n'est pas étonnant que la CJUE[411] ait décidé d'invalider le *privacy shield*, non pas sur le fondement de preuves de violation de droits fondamentaux, mais sur le risque théorique, en l'absence de garanties suffisantes, que pouvait engendrer le transfert des données à caractère personnel des personnes physiques de l'Union vers les Etats-Unis d'Amérique. Cette approche par les risques, nous serons amenés à l'étudier de manière approfondie lorsque nous aborderons le projet de règlement général sur l'IA[412].

200. Il est à noter que la CNIL n'est pas compétente pour enquêter à propos de certains traitements intéressant la sûreté de l'Etat[413], ce qui nuit à son action. Bien que d'autres autorités administratives puissent être compétentes à cet effet, elles n'offrent toutefois pas le même niveau de garantie sur la transparence de ces traitements.

B - Les pouvoirs coercitifs

201. Ses pouvoirs sont généraux, allant de l'avertissement[414], de la mise en demeure[415] à des sanctions[416]. En cas de non-respect des obligations prévues par le RGPD, l'autorité peut rappeler à l'ordre le responsable de traitement ou un sous-traitant lorsque le traitement est contraire au RGPD[417] ou bien les avertir le cas échéant qu'ils sont susceptibles de violer des obligations en matière de transparence notamment[418]. Dans l'hypothèse où l'exercice des droits de la personne physique comme le droit à l'information ou d'accès au traitement est remise en

[410] Résolution du Parlement européen du 20 mai 2021 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 Maximillian Schrems (« arrêt Schrems II »).
[411] CJUE, Grande chambre, affaire C-311/18, 16 juillet 2020.
[412] *Infra.*, n° 946 et s.
[413] En ce sens, art. 19 IV de la LIL modifiée. Nous aborderons ce point en détail plus tardivement lors de nos propositions, *Infra.*, n° 707 et s.
[414] Art. 20 I de la LIL modifiée.
[415] Art. 20 II de la LIL modifiée.
[416] Art. 20 III de la LIL modifiée.
[417] Art. 58 § 2 b) du RGPD
[418] Art. 58 § 2 a) du RGPD

cause, l'autorité peut ordonner cette mise en conformité[419]. En effet, nous ne pouvons pas seulement compter sur la bonne foi des entreprises et de leur DPD[420], quand bien même celui-ci serait certifié par la CNIL. Elle est également à même d'infliger une interdiction de traitement des données à caractère personnel définitive ou pour une durée déterminée[421].

202. Les sanctions peuvent par ailleurs être très strictes dès lors qu'elles sont « *effectives, proportionnées et dissuasives* »[422], y compris en cas de non-respect aux obligations du RGPD, et donc du principe de transparence en matière de données personnelles. Comme nous le verrons ultérieurement, le mécanisme de certification joue un rôle important dans le respect de la transparence des traitements, et il est à noter qu'en cas de violation des obligations, il est possible pour l'autorité de retirer une certification ou d'imposer à l'organisme certificateur un tel retrait[423] ainsi que d'interrompre le flux de données à caractère personnel vers un Etat tiers à l'Union européenne par l'intermédiaire d'une procédure d'urgence nationale[424]. Les sanctions administratives peuvent donc être prononcées cumulativement à ces mesures[425].

203. A titre d'exemple, dans le cadre d'un contrôle des systèmes automatisés de données, utilisés lors de l'urgence sanitaire relatif à la crise de la Covid 19, dont celui de « *StopCovid* », la CNIL a opéré un contrôle de conformité. Il est apparu que cette application n'était pas conforme au décret l'instaurant[426], y compris en matière de transparence. Elle a rappelé que les traitements de données à caractère personnel « *doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée* » conformément à l'article 5 § 1 a) du RGPD. Il est intéressant de noter que la transparence est un principe fondamental en ce qu'il permet de s'assurer que les traitements sont conformes au droit, ce qui aboutira notamment à une mise en demeure du ministère des Solidarités et de la santé[427].

---

[419] Art. 58 § 2 c) et d) du RGPD.

[420] Le délégué à la protection des données est institué par l'article 37 du RGPD remplace le correspondant informatique et libertés. Il vise à assurer la mise en conformité d'un organisme avec la réglementation. En vertu de l'article 37 § 1 du RGPD, le recours à un DPD est obligatoire lorsque « *a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;*
b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ».

[421] Art. 58 § 2 f) du RGPD.

[422] Art. 83 § 1 du RGPD.

[423] Art. 58 § 2 h) du RGPD.

[424] Art. 58 § 2 j) du RGPD.

[425] Art. 83 § 2 du RGPD.

[426] Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « *StopCovid* ».

[427] Décision n° MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des solidarités et de la santé. Cette mise en demeure fut par ailleurs clôturée après régularisation par la décision n° 2020-015 du 3 septembre 2020.

204. La CNIL dispose d'une mission significative en matière de sanctions administratives lorsqu'elle intervient en tant que Tribunal[428]. Les sanctions sont en théorie particulièrement dissuasives. Lorsque les violations portent sur le droit des personnes concernées, et donc aux obligations de droit à l'information et à la transparence ainsi qu'au droit d'accès par exemple, la condamnation peut s'établir jusqu'à 4% du chiffre d'affaires mondial de l'entreprise mettant en œuvre le traitement, et ce dans la limite d'un plafond de 20 millions d'euros[429]. En revanche, en cas de violation au principe de responsabilité[430], de certification, de la protection des données dès la conception, de registre ou d'analyse d'impact tels que nous les étudierons, parce qu'ils concourent à la compréhension de ces systèmes, une amende administrative d'un montant de 2% du chiffre d'affaires mondial de l'entreprise peut être infligée, dans la limite d'un plafond de 10 millions d'euros[431].

205. En ce sens, la première sanction ayant été prononcées par la CNIL[432] en application des dispositions du RGPD portait d'ailleurs sur un défaut d'informations sur le fondement des articles 6, 12 et 13 de cette règlementation, donc de transparence. La formation restreinte de la Commission a également constaté que la communication des informations aux personnes physiques concernées était en l'espèce difficilement accessible, car se trouvant dans de multiples documents différents telles que les conditions générales d'utilisation. De plus, concernant le caractère aisément compréhensible des informations fournies, la collecte des données et l'information afférente, ne permettait pas à l'utilisateur de prendre conscience de l'ampleur du traitement réalisé, alors que « *considérée isolément, la collecte de chacune de ces données est susceptible de révéler avec un degré de précision important de nombreux aspects parmi les plus intimes de la vie des personnes dont leurs habitudes de vie, leurs goûts, leurs contacts, leurs opinions ou encore leurs déplacements. Le résultat de de la combinaison entre elles de ces données renforce considérablement le caractère massif et intrusif des traitements dont il est question* »[433].

206. Compte tenu des errements de son homologue irlandaise en matière de respect de la règlementation générale sur les données personnelles[434] par les principaux géants du numérique

[428] Art. 58 § 2 i) du RGPD.
[429] Art. 83 du RGPD.
[430] *Infra*., n° 208 et s.
[431] *Ibid.*
[432] A titre d'exemple, voir délibération de la CNIL formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC. Cette délibération a par ailleurs été confirmée par le Conseil d'Etat dans un arrêt du 19 juin 2020, n° 430810.
[433] *Ibid*.
[434] *Supra*., n° 198.

puisqu'elle est l'autorité chef de file du fait de l'établissement de leur siège social, la CNIL les sanctionne par contournement. Elle recourt à des dispositions spéciales relatives aux traceurs (cookies) prévues par la directive « *ePrivacy* »[435] et sa transposition en droit national qui n'imposent pas ce guichet unique. Ainsi, l'autorité peut se fonder sur un manquement aux obligations d'information à des fins de consentement à ces traceurs[436]. A ce titre, elle a par exemple condamné le 7 décembre 2020 la société Google à une amende de 100 millions d'euros (40 millions d'euros à Google Ireland Limited et 60 millions d'euros à l'encontre de Google LLC)[437].

207. Au-delà de ces pouvoirs traditionnels conférés aux autorités de contrôle que nous venons de voir, le RGPD compte avant tout sur une logique de responsabilisation des acteurs.

SECTION 2 - UNE CONFORMITE A GEOMETRIE VARIABLE PREVUE PAR LE RGPD

208. Nous traiterons seulement des dispositions relatives à la conformité permettant au responsable du traitement de démontrer que les informations qu'il fournit, au titre des articles 12, 13, 14, 15 et 22 du RGPD[438], représentent dans les faits la réalité du traitement. En effet, sans ces dispositifs de conformité, en dehors des contrôles effectués par la CNIL qui restent marginaux[439], il ne serait pas possible de vérifier que les informations fournies aux personnes physiques sont correctes. De la conformité dépend l'effectivité des droits des personnes concernées au titre du RGPD, mais également des violations des libertés impactées par les traitements algorithmiques, bien que cela n'ait pas été philosophiquement pensé comme tel. En effet, la transparence prévue par cette réglementation semble être mise en œuvre seulement pour garantir l'exercice des autres droits protégés par le RGPD, ni plus ni moins.

---

[435] 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).

[436] L'article 82 de la LIL modifiée dispose en effet que sauf exception « *Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :*
1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;
2° Des moyens dont il dispose pour s'y opposer ».

[437] CNIL, Délibération SAN-2020-012 du 7 décembre 2020. Pour un commentaire de cette sanction, voir CRICHTON C., « Cookies : la CNIL sanctionne Google et Amazon », *Dalloz actualité*, 17 décembre 2020.

[438] *Supra.*, n° 80 et s.

[439] *Supra.*, n° 206 et s.

209. Parmi les obligations générales incombant au responsable du traitement, nous retrouvons ce que le règlement nomme « *responsabilité* »[440]. Cette obligation de « responsabilité », émanant de l'anglais « *accountability* » doit surtout être entendue comme un principe de conformité, de redevabilité et donc d'adéquation, le plus souvent mou, car relevant essentiellement du droit souple contrairement aux mécanismes mettant en œuvre les droits individuels de transparence tel que le droit à l'information ou encore d'accès aux traitements algorithmiques.

210. Ce principe n'est pas nouveau puisqu'il avait été envisagé par le G29. Dans son avis n° 3/2010 portant sur le principe de responsabilité en date du 13 juillet 2010[441], il avait mis en exergue la nécessité d'une telle obligation pour les responsables du traitement dans la mesure où cette dernière favoriserait la protection effective des données[442]. Or, le plus souvent, c'est bien l'effectivité des droits et libertés qui font défaut dans le cadre des traitements algorithmiques. Par rapport à la directive 95/46/CE, le RGPD modifie l'approche de la protection sur les données personnelles. Il fait basculer un régime de formalités préalables à un régime de responsabilisation des acteurs à des fins de simplification. Il était important de prendre en considération les risques inédits inhérents à l'ampleur de la nouvelle économie de la donnée dans un cadre réglementaire modifié. Ce principe participe également à ce que les autorités chargées de la protection des données, comme la CNIL, exercent une meilleure surveillance des responsables du traitement[443]. Mais est-ce vraiment le cas ?

211. L'article 24 paragraphe 1 du RGPD a repris cette obligation en précisant que *« le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* ». Mais le texte précise que le degré de redevabilité est variable « *compte tenu 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* ».

212. Cette obligation n'est donc pas absolue puisque laissée en grande partie à l'appréciation des acteurs eux-mêmes, ce qui n'est pas la solution la plus protectrice pour les personnes

[440] Art. 5 § 2 du RGPD.
[441] G29, avis n° 3/2010 sur le principe de responsabilité, WP 173, adopté le 13 juillet 2010.
[442] *Ibid*., p. 2.
[443] *Ibid*., § 74, p. 21.

physiques faisant l'objet d'un traitement de leurs données personnelles[444]. L'approche du RGPD peut sembler novatrice en la matière, mais il ne peut être exclu que dans la pratique nous assistions à une dénaturation de l'esprit du texte, qui selon nous, repose trop à certains égards sur la bonne volonté des acteurs tels que les responsables du traitement.

213. Ce même esprit se retrouve à l'article 24 paragraphe 2 du RGPD puisque si les activités de traitement ont des incidences sur les personnes physiques[445], des « *politiques appropriées en matière de protection des données par le responsable du traitement* » devront être mises en œuvre. Toutefois, une fois de plus, tel est uniquement le cas si cela est proportionné à l'activité de traitement, sans pour autant définir quels sont les cas de figure concernés par cette obligation.

214. Il s'agit donc surtout d'une relation entre d'une part l'autorité de contrôle et les acteurs, le plus souvent privés, qui participent à l'élaboration du droit, sans que la société civile n'y soit conviée. C'est essentiellement une relation entre les autorités gouvernementales et les entreprises. Les tiers ne peuvent pas constater les violations effectuées en interne par les entreprises.

215. Il est question d'aborder les principaux mécanismes du RGPD concourant à la transparence des traitements. Nous retrouvons parmi eux aussi bien des mécanismes de conformité de droit contraignant (Paragraphe 1) que de droit non contraignant (Paragraphe 2).

PARAGRAPHE 1 - Les mécanismes de droit contraignant concourant à la transparence des traitements au titre du principe de responsabilité

216. Les nouveaux mécanismes de conformité contraignants sont nombreux. Il s'agit de la protection des données dès la conception (A), de l'analyse d'impact relative à la protection des données (AIPD) et de la consultation préalable (B), de la tenue d'un registre des opérations (C) et de la désignation d'un DPD (D).

A - Protection des données dès la conception

217. L'article 25 du RGPD instaure une obligation de protection des données dès la conception d'un programme et par défaut. L'objectif est que les responsables du traitement

[444] DEBET A., « Les nouveaux instruments de conformité », *Dalloz IP/IT*, 2016, p. 592.
[445] Conformément à l'article 24 § 2 du RGPD.

imaginent dès sa création la conformité à leurs obligations, ce qui inclut donc le respect aux exigences de transparence par l'intermédiaire *« (…) tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées »*[446]. Les « *mesures techniques et organisationnelles appropriées* » en question ne sont cependant pas définies par le texte, sans doute pour ne pas prendre parti pour des techniques particulières qui tomberaient en désuétude et dénatureraient la disposition. Sa mise en œuvre est fonction de l'état de l'art. Le considérant 78 du RGPD précise également que la protection dès la conception vise *« à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel* ».

218. Le G29, dans sa documentation relative à la transparence, confirme également le rôle de la protection dès la conception à des fins de transparence. Il précise que « *les mécanismes de transparence devraient être intégrés à des systèmes de traitement dès le départ afin que toutes les sources des données à caractère personnel reçues par une entreprise puissent être suivies et retracées jusqu'à leur source à tout moment pendant le cycle de vie du traitement des données* »[447]. La faculté de pouvoir retracer le processus du traitement pendant la durée de son cycle de vie est toutefois compromise dans la mesure où certaines techniques d'IA empêchent par nature une telle implantation dans le système, ce qui leur vaut le qualificatif de boîte noire, y compris pour les concepteurs. Ce mécanisme se retrouve par ailleurs dans la directive « Police-Justice »[448].

219. Cette approche est pourtant très intéressante car elle modifie la logique répressive d'un traitement qui ne serait pas conforme au RGPD par un volet préventif à des fins d'adéquation aux exigences de transparence. Même si l'objectif est naturellement de pouvoir le cas échéant mieux renseigner la personne physique concernée par un traitement au titre du droit à l'information ou à l'explicabilité des décisions individuelles exclusivement automatisées, la mise en œuvre effective de cette mesure est complexe[449]. Au même titre que la protection des données dès la conception se décline en « *privacy by défaut* »[450], nous regrettons qu'il ne se

[446] Art. 25 § 1 du RGPD.
[447] G29, Lignes directrices sur la transparence au sens du RGPD du 11 avril 2018, p. 35.
[448] Art. 20 § 1, Directive (UE) 2016/680 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.
[449] DARY M., BENAISSA L., « Privacy by Design : Un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz* IP/IT, 2016, p. 476 à 480.
[450] Art. 25 § 2 du RGPD et art 20 § 2 de Art. 20 § 1 la Directive (UE) 2016/680 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.

décline pas, comme nous le proposerons dans la seconde partie de ces travaux en « *transparency by design* » afin que ces traitements, et le cas échéant d'autres systèmes, soient conçus de manière impérative en tenant compte techniquement des méthodes les plus appropriées pour les expliquer, et auxquels cas, dans certains domaines, une telle impossibilité aboutirait à l'exclusion de certains méthodes d'IA qualifiée d'opaque[451]. En effet, au-delà des responsables du traitement, des obligations nouvelles de transparence doivent porter sur les fournisseurs de ces produits indépendamment de la bonne volonté des acteurs d'y recourir par la contractualisation[452].

220. Le CEPD a récemment eu l'occasion de préciser dans ses lignes directrices les éléments devant être contenus par la protection des données dès la conception et par défaut. De manière non exhaustive, sont visés la

> *« - Clarté - Les informations doivent être formulées en des termes clairs et simples, concis et compréhensibles.*
>
> *- Sémantique - La communication doit avoir une signification claire pour le public concerné.*
>
> *- Accessibilité - Les informations doivent être aisément accessibles pour la personne concernée.*
>
> *- Contextualité - Les informations doivent être fournies au moment opportun et sous la forme appropriée.*
>
> *- Pertinence - Les informations doivent être pertinentes et applicables à la personne concernée spécifique.*
>
> *- Conception universelle – Les informations doivent être accessibles à toutes les personnes concernées et inclure l'utilisation de langages lisibles par machine pour faciliter et automatiser la lisibilité et la clarté.*
>
> *- Compréhensibilité - Les personnes concernées doivent avoir une juste compréhension de ce qu'elles peuvent attendre en ce qui concerne le traitement de leurs données à caractère personnel, en particulier lorsqu'il s'agit d'enfants ou d'autres groupes vulnérables.*

[451] *Infra*., n° 893 et 961 et s.
[452] DOUVILLE T., *Droit des données à caractère personnel : droit de l'Union européenne, droit Français*, *op. cit.*, p. 207.

- Canaux multiples - Les informations devraient être fournies par différents canaux et médias, au-delà du texte, afin d'accroître la probabilité que les informations parviennent effectivement à la personne concernée.

- Structuration par couches – Les informations devraient être structurées par couches de manière à résoudre la tension entre l'exhaustivité et la compréhension, tout en tenant compte des attentes raisonnables des personnes concernées »[453].

221. La CNIL publie par ailleurs sur un site internet dédié des exemples de bonnes pratiques en matière d'informations des personnes physiques concernées par un traitement de données personnelles[454].

B - L'analyse d'impact relative à la protection des données et la consultation préalable

1 – L'analyse d'impact relative à la protection des données

222. AIPD est obligatoire dans de nombreux cas. Elle est censée aboutir à une conception respectueuse de l'outil, conformément aux obligations du responsable du traitement, tout en assurant la démonstration de la conformité de ce dernier. Elle doit donc avoir lieu avant que le traitement ne soit mis en œuvre[455].

223. Elle est obligatoire lorsqu'un traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* »[456]. Elle est également requise pour trois types de traitement visés par le RGPD, à savoir

« *a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le*

[453] CEPD, Lignes directrices 4/2019 relatives à l'article 25, protections des données dès la conception et protections des données par défaut, version 2.0, adoptées le 20 octobre 2020, p. 17 et 18.
[454] *Site Données & Design par LINC* [en ligne] [Consulté le 23 février 2021]. Disponible à l'adresse : https://design.cnil.fr/
[455] Art. 35 § 1 du RGPD.
[456] Art. 35 § 1 du RGPD. Bien que le protocole 108+ laisse aux parties l'appréciation des mesures appropriées dans le but de la conformité aux obligations de la convention (art. 10 § 4), l'article 10 § 2 du protocole précise tout de même que « *chaque Partie prévoit que les responsables du traitement, ainsi que, le cas échéant, les sous-traitants, doivent procéder, préalablement au commencement de tout traitement, à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées, et qu'ils doivent concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés fondamentales* ».

profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire; b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou c) la surveillance systématique à grande échelle d'une zone accessible au public. »[457]

224. L'analyse d'impact est réalisée par le responsable du traitement aussi bien sur les algorithmes que sur les données utilisées, ce qui n'est pas sans poser la question de la véracité entre ce qui est déclaré par le responsable du traitement et ce qu'il est ou adviendra réellement du traitement, décorrélant le traitement de la fiction juridique découlant de cette disposition. De plus, le caractère facultatif de certaines AIDP, laissée à l'appréciation du responsable du traitement, ne peut que dénaturer l'intention première, à savoir la philosophie du texte dans la mesure où ce mécanisme est censé offrir une traçabilité du traitement. Cela illustre la façon dont le déploiement de certaines techniques juridiques ne sert pas nécessairement le but initialement poursuivi, puisque au contraire, il rend inopérant l'esprit de la disposition. Il est à noter que la frontière entre une APID obligatoire et facultative est floue, notamment car il existe des exceptions[458], raison pour laquelle le responsable du traitement doit être attentif aux lignes directrices du G29, de la CNIL et autres recommandations, avis, ou encore règlements types susceptibles de l'imposer. Des opérations de traitement sont notamment soumises à l'obligation d'analyse d'impact. A cette fin, des listes sont publiées par les autorités de contrôle[459].

225. Pourtant, l'AIPD est en mesure de renseigner sur de nombreuses caractéristiques du traitement et est censée protéger à la fois le responsable du traitement d'éventuelles violations à la réglementation, mais aussi les personnes physiques concernées par ce traitement. Ainsi, elle doit au minimum contenir

[457] Art. 35 § 3 du RGPD.
[458] Voir en ce sens à titre d'exemple l'article 35 § 10 du RGPD, « *Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.* ».
[459] Art. 35 § 4 et 5 du RGPD.

« a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement; b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités; c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées »[460].

226. Nous regrettons par ailleurs que le recours aux audits ne soit pas davantage utilisé par le RGPD pour suivre l'évolution du traitement alors que la conformité du traitement dans le temps avec l'analyse d'impact ne devrait pas être laissée à l'appréciation du responsable du traitement[461]. Naturellement, il convient de reconnaître que ces opérations ont un coût, mais il est essentiel à l'effectivité des droits et libertés.

227. Comme a pu le préciser le G29 dans ses lignes directrices relatives à l'AIPD, bien que le RGPD n'impose pas de publier ces analyses, il « *serait utile pour susciter la confiance dans les opérations de traitement du responsable du traitement et pour donner des gages de responsabilité et de transparence* »[462], surtout lorsque « *des citoyens sont affectés par l'opération de traitement* »[463]. Nous ne comprenons pas que la publication de ces AIPD ne soit pas obligatoire, même si cela impliquerait que certaines mentions soient occultées pour des raisons de conciliation entre la transparence directe et la sécurité ainsi que le secret des affaires par exemple. Mais une telle publication participerait nécessairement à ce que la société civile puisse concourir à la conformité quand bien même serait-elle mineure compte tenu du faible nombre d'informations publiées.

228. L'autorité de contrôle dispose toutefois de tous les éléments si elle en fait la demande, ou bien si la communication est obligatoire. On retrouve donc ici une transparence effectuée par l'intermédiaire d'un tiers de confiance. La confiance dans cette autorité doit alors être

[460] Art. 35 § 7 du RGPD.
[461] Art. 35 § 11 du RGPD.
[462] G29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, p. 21.
[463] *Ibid.*

certaine, ce qui nécessite de la part du citoyen un important contrôle au sujet de son action, et une augmentation de ses moyens afin que cette conformité soit correctement réalisée.

2 - Consultation préalable

229. Comme nous l'avons évoqué, sauf dans de rares situations, la nouvelle règlementation a mis fin au régime d'autorisation préalable[464]. Le RGPD prévoit dans certains cas que le responsable du traitement consulte l'autorité de contrôle[465] afin qu'il lui transmette des informations sur le traitement[466], en vue de le conseiller et de formuler un avis, ce qui concourt à la transparence vis-à-vis du régulateur et est susceptible de l'alerter sur de nombreuses irrégularités, et le cas échéant de cibler des contrôles pour qu'elle s'assure qu'elles ont été comblées lorsque le traitement est mis en œuvre. La CNIL joue parallèlement, dans le cadre de cette procédure, un rôle de conseil auprès du responsable du traitement. Il s'agit, au même titre que l'AIPD d'une intervention en amont, c'est-à-dire avant que n'entre en fonctionnement le traitement.

230. Elle s'applique dans l'hypothèse où l'AIPD conclut à ce « *que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque* »[467]. Le G29 précise que « *lorsque le responsable du traitement ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable (à savoir que les risques résiduels demeurent élevés), une consultation de l'autorité de contrôle est obligatoire* »[468].

231. La CNIL est donc amenée à se prononcer par un avis sur ces éléments si elle estime que le responsable du traitement n'a pas apporté les corrections nécessaires en vue d'atténuer ou d'identifier le risque. La mise en œuvre du traitement restera suspendue jusqu'à ce que l'autorité

---

[464] *Supra*., n° 208 et s.
[465] Art. 36 du RGPD.
[466] « *a) le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises;*
b) les finalités et les moyens du traitement envisagé ;
c) les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu du présent règlement ;
d) le cas échéant, les coordonnées du délégué à la protection des données ;
e) l'analyse d'impact relative à la protection des données prévue à l'article 35 ; et
f) toute autre information que l'autorité de contrôle demande », art. 36 § 3 du RGPD.
[467] Art. 36 § 1 du RGPD.
[468] G29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, p. 22.

de contrôle bénéficie des éléments suffisants, même s'il ne s'agit pas pour autant d'un régime d'autorisation.

C – Le registre des opérations

232. Bien que le G29 ne mentionne pas comme tel le registre des activités de traitement comme une mesure de transparence, il nous apparaît qu'il peut concourir à la compréhension des traitements. C'est un véritable outil de conformité au RGPD. Les organisations de moins de 250 salariés ne sont cependant pas tenues d'avoir un tel registre sauf à manipuler des données sensibles ou si le « *si le traitement effectué est susceptible de comporter un risque pour les droits et des libertés des personnes concernées* »[469].

233. Lorsque la tenue d'un registre est obligatoire pour le responsable du traitement ou son représentant, il contient de nombreuses informations sur le traitement des données tels que la finalité, les transferts de données vers un Etat tiers, les délais prévus pour l'effacement, les noms et coordonnées des responsables du traitement notamment[470]. A cet égard, le registre permet de vérifier la conformité ainsi que la traçabilité du processus.

234. De plus, nous ne pouvons que regretter comme le souligne Christina Koumpli, que ces registres ne soient pas rendus publics aux utilisateurs qui en feraient la demande, ne serait-ce à des fins de contribution d'une plus grande transparence[471]. Il convient toutefois de préciser que conformément aux dispositions du CRPA[472], si une entreprise privée se voit confier un traitement de données à caractère privé à des fins d'une mission de service public, ou d'une administration, il est possible pour l'usager de ce service d'en obtenir la communication, car il s'agit d'un document administratif communicable, sous réserve des secrets protégés par la loi.

235. Dans l'hypothèse où le responsable du traitement omettrait de prévenir la personne physique qu'un traitement s'opère, par la voie d'une mention explicite, l'accès au registre permettrait de découvrir l'existence d'un traitement, et donc de faire valoir ensuite son droit d'accès à ses données personnelles par exemple. Au titre de ses obligations de responsable du

---

[469] Art. 30 § 5 du RGPD.
[470] Art. 30 du RGPD.
[471] Christina Koumpli note à cet égard qu'« *on peut légitimement se demander pourquoi le registre n'est pas directement accessible au public afin de satisfaire plus facilement le droit à la transparence des personnes concernées ? Finalement, il semble paradoxal que les nouvelles technologies aujourd'hui très développées pour le traitement des données ne soient pas aussi utilisées au bénéfice des personnes concernées afin de garantir l'effectivité de leurs droits prévus par la RGPD* », KOUMPLI C., *Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données à caractère personnel : étude comparée : Union européenne, Allemagne, France, Grèce, Royaume-Uni*, *op. cit*., spec. p. 470.
[472] *Infra*., n° 410 et s.

traitement, la CNIL[473] a notamment eu à publier son registre, mais elle y a fait figurer dans ce document les obligations complémentaires telles que les informations visées par les articles 13, 14 et 15 du RGPD[474], ce qui offre plus de clarté et de transparence[475]. Or, nous ne pouvons que regretter de ce caractère facultatif, dans la mesure où le plus souvent ce sont les plus irréprochables qui offrent le plus haut degré de transparence, d'où la nécessité d'imposer un seuil maximal de transparence pour tous les acteurs. La difficulté est au contraire d'obtenir une information véritable de la part de ceux les plus susceptibles de ne pas respecter leurs obligations.

236. L'article L. 121-4-2 du Code de l'éducation concourt également à une certaine transparence des traitements algorithmiques. En effet, lors des discussions de la LIL de 2018[476], a été introduit dans le Code de l'éducation une nouvelle disposition. Ainsi, « *l'autorité responsable des traitements de données à caractère personnel mis en œuvre dans les établissements publics d'enseignement scolaire met à la disposition du public le registre comportant la liste de ces traitements […]* ». La mise à disposition du public d'un registre indiquant la liste des traitements déployés par l'Education nationale permet tout un chacun de consulter ces informations, et donc y compris aux parents d'élèves, ce qui permet d'enquêter sur la base de cette prise de connaissance. Il est effectivement impossible, comme nous l'avons déjà évoqué, d'obtenir la transparence de ces traitements lorsqu'on ignore leur existence. Toutefois, force est de constater que le degré et la nature de ce principe de transparence qui ne dit pas son nom, bien que certains membres de la doctrine l'aient nommé comme tel[477], est imprécis et ne permet pas de connaître l'exactitude du fonctionnement des traitements mis en œuvre dans la mesure où, comme nous l'avons vu, le RGPD n'offre pas toujours une très grande transparence à ce sujet. En effet, la transparence telle que prévue par cette règlementation empêche de rejouer les opérations du traitement, à moins qu'il ne s'agisse d'une décision administrative individuelle, auquel cas, c'est le régime juridique de la transparence se trouvant dans le CRPA qui s'y appliquera[478].

---

[473] Et comme le considérant 52 incite les institutions de l'UE à le faire pour plus de transparence.
[474] *Supra.*, n° 86 et s.
[475] CNIL, La CNIL publie son registre RGPD, *CNIL.fr* [en ligne], 02 décembre 2019, mis à jour le 13 mai 2020. [Consulté le 10 août 2020]. Disponible à l'adresse : https://www.cnil.fr/fr/la-cnil-publie-son-registre-rgpd ; MAXIMIN N., « Données personnelles : pourquoi la CNIL publie-t-elle son registre RGPD ? », *Dalloz actualité*, 6 décembre 2019.
[476] Art. 22 de la LIL modifiée.
[477] BROGLI M., CATELAN N., CASTETS-RENARD C., DE LA CLERGERIE M., DUBOIS L., FAVRO K., JAULT-SESEKE F., GAULLIER F., GRYNWAJC S., LE BRET A., MARTIAL-BRAZ N., MATSUBARA M., MAXWELL W., PAULIN B., ROCHFELD J, STALLA-BOURDILLON S., TOULOTTE T., ZANOTTI F., ZOLYNSKI, C., *Droit des données personnelles, Les spécificités du droit français au regard du RGPD, Dalloz décryptage*, 2019, spec. p. 116.
[478] *Infra*., n° 435 et s.

D - Le délégué à la protection des données à caractère personnel

237. Il est l'héritier du correspondant à la protection des données à caractère personnel institué par la loi n° 2004-801 du 6 août 2004. Sa désignation n'était que facultative mais ouvrait en contrepartie la possibilité à des simplifications, voire à des dispenses, dans le régime d'autorisation précédant l'entrée en application du RGPD.

238. Très brièvement, car nous serons amenés à évoquer la réforme de cette institution dans le cadre de cette seconde partie afin d'étendre ses missions au-delà des données personnelles[479], le DPD concourt à l'effectivité des nombreuses dispositions relatives à la transparence prévues par la réglementation. Lorsqu'il n'est pas entravé dans ses missions il est un atout majeur de la conformité. Il s'agit donc d'un mécanisme de corégulation pragmatique partant du postulat que le régulateur ne peut pas contrôler en permanence tous les acteurs, et qu'il conviendrait mieux d'associer ces professionnels à leur mise en conformité, et ce par l'intermédiaire de cette institution, n'empêchant pas par ailleurs des contrôles opérés par la CNIL[480].

239. Désormais, selon ce texte, sa désignation est obligatoire dans quatre situations, aussi bien pour le responsable du traitement que le sous-traitant, à savoir lorsque

> « *a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;*
>
> *b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou*
>
> *c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à*

[479] *Infra*., n° 883 et s.

[480] TURK A., Rapport public n°218 sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés du Sénat, session ordinaire de 2002-2003, fait au nom des lois constitutionnelles, de législation, du suffrage universel, Règlement et d'administration générale, enregistré à la Présidence du Sénat le 19 mars 2003, « *Leur mise en place doit permettre à la CNIL de disposer d'un réseau de correspondants, ainsi que cela existe déjà dans le secteur public. En effet, une seule autorité de contrôle ne peut pas tout assurer* », p. 95.

l'article 9[481] *ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10* »[482].

240. Enfin, l'Union européenne ou les Etats membres ont par ailleurs la possibilité de le rendre obligatoire pour les responsables du traitement ou leurs sous-traitants ou « *les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants* »[483].

241. Il est une interface aussi bien vis-à-vis de l'autorité de contrôle[484] que des personnes physiques concernées par un traitement, et a également pour mission de conseiller le responsable du traitement ou le sous-traitant qui l'emploie dans sa mise en conformité[485]. Il est un interlocuteur privilégié et l'un des garants de l'exercice des droits, y compris du droit à l'information de la personne physique concernée par un traitement[486] : à cet égard, *« les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement* »[487]. Par ailleurs, le DPD exerce un rôle significatif dans l'élaboration et le suivi du registre des opérations, de l'AIPD et de la consultation préalable[488].

242. Il est un outil important de conformité lorsqu'il est compétent, raison pour laquelle la CNIL peut procéder à la certification des compétences du DPD selon deux référentiels qu'elle a établi. Le premier permet à la CNIL d'évaluer le délégué lui-même[489], tandis que l'autre certifie par l'obtention d'un agrément les organismes habilités à certifier les DPD[490]. Toutefois, cette certification n'est pas obligatoire pour exercer cette fonction et il n'est pas pleinement indépendant, notamment car il ne bénéficie pas du statut de salarié protégé[491].

---

[481] Il s'agit des données sensibles prévues à l'article 9 du RGPD. *Supra*., n° 110.
[482] Art. 37 § 1 du RGPD. Il convient d'ajouter que l'article 103 de la LIL modifiée prévoit que les traitements de données personnelles en matière de police et de justice, à l'exception de ceux utilisés par les juridictions dans ce domaine, imposent la désignation d'un DPD. Le cas échéant la désignation d'un seul DPD pour plusieurs services est autorisée.
[483] Art. 37 § 4 du RGPD.
[484] Art. 39 § 1 d) du RGPD.
[485] Art. 39 du RGPD.
[486] Art 13 § 1 b) et 14 § 1 b) du RGPD.
[487] Art. 38 § 4 du RGPD.
[488] *Supra*., n° 216 et s.
[489] CNIL, Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPD).
[490] CNIL, Délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPD).
[491] SENAT, Statut des délégués à la protection des données, Réponse ministérielle publiée dans le JO du Sénat le 7 février 2019, p. 712, www.s*enat.fr*, [en ligne]. [Consulté le 02 mars 2021]. Disponible à l'adresse :

PARAGRAPHE 2 - Les mécanismes de droit non contraignant

243. Afin de compléter et démontrer cette mise en conformité, le législateur européen propose également le recours au code de conduite[492] ou à la certification[493], ce que rappelle par ailleurs le G29 dans ses lignes directrices sur la transparence[494]. Bien que ces éléments soient à géométrie variable, un mécanisme de droit souple peut toutefois devenir du droit dur si un engagement a été pris par l'acteur concerné. Les codes de conduite (A) et la certification et labels (B) sont cités par le RGPD à des fins de conformité et sont encouragés par les Etats membres afin d'assurer la conformité des traitements notamment aux règles de transparence.

A - Les codes de conduite

244. A la lumière du préambule du RGPD[495], qui a une valeur interprétative du texte, le code de conduite apparaît comme un outil permettant « *la mise en œuvre de mesures appropriées et à la démonstration par le responsable du traitement ou leur sous-traitant du respect du présent règlement* ». Il convient donc logiquement d'en déduire que les codes de conduite participent à la démonstration de la conformité du principe de transparence garanti par le RGPD[496]. En ce sens, le CEPD précise que cet outil est susceptible d'instaurer la confiance en améliorant la transparence du traitement à l'encontre des individus[497].

245. Selon l'article 40 § 1 du RGPD, les codes de conduite peuvent notamment être élaborés afin de préciser les modalités en matière de loyauté et de transparence du traitement[498], la collecte des données à caractère personnel[499], les informations communiquées au public et aux personnes concernées[500] et l'exercice de leurs droits[501]. Ils ne peuvent être pris qu'à l'initiative

https://www.senat.fr/questions/base/2018/qSEQ180102896.html#:~:text=Minist%C3%A8re%20du%20travail-,publi%C3%A9e%20dans%20le%20JO%20S%C3%A9nat,%2F02%2F2019%20%2D%20page%20712&text=Le%20r%C3%A8glement%20est%20un%20acte,de%20son%20entr%C3%A9e%20en%20vigueur

[492] Art. 40 et 41 du RGPD.

[493] Art. 42 du RGPD.

[494] G29, Lignes directrices sur la transparence au sens du RGPD du 11 avril 2018.

[495] Considérant 100 du RGPD.

[496] Conformément au contenu du principe abordé lors du premier chapitre de cette thèse, *Supra.*, n° 86 et s.

[497] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, version 2.0 uniquement en anglais, adopté le 4 juin 2019, « *Codes can be an effective tool to earn the trust and confidence of data subjects. They can address a variety of issues, many of which may arise from concerns of the general public or even perceived concerns from within the sector itself, and as such constitute a tool for enhancing transparency towards individuals regarding the processing of their personal data* », p. 10. Nous traduisons « Les codes peuvent être un outil efficace pour gagner la confiance des personnes concernées. Ils peuvent aborder une variété de questions, dont beaucoup peuvent découler de préoccupations du grand public ou même de préoccupations perçues au sein du secteur lui-même, et constituent donc un outil permettant d'améliorer la transparence envers les individus en ce qui concerne le traitement de leurs données personnelles ».

[498] Art. 40 § 2 (a) du RGPD.

[499] Art. 40 § 2 (c) du RGPD.

[500] Art. 40 § 2 (e) du RGPD.

[501] Art. 40 § 2 (f) du RGPD.

d'association ou d'organismes du secteur professionnel en question, et sont fortement encouragés[502]. Il est à noter que les projets de code de conduite, incités par les Etats membres et les autorités de contrôle[503], devront être validés par ces derniers afin de s'assurer qu'ils offrent une conformité au RGPD[504]. Bien que l'élaboration d'un code de conduite soit facultative, même si certains Etats membres les ont rendus obligatoires dans certains domaines[505], il n'en demeure pas moins qu'une fois élaboré et validé par l'autorité compétente, il engage ceux qui l'ont adopté à le respecter. Le code de conduite est également fortement recommandé par le Règlement aux responsables du traitement qui ne seraient pas soumis au RGPD[506]. Ce n'est qu'après sa validation, afin de s'assurer de sa conformité à la réglementation[507], que l'autorité de contrôle mentionne son existence dans un registre afin notamment de le mettre à la disposition du public[508], à moins que cette communication ne remette en cause, par exemple, le secret des affaires. A cet égard, la conformité à ces obligations est uniquement réalisée par l'autorité de contrôle de l'Etat membre concerné, ou à défaut par l'autorité de contrôle de l'Union européenne[509]. Il est également possible que ce respect soit assuré par un organisme agrée[510]. Par ailleurs, s'il s'agit d'un code de bonne conduite applicable à l'échelle de l'Union, après avis du CEPD[511], la Commission est susceptible de le rendre d'application générale pour tous les Etats membres[512]. Ce dernier est ensuite enregistré et publié par l'autorité de contrôle[513]. La CNIL a en ce sens été amenée à approuver le premier code de conduite européen initié par l'association européenne de fournisseurs de services d'infrastructure Cloud[514]. Ce code de conduite détaille par ailleurs des exigences de transparence sectorielles, notamment en matière de sécurité[515]. Il s'agit d'un complément à l'effectivité du RGPD, puisque l'adoption d'un tel code, même au niveau européen, ne dispense pas d'éventuels contrôles des autorités nationales de l'Union.

[502] Art. 40 § 2 et cons. 98 du RGPD.
[503] Art. 40 § 1 et cons. 98 du RGPD.
[504] Art. 40 § 5 du RGPD.
[505] Tel est le cas par exemple le cas de la DPA Anglaise pour les traitements journalistiques. En ce sens, voir, TAMBOU O., *Manuel de droit européen de la protection des données à caractère personnel*, *Bruylant*, 2020, p. 299.
[506] Art. 40 § 3 du RGPD.
[507] Art. 40 § 5 du RGPD.
[508] Art. 40 § 11 du RGPD.
[509] Art. 40 § 4 du RGPD.
[510] Organisme agréé par l'art. 41 § 1 en vertu de l'art. 40 § 4 du RGPD.
[511] Art. 40 § 8 du RGPD
[512] Art. 40 § 9 du RGPD
[513] Art. 40 § 11 du RPGD.
[514] CNIL, Délibération n° 2021-065 du 3 juin 2021 portant approbation du code de conduite européen porté par Cloud Infrastructure Service Providers Europe (CISPE).
[515] CISPE, *Code de conduite des Fournisseurs d'infrastructures Cloud relatif à la Protection des données*, du 9 février 2021.

246. Il est intéressant de noter que le code de conduite comporte un volet collaboratif faisant aussi bien participer les autorités de contrôle que les responsables du traitement ou leur regroupement à l'élaboration de leur propre conformité. Cela rejoint parfaitement le qualificatif de gouvernance collaborative, désigné par Margot E. Kaminski. Qu'ils soient de nature privée ou publique, ces acteurs s'associent et participent à l'édiction de la norme juridique de droit souple. En recevant ces propositions, l'autorité de contrôle enrichit le projet de code de conduite afin qu'il soit amélioré puis validé. Mais comme certains auteurs l'indiquent[516], nous pouvons regretter que les personnes physiques faisant l'objet de ces traitements ne soient pas associées à l'élaboration de ces normes alors qu'elles sont susceptibles d'être concernées en premier lieu par leur application[517].

B - La certification

247. Conformément au considérant 100 du RGPD et à l'article 42 paragraphe 1 de ce dernier, la certification et les labels ont vocation à ce que les responsables de traitement ou bien leurs sous-traitants, procèdent à des opérations de traitement conformes à la réglementation. En s'assurant de la conformité d'un système à un référentiel préalablement établi par un organisme tiers ou par une autorité de contrôle, elle participe d'une manière générale au respect du RGPD tout en y favorisant une plus grande transparence[518].

248. Cela étant, le texte dispose que les exigences de certification diffèrent en fonction de la taille de l'entreprise, ce qui interroge puisque cela se fait nécessairement au détriment des droits attachés à la personne. Il est important de rappeler que ce n'est pas parce que « les opérations de traitement » ont fait l'objet d'une certification que cela exonère les responsables du traitement et ses éventuels sous-traitants de leurs obligations d'information que nous avons étudiées[519]. La certification est volontaire, et donc non obligatoire. Elle doit toutefois être

[516] KAMINSKI M, E., « Binary Governance : Lessons from the GDPR's Approche to Algorithmic Accountability », *op. cit.,* p. 1609.
[517] En ce sens, le considérant 99 du RGPD se prononce en faveur de cette option, mais il n'a aucune force obligatoire : « *Lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations* ».
[518] RGPD, considérant 100, « *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* ».
[519] *Supra.,* n° 93 et s.

accessible à travers un processus transparent[520]. La disposition précise également que les responsables du traitement qui ne sont pas soumis au RGPD peuvent toutefois recourir à la certification afin de démontrer qu'ils respectent « *des garanties appropriées dans le cadre des transferts de données à caractère personnel vers un pays tiers* ». Concernant les transferts de données prévues à l'article 46 du RGPD, les garanties prévues à l'article 46 paragraphe 1 sont satisfaites dès lors qu' *« un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées* »[521].

249. Il est recommandé par le CEPD dans ses lignes directrices que l'évaluation d'un produit porte notamment sur les opérations de traitement ainsi que sur ses finalités[522]. Néanmoins, la pertinence de la certification est variable puisqu'elle dépend des moyens et de l'intention des sociétés qui décident d'y recourir, ce qui influe de fait sur sa pertinence. La documentation de l'évaluation joue de plus un rôle essentiel car elle permet également une meilleure transparence du mécanisme de certification puisque « *l'évaluation permettra de comparer la documentation de la certification avec la situation réelle sur site et par rapport aux critères de certification.* »[523]. Il est intéressant de souligner que le CEPD porte une attention particulière à l'intelligibilité de la certification auprès des clients de ces produits. En effet, les organismes certificateurs doivent rendre accessible et intelligible un certain nombre d'informations au sujet de la certification des opérations de traitement tels que

> *« (…) la description de la cible d'évaluation ; • la référence aux critères approuvés appliqués à la cible d'évaluation spécifique ; • la méthodologie de l'évaluation des critères (évaluation sur site, documentation, etc.) ; et • la durée de validité du certificat ; et • devraient permettre la comparabilité des résultats par les autorités de contrôle et le public. »*[524]

[520] Art. 42 § 3 du RGPD.
[521] Art. 46 § 2 f) du RGPD.
[522] CEPD, Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement, version 3.0 du 4 juin 2019, § 61, p. 21 [en ligne] [Consulté le 15 juin 2020]. Disponible à l'adresse :
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_fr.pdf
[523] *Ibid.*, § 63 et 64, p. 21.
[524] *Ibid.*, § 66, p. 22.

250. Enfin, concernant le choix des critères de certification, les critères retenus doivent être uniformes et vérifiables à des fins de conformité, notamment *« afin de faciliter l'évaluation des opérations de traitement au titre du RGPD »*[525].

251. En France, ce travail de certification peut être aussi bien opéré par l'autorité de contrôle nationale que par un tiers certificateur bénéficiant d'un agrément délivré par la CNIL[526]. Au-delà de la certification des traitements algorithmiques, il semble curieux que le législateur national ait permis la certification des personnes[527], comme des DPD[528], dans la mesure où cela laisse à penser que les prestations de service de ces personnes seraient nécessairement en conformité avec le RGPD, ce qui pourrait être fallacieux pour les entreprises recourant au service de ces personnes ou le consommateur, quand bien même cette certification peut dans les faits faire l'objet d'un retrait en cas de manquement[529] à la suite d'un contrôle. Une fois délivrée, la durée de la certification ne peut excéder trois ans[530]. Quant à l'agrément dont bénéficie le tiers certificateur, sa durée est de cinq ans maximums renouvelable[531]. Si l'autorité de contrôle a pour mission ce rôle de certificateur, elle se doit d'être particulièrement transparente dans le cadre de cette tâche et veiller à prévenir tout risque de conflit d'intérêt ou de séparation des pouvoirs avec ses compétences en matière d'enquête[532].

252. Pour conclure, la certification reflète à notre sens le fait que le traitement algorithmique est conforme au RGPD à un instant T en fonction des critères préétablis. Or, en informatique, les traitements évoluent en permanence, et nous avons l'impression, qu'au même titre que les labels, la certification est davantage susceptible d'être un argument commercial qu'un véritable gage de conformité à l'inverse d'un audit. Le coût de ces certifications est par ailleurs un frein à leur généralisation.

---

[525] *Ibid*., § 67, p. 23.
[526] Dans les conditions prévues à l'art 43 du RGPD.
[527] Art. 8 h) de la LIL modifiée, au regard de la loi informatique et libertés, la CNIL « *(…) peut décider de certifier des personnes, des produits, des systèmes de données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et à la présente loi* ».
[528] *Supra*., n° 237 et s.
[529] Art. 20 III 4° de la LIL modifiée.
[530] Art. 42 § 7 du RGPD.
[531] Art. 43 § 4 du RGPD.
[532] CEPD, Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement, version 3.0 du 4 juin 2019, *op. cit.*, § 22, p. 11.

CONCLUSION DU CHAPITRE II

253. Comme nous l'avons constaté, le RGPD repose sur une ambivalence. D'une part, il souhaite un haut niveau de protection des droits des individus sur le traitement de leurs données à caractère personnel, et d'autre part, il donne un rôle significatif aux acteurs abordés dans leur mise en conformité afin de faciliter la libre circulation de ces données au sein de l'Union. La synthèse de ces deux objectifs créée un déséquilibre tant les exceptions sont nombreuses et les pouvoirs des autorités de contrôle affaiblis à certains égards puisque l'effectivité du principe ne repose que trop grandement sur la bonne volonté des responsables du traitement.

CONCLUSION DU TITRE I

254. Le droit européen et national ambitionne aussi bien une transparence théorique (les informations à communiquer) qu'effective (les mécanismes de contrôle) des traitements de données à caractère personnel. Ce régime juridique demeure toutefois imparfait. Il s'agit avant tout d'une règlementation visant à fluidifier la circulation des données au sein de l'Union européenne, ce qui se fait souvent au détriment des droits des personnes physiques concernées par les traitements. Le basculement d'un régime d'autorisation vers celui d'une responsabilisation des acteurs repose sur de nombreux mécanismes de droit non contraignant illustrant une certaine naïveté de la part du législateur européen au sujet de responsables du traitement peu scrupuleux.

255. En effet, afin de s'assurer de l'effectivité de cette transparence, les personnes physiques concernées par ces traitements sont dans une situation de vulnérabilité en ce qu'ils ne peuvent vérifier la véracité des informations qui leur sont communiquées au titre de leurs droits. La conformité de ces informations, de plus parfois stéréotypées, ne peut être effectuée que par une autorité publique qui ne bénéficie pas pour l'heure des moyens adéquats. De plus, l'élaboration de nombreux mécanismes de conformité sont laissées à l'appréciation des acteurs, donnant l'impression d'une transparence à géométrie variable.

TITRE II - DE L'ELABORATION D'UN REGIME JURIDIQUE SECTORIEL CONCOURANT A LA TRANSPARENCE DES TRAITEMENTS

256. Avant de débuter l'étude de ces nouveaux régimes juridiques spécifiques à la transparence des traitements algorithmiques, il convient de reconnaître que des dispositions générales pourraient très bien permettre une certaine transparence de ces dispositifs bien qu'ils n'aient pas été juridiquement pensés pour cela initialement. Le juge est susceptible, par son pouvoir d'interprétation, de recourir à d'autres normes plus générales afin d'obtenir la transparence de ces nouveaux outils. Mais ces normes n'offrent pas de garanties suffisantes, car elles sont trop générales et nécessitent un affinement jurisprudentiel conséquent actuellement en construction, ce qui n'est d'ailleurs pas sans risque d'aléas. C'est la raison pour laquelle nous nous intéresserons qu'aux principaux régimes juridiques traitant de la compréhension de ces algorithmes.

257. Le pouvoir politique détient donc un rôle fondamental afin de parvenir à l'intelligibilité et à la clarté des outils numériques dans ce domaine. Son intervention a déjà esquissé un droit particulier des algorithmes, mais il demeure encore perfectible à bien des égards. En fonction de la branche du droit ou du secteur d'intervention de ces nouveaux régimes juridiques, ils s'inscrivent le plus souvent dans des objectifs juridiques déjà existants.

258. Indépendamment du droit des données à caractère personnel qui est un régime juridique général instaurant un droit à l'information et parfois à l'explicabilité des traitements des personnes physiques[533], nous constatons que la puissance publique s'immisce spécifiquement dans l'économie de marché à des fins de régulation (Chapitre I). Les objectifs poursuivis sont connus, à savoir pallier les déséquilibres entre acteurs économiques, et le cas échéant avec le consommateur. Au-delà d'une transparence indirecte des algorithmes effectuées par les autorités de contrôle, la technique juridique la plus utilisée est le droit à l'information, notamment pour assurer un consentement libre et éclairé.

259. Quant au droit public, de nouveaux mécanismes de transparence des traitements algorithmiques s'inscrivent dans la poursuite de la transparence administrative ou de la vie politique (Chapitre II).

[533] *Supra.*, 80 et s.

CHAPITRE I - L'EMERGENCE D'UN DROIT PRIVE SPECIAL DES ALGORITHMES : L'ETUDE DES DISPOSITIONS RELATIVES A LA TRANSPARENCE

260. En attendant qu'une nouvelle règlementation européenne harmonisée[534] sur les plateformes en ligne ne permette une meilleure compréhension des traitements algorithmiques mis en œuvre par les opérateurs économiques, certains d'entre eux ont pu jusque-là agréger un nouveau pouvoir par l'intermédiaire de services utilisés par de nombreuses communautés d'utilisateurs. Il est donc compréhensible que référencer ou encore hiérarchiser des contenus par le truchement de traitements algorithmiques contribue à l'exercice d'un pouvoir sur des personnes physiques ou morales, et plus largement sur la société. Ces algorithmes sont souvent qualifiés de secret et contrôlant l'économie et l'information[535]. Cette nouvelle force ne peut être acceptée sans contreparties, y compris de transparence. C'est donc naturellement pour cela que la puissance publique a jugé opportun de s'immiscer dans ces nouveaux rapports, pourtant issus de la loi du contrat.

261. Les objectifs poursuivis par cette transparence sont connus[536] puisqu'il s'agit de pallier les risques d'iniquité, de déloyauté ou encore de pratiques anticoncurrentielles dans les rapports contractuels entre professionnels, mais aussi avec les consommateurs. Afin d'assurer un consentement libre et éclairé, notion au cœur des rapports économiques, les techniques juridiques de transparence sont classiques à travers un droit à l'information. Son étendue est cependant variable en fonction des situations et des acteurs concernés.

262. Le législateur, qu'il soit européen ou national, s'est saisi dans un premier temps des algorithmes utilisés en matière de pratiques commerciales, notamment à des fins d'ordre public économique (section I). Puis une régulation spécifique a ensuite été apportée, mais de manière plus disparate, afin d'encadrer certains hébergeurs de contenus, ainsi que les outils d'aide à la prise de décision et de délégation privée (section II).

[534] Voir en ce sens, proposition de Règlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, 15 décembre 2020 ; Proposition de règlement n° 2020/0374 du Parlement européen et du Conseil relatif aux marchés numériques (législation sur les marchés numériques) en date du 15 décembre 2020 ; proposition de règlement 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 du 21 avril 2021.

[535] PASQUALE F., *Black Box Society : Les algorithmes secrets qui contrôlent l'économie et l'information*, *op. cit.*

[536] Voir notamment en ce sens, VIGNAL N., *La transparence en droit privé des contrats (approche critique de l'exigence), Presses Universitaires d'Aix-Marseille,* 1998, 352 p.

SECTION I - LA TRANSPARENCE DES ALGORITHMES EN MATIERE DE PRATIQUES COMMERCIALES ET D'ORDRE PUBLIC ECONOMIQUE

263. Le devoir de loyauté, bien qu'initialement civiliste en matière contractuelle[537], a eu les faveurs du législateur en matière de droit à l'information concernant les algorithmes utilisés par les plateformes en ligne. Compte tenu du secret industriel et commercial, il n'est juridiquement pas possible, pour l'utilisateur, de contrôler le contenu de ces traitements automatisés de données en l'état du droit[538]. Pourtant, la hiérarchisation des contenus opérée par les plateformes ne fait d'ailleurs pas nécessairement intervenir des données à caractère personnel, ce qui engendrait une fois de plus un angle mort juridique : la LIL ne s'y appliquant pas.

264. Le législateur, notamment en reprenant les travaux du Conseil d'Etat, a alors introduit par l'intermédiaire de la LRN de 2016[539], un principe de loyauté, de clarté et de transparence des plateformes en ligne en faveur du consommateur (Paragraphe 1). Puis, suivant cette dynamique, le droit de l'Union européenne s'est aussi prononcé en faveur d'une loyauté et d'une transparence au bénéfice des entreprises utilisatrices des plateformes en ligne, mais aussi spécifiquement de certains opérateurs économiques vis-à-vis de l'Etat (Paragraphe 2).

PARAGRAPHE 1 - La transparence des opérateurs économiques par le biais du droit de la consommation

265. Du fait de l'immixtion du numérique dans notre quotidien, ce dernier est de plus en plus saisi par le droit de la consommation. Il interfère au point d'influencer notamment les choix du consommateur. A ce titre, des obligations générales d'information précontractuelle sont apparues afin d'assurer une loyauté, une clarté et une transparence des plateformes en ligne (A), Parallèlement, la lutte contre l'obsolescence logicielle a également vu naître, par l'intermédiaire d'une communication d'informations relatives aux mises à jour logicielle des biens numériques, de nouvelles obligations en la matière (B). Ces règles s'accompagnent également de mesures de contrôle et de sanction spécifiques en cas de non-respect (C).

[537] PETIT F. (dir.), *Droit et loyauté*, Thèmes et commentaire, *Dalloz*, 2015, p. 1. La notion de loyauté renverrait à la notion de bonne foi en matière contractuelle que l'on retrouve à l'article 1134 alinéa 3 du Code civil.
[538] *Infra*, n° 592 et s.
[539] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

A - Les dispositions générales de loyauté, de transparence et de clarté des plateformes en ligne vis-à-vis des consommateurs

1 - Les plateformes concernées

266. Avant la LRN la loi n° 2015-990 du 6 août 2015 avait déjà saisi certains aspects relatifs à la loyauté, la clarté et à la transparence des plateformes en ligne.

En effet,

> « *toute personne dont l'activité consiste à mettre en relation, par voie électronique, plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un bien ou d'un service est tenue de délivrer une information loyale, claire et transparente sur les conditions générales d'utilisation du service d'intermédiation et sur les modalités de référencement, de classement et de déréférencement des offres mises en ligne.* »[540]

267. Toutefois, la notion d'opérateur de plateforme en ligne devait se doter d'une définition et d'obligations juridiques plus précises.

268. Dès l'étude d'impact de la LRN[541] il est frappant de constater que c'est par le truchement du Code de la consommation que des obligations particulières de loyauté, de clarté et de transparence vont s'appliquer à certaines plateformes en ligne concernant leurs algorithmes. En effet, il n'est pas question d'assujettir toutes les plateformes à ces obligations, mais les plus importantes parce que, par leur puissance, elles disposent d'un pouvoir de marché et d'une audience incontournable, ce qui est de nature à biaiser « *le fonctionnement du marché* »[542]. Et c'est précisément pour cela qu'une nouvelle « *obligation générale de loyauté vis-à-vis des consommateurs* »[543] va être imposée par le législateur aux professionnels. Il s'agit spécifiquement d'une information concernant les règles de référencement, de déréférencement et de hiérarchisation des contenus opérés par ces plateformes. Mais la loyauté n'est rien sans la clarté et la transparence. C'est justement parce qu'il existe une transparence que l'on peut s'assurer que cette loyauté est bien mise en œuvre.

---

[540] Ancien art. L. 111-5-1 du Code de la consommation (abrogé).
[541] Projet de loi pour une République numérique, étude d'impact, *Legifrance* [en ligne]. 9 décembre 2015 [Consulté le 12 juin 2020]. Disponible à l'adresse : www.legifrance.gouv.fr/content/download/9558/114488/version/1/file/ei_republique_numerique_cm_09.12.2015.pdf
[542] *Ibid.*, p. 84.
[543] *Ibid.*

269. Les plateformes concernées par des obligations d'information précontractuelles de loyauté, de clarté et de transparence sont prévues à l'article L. 111-7 I du Code de la consommation.

Il dispose qu'

« I.- Est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur :

1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ;

2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service. (…) ».

270. Cette définition de la plateforme en ligne apparaît donc comme très large puisqu'elle englobe l'intermédiation[544].

2 - La nature de l'obligation d'information précontractuelle

a - Les obligations générales d'information précontractuelle

271. Les plateformes en ligne mentionnées à l'article L. 111-7 I du Code de la consommation ont pour obligation de délivrer une information « *loyale, claire et transparente* » aux consommateurs[545]. Cette information porte sur les conditions générales d'utilisation du service ainsi que « *sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder* »[546], ce qui retient particulièrement notre attention dans la mesure où ces modalités sont mises en œuvre par des traitements algorithmiques. Toujours en lien avec les algorithmes effectuant cette hiérarchisation, « *l'existence d'une relation contractuelle, d'un lien capitalistique ou d'une*

[544] ROCHFELD J., ZOLYNSKI C., « La « loyauté » des « plateformes ». Quelles plateformes ? Quelle loyauté ? », *Dalloz IP/IT*, 2016, p. 520 : *« la plateforme se retrouve ainsi définie sur le fondement de critères d'apparence, pour le consommateur, de l'existence d'un service spécifique – une intermédiation -, que ce service porte sur la mise à disposition d'informations fournies par autrui ou sur l'organisation d'échanges de biens et de services proposés par des tiers* ».
[545] Art. L. 111-7 II du Code de la consommation.
[546] Art. L. 111-7 II 1° du Code de la consommation.

rémunération » entre le prestataire et la plateforme doit être mentionnée au consommateur dès lors qu'ils ont une influence sur la manière dont le contenu est référencé[547].

272. De plus, lorsque le consommateur est mis en relation par la plateforme avec un prestataire, qu'il soit professionnel ou non, il doit également pouvoir prendre connaissance de la qualité de l'annonceur ainsi que de ses droits et obligations en matière civile et fiscale[548].

273. Les services de comparaison sont soumis à des disposition particulières concernant les critères de classement des offres de biens et services[549]. L'information doit par ailleurs être « *directement et aisément accessible sur toutes les pages du site et est matérialisée par une mention ou un signe distinctif* »[550]. Toutes ces informations précontractuelles constituent un formalisme impératif nécessaire à la transparence de l'activité de ces plateformes[551].

274. Le Conseil d'État rappelait dans son étude annuelle[552] que les plateformes

> *« sont libres, dans le cadre de leur liberté d'entreprendre, de définir les algorithmes de classement ou de référencement des contenus, produits ou services accessibles par leur intermédiaire, dans le but de fournir le service le plus efficace aux utilisateurs. Toutefois, le principe de loyauté leur interdit d'introduire dans ces algorithmes des considérations étrangères à l'intérêt de l'utilisateur »*[553].

275. Il est intéressant de noter que selon cette étude, il n'est pas admis que le législateur s'immisce dans les choix opérés par les opérateurs en ligne dans les algorithmes qu'ils utilisent au nom de la liberté d'entreprendre. Cela étant, cette analyse est contestable dans la mesure où le législateur pourrait très bien considérer ce qui est tolérable ou non de la part d'une plateforme

---

[547] Art. L. 111-7 II 2° du Code de la consommation.
[548] Art. L. 111-7 II 3° du Code de la consommation.
[549] Art. D. 111-1 du Code de la consommation « *1° Les différents critères de classement des offres de biens et de services ainsi que leur définition ;*
2° L'existence ou non d'une relation contractuelle ou de liens capitalistiques entre le site de comparaison et les professionnels référencés ;
3° L'existence ou non d'une rémunération du site par les professionnels référencés et, le cas échéant, l'impact de celle-ci sur le classement des offres ;
4° Le détail des éléments constitutifs du prix et la possibilité que des frais supplémentaires y soient ajoutés ;
5° Le cas échéant, la variation des garanties commerciales selon les produits comparés ;
6° Le caractère exhaustif ou non des offres de biens ou de services comparées et du nombre de sites ou d'entreprises référencés ;
7° La périodicité et la méthode d'actualisation des offres comparées. »
[550] Art. D. 111-1 al 2 du Code de la consommation.
[551] TGI de Paris, jugement du 17 décembre 2019, RG 17/06223.
[552] CONSEIL D'ETAT, *Le numérique et les droits fondamentaux*, étude annuelle 2014, *La Documentation française*, 2014.
[553] *Ibid*., p. 279.

sans nécessairement l'empêcher d'intervenir dans ce secteur, car il convient de rappeler qu'elle n'est pas une liberté absolue[554].

276. A quoi pourrait donc bien servir la transparence et la clarté lorsqu'elles sont combinées avec la loyauté en matière de recours aux algorithmes ? La loyauté renverrait initialement fort étrangement à l'idée de neutralité du traitement de l'information[555], car on peut supposer que cet objectif de neutralité ne puisse être atteint dès lors que toute tentative de hiérarchisation de biens ou services implique de la part des concepteurs des algorithmes une priorisation de l'information[556]. Or, le Conseil d'Etat dans son étude annuelle avait considéré à juste titre que le principe de neutralité ne pouvait pas être transposable aux plateformes dans la mesure où l'objectif était de « *fournir un accès organisé, hiérarchisé ou personnalisé aux contenus* » contrairement au principe de « neutralité du net » qui impose aux fournisseurs d'accès de véhiculer de manière égale tous les contenus[557]. La clarté ferait quant à elle davantage référence à l'intelligibilité de ces dispositifs auprès du consommateur, à sa compréhension des règles mises en œuvre par la plateforme, tandis que la transparence a pour objet d'assurer que l'obligation de loyauté est conforme à l'explication claire faite au consommateur.

> « *Les plateformes, qui constitueraient, une nouvelle catégorie juridique, seraient quant à elles soumises à une obligation de loyauté, consistant à assurer de bonne foi le service de classement ou de référencement, sans chercher à altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs* »[558].

277. Dans l'esprit de cette loi inspirée du rapport du Conseil d'Etat, la loyauté serait donc l'objectif principal poursuivi par le législateur. Et l'information claire et transparente correspondrait davantage à l'intelligibilité du positionnement algorithmique dans le cyberespace. La transparence, quant à elle, permettrait en théorie la vérification de la conformité de cette bonne foi, c'est-à-dire la façon dont il est possible de s'assurer que les critères déclarés aux consommateurs sont bel et bien ceux opérant le classement sur la plateforme.

---

[554] *Infra*., partie II, sur la conciliation des droits et libertés entre elles afin de parvenir à la transparence de ces algorithmes, n° 653 et s.
[555] ROCHFELD J., ZOLYNSKI C., « La « loyauté » des « plateformes ». Quelles plateformes ? Quelle loyauté ? », *op. cit.*, p. 520.
[556] CARDON D., « Le pouvoir des algorithmes », *op. cit.*
[557] Le Conseil d'Etat a précisé que *« les plateformes ne peuvent être soumises à la même obligation de neutralité que les opérateurs de communications électroniques, car leur rôle est de fournir un accès organisé, hiérarchisé ou personnalisé aux contenus mis à disposition sur leur site ou auxquels elles donnent accès : un traitement égalitaire ne peut être demandé à un moteur de recherche, puisque l'objet même d'un moteur de recherche est de hiérarchiser les sites internets »*, CONSEIL D'ETAT, *Le numérique et les droits fondamentaux*, *op. cit*., p. 21.
[558] *Ibid*., p. 26.

278. Le législateur n'a en revanche pas pris en compte les considérations relatives à l'économie de l'attention, alors que c'est pourtant le propre de ces plateformes, c'est-à-dire la manière dont le comportement du consommateur va être extrait par la plateforme afin d'établir des profils de personnes ou de groupes à qui il convient ensuite de recommander certains biens ou services, tout en leur laissant l'illusion d'un consentement libre et éclairé[559]. Sans doute cela s'explique-t-il car le Conseil d'Etat n'avait pas souhaité que le législateur s'immisce au nom de la liberté d'entreprendre dans l'architecture de ces plateformes[560].

b - Les obligations d'information précontractuelle renforcées (L. 111-7-1 du Code de la consommation)

279. Pour les plateformes dont le nombre de connexions est fixé « *à cinq millions de visiteurs uniques par mois, par plateforme, calculé sur la base de la dernière année civile* »[561], une obligation de transparence et de clarté renforcée a été imposée par le législateur. A ce titre, elles « *élaborent et diffusent aux consommateurs des bonnes pratiques visant à renforcer les obligations de clarté, de transparence et de loyauté mentionnées à l'article L. 111-7* »[562].

280. L'article L. 111-7-1 du Code de la consommation prévoit que l'autorité compétente, en l'occurrence la DGCCRF, peut procéder à des enquêtes pour évaluer et comparer les pratiques des opérateurs. Elle peut à ce titre « *recueillir auprès de ces opérateurs les informations utiles à l'exercice de cette mission* »[563]. Elle diffuse également *« périodiquement les résultats de ces évaluations et de ces comparaisons* ». Reprenant la méthode anglophone du « *name and shame* », elle publie à cette fin la liste des plateformes en ligne qui ne respecteraient pas les obligations précontractuelles de loyauté, de clarté et de transparence prévue à l'article L. 111-7 du Code de la consommation.

281. Qu'il s'agisse des obligations de l'article L. 111-7 et L. 111-7-1 du Code de la consommation, la nature de cette transparence est imprécise. Le législateur a en effet davantage fait confiance au droit souple qu'au droit dur pour régler cette question. Ces opérateurs de plateformes en ligne visés par les obligations de loyauté, de clarté et de transparence doivent

[559] ZUBOFF S., *L'âge du capitalisme de surveillance. Le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, *op. cit*.
[560] *Supra.*, n° 275.
[561] Art. D. 111-15 du Code de la consommation.
[562] Art. L. 111-7-1 du Code de la consommation.
[563] Art. L. 111-7-1 al. 2 du Code de la consommation.

donc en ce sens élaborer et diffuser aux consommateurs les bonnes pratiques[564]. Il est regrettable de considérer que l'effectivité de ces obligations ne soient subordonnées qu'à la bonne volonté des acteurs par le droit souple. Le « *name and shame* » serait à ce titre sans incidence. Cette méthode qui entre dans le cadre des obligations renforcées de transparence de ces plateformes est selon nous un aveu d'impuissance dans la mesure où les plateformes soumises à ce droit souple sont les opérateurs les plus puissants, c'est-à-dire ceux exerçant une emprise telle sur le marché que les consommateurs en sont captifs, le plus souvent faute de concurrence. En effet, le consommateur souhaite également utiliser le service le plus performant, au risque que la transparence soit imparfaite. Il nous semblait donc important que des mécanismes de sanction plus durs soient mis en œuvre. Il y a fort à parier qu'une mauvaise publicité de la plateforme d'un géant du numérique n'affecte aucunement son activité, et donc assez peu sa politique de transparence.

c - Les avis en ligne (D. 111-16 à D. 111-19 du Code de la consommation)

282. Au titre de l'obligation générale d'information précontractuelle, l'article L 111-7-2 du Code de la consommation dispose de plus que

> « (…) *toute personne physique ou morale dont l'activité consiste, à titre principal ou accessoire, à collecter, à modérer ou à diffuser des avis en ligne provenant de consommateurs est tenue de délivrer aux utilisateurs une information loyale, claire et transparente sur les modalités de publication et de traitement des avis mis en ligne* »

283. Concernant la mise en œuvre de ces principes, la plateforme est tenue de préciser si les avis en ligne ont fait l'objet d'un contrôle[565]. Dans l'affirmative, les principales caractéristiques de ce contrôle doivent être communiquées au consommateur. La date de la publication de l'avis ainsi que ses éventuelles modifications sont aussi à préciser[566]. Dans l'hypothèse où l'avis d'un consommateur n'a pas été publié par la plateforme, les raisons justifiant son rejet doivent lui être notifiées[567]. Pour finir, elle met *« en place une fonctionnalité gratuite qui permet aux*

[564] Art. L. 111-7 du Code de la consommation.
[565] *Ibid*., al. 2.
[566] *Ibid*., al. 3.
[567] *Ibid*., al. 4.

responsables des produits ou des services faisant l'objet d'un avis en ligne de lui signaler un doute sur l'authenticité de cet avis, à condition que ce signalement soit motivé »[568].

284. Ces obligations de loyauté, de clarté et de transparence visent à pallier tout risque de pratique commerciale déloyale ou de pratique commerciale trompeuse[569]. Ces dispositions sont intéressantes, car elles marquent le fait que ces avis, qui sont parfois hiérarchisés par les algorithmes, sont saisis par le droit alors même que des utilisateurs mal intentionnés sont susceptibles de jouer avec ces traitements automatisés pour favoriser la promotion d'un service, et ce malgré le consentement de la plateforme en ligne. C'est pour cela que l'utilisateur peut également faire l'objet d'une condamnation. La transparence est donc déployée afin d'assurer une certaine confiance dans l'économie même si trop de transparence vis-à-vis du consommateur pourrait donner des indications sur la façon dont il conviendrait de manipuler ces algorithmes pour en tirer profit par exemple.

d - Les comparateurs de prix et la publicité

285. Les plateformes en ligne évoquées qui recourraient à « *la comparaison des prix et des caractéristiques de biens et de services* », doivent communiquer au consommateur *« les différents critères de classement des offres de biens et de services* », et le cas échéant les liens capitalistiques en cas de référencement moyennant rémunération, par l'intermédiaire d'une rubrique accessible sur la page du site en ligne[570]. Néanmoins, si une plateforme en ligne effectue des comparatifs sans qu'aucun algorithme n'intervienne, c'est-à-dire que la comparaison s'opère uniquement par le truchement d'une intervention purement humaine, et ce malgré la dénomination de comparateur du site internet, il n'est pas soumis à ces obligations de transparence. Il convient donc au consommateur de démontrer la présence d'un algorithme pour exiger la communication de ces informations[571].

286. Il est à noter qu'une proposition de règlement[572] ambitionne par ailleurs d'assurer une plus grande protection du consommateur à travers de nouveaux droits à l'information de ces plateformes en matière de publicité en ligne ou encore de recommandations. Ainsi, l'utilisateur

[568] *Ibid*., al. 5.
[569] FERAL-SCHUHL C., *Cyberdroit, le droit à l'épreuve de l'internet, op. cit*., p. 525.
[570] Art. D. 111-11 du Code de la consommation.
[571] Voir en ce sens, TGI de Paris, jugement du 24 novembre 2020, association consommation, logement et cadre de vie c/ Be Labo.
[572] 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, 15 décembre 2020.

final, qu'il soit professionnel ou non, pourrait « *obtenir des informations utiles concernant les principaux paramètres utilisés pour déterminer le bénéficiaire auquel la publicité est présentée* »[573]. Quant aux très grandes plateformes[574], elles auraient pour obligation de conserver par la voie d'un registre public inventoriant l'historique du ciblage publicitaire jusqu'à un an après l'ultime affichage de cette dernière[575]. Les conditions générales d'utilisation devraient préciser « *de manière claire, accessible et aisément compréhensible, les principaux paramètres utilisés dans leurs systèmes de recommandation* »[576].

B - Les dispositions relatives à l'obsolescence logicielle

287. Sans attendre le droit européen, le législateur national est intervenu à de nombreuses reprises au sujet de l'obsolescence programmée, et en particulier logicielle. Mais il s'agit encore d'un régime juridique en construction. Dès 2015, un délit d'obsolescence programmée a fait son apparition dans le droit de la consommation[577]. Il figure aujourd'hui dans un chapitre unique sur les tromperies à l'article L. 441-2 et suivants du Code de la consommation. L'obsolescence programmée est une pratique « *qui se définit par le recours à des techniques par lesquelles le responsable de la mise sur le marché d'un produit vise à en réduire délibérément la durée de vie pour en augmenter le taux de remplacement* ». Depuis la loi n° 2020-105 du 10 février 2020, nous retrouvons parmi ces techniques le recours au logiciel dans le but de réduire « *délibérément la durée de vie pour en augmenter le taux de remplacement* »[578]. Il convient de reconnaître que l'intention d'utiliser un programme informatique afin de réduire la durée de vie d'un appareil afin qu'il soit remplacé demeure difficile à démontrer tant les algorithmes rendent le processus d'observation complexe, raison pour laquelle est envisagée une inversion de la charge de la preuve[579].

---

[573] *Ibid*., art. 24.
[574] Selon l'article 25 § 1, les très grandes plateformes en ligne sont celles dont le nombre d'utilisateurs actif est égal ou supérieur à 45 millions.
[575] Art. 30 de la proposition.
[576] *Ibid*.
[577] La loi n° 2015-992 du 17 août 2015 a créé un délit d'obsolescence programmée à l'article L. 213-4-1 du Code de la consommation, aujourd'hui abrogé.
[578] Art. L. 441-2 du Code de la consommation. Un arrêté fixera « *la liste des produits et les motifs légitimes, notamment la sécurité ou la santé des utilisateurs, pour lesquels le professionnel n'est pas tenu par cette obligation*. », *Ibid*., al. 2.
[579] Voir en ce sens, THIEBAUT V., Rapport n°4196 sur la proposition de loi visant à réduire l'empreinte environnementale du numérique en France de l'Assemblée nationale, 15 e législature, fait au nom de la Commission du développement durable et de l'aménagement du territoire, enregistré à la Présidence de l'Assemblée nationale 26 mai 2021, p. 37.

288. Des obligations d'informations incombent également au responsable de la mise sur le marché vis-à-vis du consommateur[580]. Cela se justifie par des raisons qui sont notamment d'ordre environnementale. En effet, l'article L. 541-1 du Code de l'environnement précise que c'est par l'information des consommateurs que s'opère la lutte contre l'obsolescence programmée dans un but de « *politique nationale de prévention et de gestion des déchets* »[581]. Elles ne portent pas sur les algorithmes en eux-mêmes mais sur leur fonction. Ainsi, le vendeur doit communiquer à ses clients la durée des mises à jour logicielle assurant un usage normal de l'appareil[582]. Un décret fixera les modalités de cette transparence et les appareils concernés par cette dernière. Il apparaît d'ores et déjà, du fait d'un projet de décret notifié à la Commission européenne[583], un certain nombre d'éléments. Il en ressort des informations précontractuelles telles que le logiciel ou les logiciels de l'appareil faisant l'objet de mises à jour, leur durée et le cas échéant la date de leur fin. Cette communication s'effectue par l'intermédiaire du support qui accompagne la vente de l'objet, et ce de manière lisible et compréhensible. L'objectif est également que le consommateur soit informé de façon suffisamment claire et précise sur ces mises à jour sur les « *modalités d'installation* », afin qu'il ne les installe pas le cas échéant[584]. Ces mises à jour étant régulières en matière de numérique, le producteur transmet au vendeur leurs évolutions afin qu'il puisse actualiser le support de vente. De plus, lorsque l'actualisation des programmes a lieu au-delà d'une durée de deux ans, ce qui est le minimum obligatoire[585], l'information doit porter sur leurs incidences sur les performances du bien. Cette disposition n'est pas sans rappeler la polémique relative à la mise à jour de certains iPhones ayant affecté leurs performances, officiellement pour préserver le plus possible les batteries usées[586]. Enfin, si un bien numérique fait l'objet d'une « *fourniture continue d'un contenu numérique ou d'un service numérique pendant une période supérieure à deux ans* », le vendeur s'assure que le consommateur reçoive les mises à jour prévues, y compris de sécurité.

289. Ce régime juridique est toutefois amené à évoluer. En ce sens, l'article 27 de la loi 2020-105 du 10 février 2020 prévoyait la publication d'un rapport afin que le gouvernement émette

[580] L'article 17 de la loi n° 2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire a ajouté dans le code de la consommation une nouvelle section au chapitre VII intitulée « Information du consommateur et obligations du vendeur concernant les mises à jour de logiciels ».
[581] Art. L. 541-1 I du Code de l'environnement.
[582] Selon l'article L. 217-21 du Code de la consommation est qualifié d'usage normal « *lorsque ses fonctionnalités répondent aux attentes légitimes du consommateur* ».
[583] COMMISSION EUROPEENNE, Projet de décret relatif à l'information du consommateur sur les mises à jour de logiciel, *ec.europa.eu* [en ligne]. 18 décembre 2020. [Consulté le 12 février 2021] Disponible à l'adresse : https://ec.europa.eu/growth/tools-databases/tris/fr/search/?trisaction=search.detail&year=2020&num=830
[584] Art. L. 217-22 du Code de la consommation.
[585] Art. L. 217-23 du Code de la consommation.
[586] *Infra.*, n° 297.

des propositions sur l'obsolescence logicielle notamment en vue de transposer la directive UE 2019/771[587]. Est proposé la possibilité de dissocier les mises à jour de sécurité des mises à jour de fonctionnalité. L'idée étant, qu'au-delà d'une éventuelle communication des caractéristiques des logiciels, le consommateur puisse garder la main sur les fonctionnalités du bien numérique en fonction des informations dont il dispose[588]. Dans le cadre du projet de loi « climat et résilience »[589] a été évoqué la possibilité d'ajouter à l'article L. 217-23 du Code de la consommation que lorsque « *le vendeur ne fournit plus de mises à jour, il diffuse gratuitement sous format électronique, dans un standard ouvert librement réutilisable et exploitable par un système de traitement automatisé, les codes sources afférents au produit concerné* »[590]. Cette initiative[591] ne vise cependant pas la transparence de ces programmes, mais le rallongement de la durée de vie des appareils afin qu'une communauté d'utilisateurs s'approprie leur objet. Néanmoins, nous considérons que cette diffusion aurait renseigné sur le fonctionnement de l'appareil, voire d'une autre gamme de produits utilisant des fragments de ces logiciels, et ce quand bien même le produit serait en fin de vie pour le constructeur. C'est d'ailleurs la raison pour laquelle le rapport gouvernemental avait évincé cette possibilité au regard de sa conciliation avec la propriété intellectuelle[592].

290. Il s'agit donc d'une transparence particulière qui ne repose pas sur les caractéristiques des algorithmes. Les autorités de contrôle ont en revanche pour mission de s'assurer de l'adéquation entre l'information communiquée et leur véracité.

[587] Directive (UE) 2019/771 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens, modifiant le règlement (UE) 2017/2394 et la directive 2009/22/CE et abrogeant la directive 1999/44/CE (Texte présentant de l'intérêt pour l'EEE).

[588] Voir en ce sens, CASTELLAZI M., MOATTI A et al., Rapport CGEDD n°013416-01 et CGE 2020/11/CGE/SG du gouvernement, février 2021, p. 46, *écologie.gouv.fr* [en ligne]. Février 2021. [Consulté le 2 mars 2021]. Disponible à l'adresse : https://www.ecologie.gouv.fr/sites/default/files/Obsolescence%20logicielle.pdf

[589] Projet de loi n° 3875 portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets, du 10 février 2021.

[590] Projet de loi n° 3875 portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets, du 10 février 2021, amendement 2370 du 3 mars 2021 rejeté par la commission spéciale chargée d'examiner le projet le 12 mars 2021.

[591] L'association Halte à l'obsolescence programmée est à l'origine de cette recommandation. Voir en ce sens, HALTE A L'OBSOLESCENCE PROGRAMMEE, Livre blanc. 50 mesures pour une consommation et une production durables, Recommandation n° 48, *halteobsolescence.org* [en ligne]. Février 2019. [Consulté le 20 avril 2020]. Disponible à l'adresse : https://www.halteobsolescence.org/wp-content/uploads/2019/03/Livre-Blanc.pdf

[592] CASTELLAZI M., MOATTI A et al., Rapport CGEDD n° 013416-01 et CGE 2020/11/CGE/SG, *op. cit.*, p. 47 : « *Une telle mesure peut présenter des problèmes liés à la propriété intellectuelle du logiciel, puisque cette ouverture du code ne serait ni plus ni moins qu'une spoliation des droits de son éditeur* ».

C - Contrôles et sanctions

291. Afin de s'assurer de la conformité des opérateurs économiques il convient qu'une autorité de contrôle réalise ce travail de vérification. Il existe donc plusieurs rapports dans la transparence de ces algorithmes : le rapport entre la plateforme et le consommateur par l'intermédiaire de cette obligation d'information précontractuelle que nous avons vu précédemment, et enfin le nécessaire contrôle du respect de la conformité de cette obligation d'information précontractuelle à la réalité du traitement informatisé, ce qui implique nécessairement le recours à un tiers de confiance dans la mesure où ces algorithmes ne peuvent être connus du public.

1 - La Direction Générale de la Concurrence, de la Consommation et de la Répression des fraudes

292. Cette réglementation concerne particulièrement la question des algorithmes dans la mesure où ces acteurs du numérique, ces plateformes en ligne, recourent finalement le moins possible aux travailleurs, bien qu'il existe de nombreux travailleurs du clic[593]. Le positionnement économique de ces acteurs s'effectue donc à travers de nombreux traitements algorithmiques.

293. Comme nous l'avons vu, l'obligation de clarté et de transparence est au service de la loyauté. En ce sens, il convient de s'assurer que la loyauté affichée n'est pas qu'une apparence, mais est bien réelle. C'est donc la DGCCRF qui est chargée du contrôle de conformité de l'information communiquée par les plateformes aux consommateurs. Le manquement à ces obligations d'information précontractuelles est *« passible d'une amende administrative dont le montant ne peut excéder 75 000 euros pour une personne physique et 375 000 euros pour une personne morale* »[594]. De plus, dans le cadre des obligations d'informations renforcées, la DGCCRF peut procéder à des enquêtes pour évaluer et comparer la politique de ces acteurs[595].

294. Dans la mesure où la levée du secret des affaires autour de ces algorithmes vis-à-vis des consommateurs ne peut être réalisée, seule la DGCCRF aurait la capacité de s'assurer que les droits du consommateur sont véritablement effectifs.

---

[593] CASILLI A. A., *En attendant les robots - enquête sur le travail du clic*, *Le Seuil*, 2019, 394 p.
[594] Art. L. 131-4 du Code de la consommation.
[595] Art. L. 111-7-1 al. 2 du Code de la consommation.

295. Le Code de la consommation ne nous informe pas davantage sur la façon dont il convient précisément d'opérer un contrôle entre ce qui est communiqué par la plateforme au titre de son obligation précontractuelle et ce qu'il en est vraiment[596]. De plus, ce principe de loyauté, tel que présenté par le Conseil d'Etat initialement, permettrait d'obtenir de la part des plateformes des informations, des explications à l'utilisateur sur la logique générale de l'algorithme, voire la façon dont il est paramétré, sans pour autant remettre en cause le secret industriel, empêchant de ce fait la communication du code source du programme ou l'accès aux traitements algorithmiques. Cette logique de compromis se heurte néanmoins à un contrôle de la conformité difficile, si ce n'est impossible à réaliser par le consommateur lui-même, d'où l'importance d'instaurer un tiers de confiance techniquement compétent et jouissant d'une confiance, tel un garant de cette conformité.

296. Il existe à cet égard un nouveau protocole entre la CNIL et la DGCCRF afin d'harmoniser les contrôles de ces plateformes lorsque des traitements de données à caractère personnel des consommateurs sont mis en œuvre[597]. Cette collaboration déjà existante est renforcée dans le but notamment de mutualiser les expertises ainsi que les échanges d'informations.

297. Enfin, en matière d'obsolescence logicielle, le parquet de Paris à la suite d'une plainte de l'association Halte à l'obsolescence programmée en 2018 a ouvert une enquête en lien avec la DGCCRF. Certains téléphones de la marque Apple se sont vus proposer en 2017 une mise à jour ralentissant leurs performances lorsque la batterie était ancienne, ce qui a été qualifié de pratique commerciale trompeuse par omission. Sans entrer dans l'étude du code source, le ralentissement du fonctionnement de l'appareil était facilement observable par les utilisateurs et l'autorité de contrôle. Le groupe Apple a accepté une transaction pénale de 25 millions d'euros[598]. Il s'agit de la première transaction à ce sujet[599], ce qui démontre que, malgré la jeunesse de ce régime juridique, la preuve reste compliquée à apporter dans ce domaine, et ce d'autant plus lorsqu'il convient d'établir l'intentionnalité de l'auteur.

---

[596] *Ibid*.

[597] CNIL, « La CNIL et la DGCCRF font évoluer leur protocole de coopération pour renforcer la protection des consommateurs et de leurs données personnelles », *CNIL.fr* [en ligne], 31 janvier 2019. [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.cnil.fr/fr/la-cnil-et-la-dgccrf-font-evoluer-leur-protocole-de-cooperation-pour-renforcer-la-protection-des.

[598] DGCCRF, Transaction avec le groupe APPLE pour pratique commerciale trompeuse, *economie.gouv.fr* [en ligne]. 7 février 2020. [Consulté le 12 mars 2020]. Disponible à l'adresse : https://www.economie.gouv.fr/dgccrf/transaction-avec-le-groupe-apple-pour-pratique-commerciale-trompeuse

[599] SORDINO M-C., « Première transaction pénale en cas d'obsolescence « logicielle » constitutive de pratiques commerciales trompeuses », *RSC*, 2020, p. 960.

298. Il serait toutefois primordial de doter ce tiers de confiance d'une puissance suffisante pour vérifier le contenu et l'adéquation de ces algorithmes au droit[600], ce qui n'est pas une réalité dans les faits.

2 - Le rôle des justiciables

299. Mais la DGCCRF n'est pas la seule garante du bon respect des exigences de loyauté puisque les justiciables concourent également à cette transparence. Au regard des rares décisions de justice rendues pour l'heure[601] sur le fondement de l'article L. 111-7 du Code de la consommation, et spécifiquement sur la question de la transparence des critères de classement de ces algorithmes informatiques, il ressort qu'une association de consommateurs a pu démontrer que les critères mis en avant par une plateforme en ligne n'étaient pas conformes à la réalité. En effet, ce service de comparaison des prix en matière d'assurance ne se fondait pas uniquement sur le prix des prestations pour hiérarchiser des offres de service, mais également sur le profil d'assuré du consommateur qui avait été établi par l'intermédiaire d'un questionnaire[602]. La méthode est donc simple à réaliser afin de s'assurer que les recommandations ne répondent pas qu'à un classement sur le seul fondement du prix. Toutefois, plus les critères sont nombreux et plus il est difficile de déceler les mauvaises pratiques. C'est alors que l'expertise informatique peut devenir indispensable. De la même manière, une plateforme en ligne comparant des services ou des biens ne peut pas « *davantage se borner à renvoyer à (…) ses conditions générales d'utilisation en ce qui concerne la définition et le contenu des différents critères de classement disponibles pour le consommateur* »[603]. C'est en effet dans le cadre de chaque recherche par le consommateur que ces critères doivent être expliqués dans une rubrique distinctive[604].

300. Le contrôle des informations communiquées au consommateur est primordial puisqu'il conditionne la conformité de ces dernières avec la réalité afin qu'il n'existe pas d'asymétrie informationnelle. Contrôler les traitements automatisés de données opérés par ces plateformes

[600] *Infra.*, n° 694 et s.
[601] BERNHEIM-DESVAUX S, « L'association de consommateurs CLCV obtient la condamnation d'une importante plateforme numérique, comparateur de produits d'assurance », *Contrat Concurrence Consommation*, n° 3, Mars 2020, comm. 54.
[602] En ce sens, TGI de Paris, jugement du 17 décembre 2019, RG 17/06223.
[603] TGI de Paris, jugement du 17 décembre 2019, RG 17/06223.
[604] TGI de Paris, jugement du 24 septembre 2019, RG 17/06224.

en ligne n'est toutefois pas aisé compte tenu de leur multiplicité et aussi de leur complexité, reposant essentiellement sur la bonne volonté de la plateforme[605].

301. Les obligations d'information précontractuelle incluant la transparence des plateformes ont concerné dans un premier temps le consommateur, mais force est de constater que les professionnels aussi sont dépendants commercialement de ces grands opérateurs économiques.

PARAGRAPHE 2 - La transparence des algorithmes dans les rapports entre professionnels et vis-à-vis de l'Etat

302. Le droit de la concurrence n'est pas étranger à la question des algorithmes de référencement des contenus par les géants du numérique. En ce sens, la Commission européenne a par exemple déjà infligé à Google une amende de 2 424 495 000 euros pour abus de position dominante[606]. Une enquête avait en effet permis de constater que par l'intermédiaire d'une manipulation de ses algorithmes, le service de Google était soumis à un meilleur référencement que celui de ses concurrents, aboutissant à une moindre visibilité de ces derniers. Il existe par ailleurs de nombreuses collaborations au niveau européen afin d'enquêter sur ces algorithmes. En ce sens, l'autorité de la concurrence fédérale allemande et Française unissent leur expertise pour mieux comprendre les algorithmes utilisés dans l'économie de marché[607]. La régulation de ces algorithmes est un enjeu majeur pour le maintien de l'ordre public économique[608].

303. Des réglementations spécifiques sont toutefois intervenues pour imposer un devoir de diligences à ces plateformes (A). Il existe également un domaine dans lequel l'immixtion des algorithmes est de plus en plus présente et pressante, il s'agit des plateformes de marché à travers le trading algorithmique (B).

---

[605] MIGAYRON S., « Contradictoire et confidentialité dans les expertises des litiges du monde numérique : une mission impossible ? », *Revue communication-commerce électronique*, n° 4, avril 2020.
[606] Commission européenne, décision du 27 juin 2017, affaire AT.38740, Moteur de recherche Google (Shopping).
[607] LE DORZE Y., Algorithmes et concurrence, l'Autorité et le Bundeskartellamt publient une étude commune, *Autorité de la concurrence.fr* [en ligne]. 06 novembre 2019. [Consulté le 12 novembre 2020]. Disponible à l'adresse : https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/algorithmes-et-concurrence-lautorite-et-le-bundeskartellamt-publient-une#:~:text=de%20l'institution-,Algorithmes%20et%20concurrence%2C%20l'Autorit%C3%A9%20et%20le,Bundeskartellamt%20publient%20une%20%C3%A9tude%20commune&text=Dans%20leur%20projet%20conceptuel%20commun,pouvant%20%C3%AAtre%20associ%C3%A9s%20aux%20algorithmes.
[608] Voir en ce sens, HARNAY S., MARTY F., TOLEDANO J., Concurrence et risque algorithmique : quelle régulation des algorithmes ?, *Chairgovreg.fondation-dauphine.fr* [en ligne]. [Consulté le 12 septembre 2020]. Disponible à l'adresse : https://chairgovreg.fondation-dauphine.fr/sites/chairgovreg.fondation-dauphine.fr/files/attachments/GovRegNotes_Concurrence%20et%20risque%20algorithmique.pdf

A - La transparence des plateformes en ligne dans les relations « *Plateform to Business* » : le cas des entreprises utilisatrices

304. Il a également été question de dupliquer les obligations d'informations que nous avons vu précédemment entre professionnels[609], car le Code de la consommation ne concerne que les rapports entre le professionnel et les consommateurs[610]. En effet, dans l'hypothèse de l'intermédiation entre professionnels, il n'était pas possible de connaître la manière dont la plateforme recourt à la recommandation de certains vendeurs plutôt qu'à d'autres. C'est du côté du droit de l'Union européenne que ces exigences ont été établies, pour plus de cohérence.

305. Comme le fait remarquer à juste titre Fernanda Sabrinni « *grâce à ce pouvoir, certaines plateformes façonnent et déterminent les conditions d'accès aux informations de manière subtile sans qu'il soit possible de savoir s'il s'agit d'une publicité, d'une adaptation personnalisée ou d'une sélection aléatoire des algorithmes* »[611].

306. La transparence de ces plateformes est primordiale parce que ces géants du numérique sont à même de privilégier un fournisseur de services ou de biens par rapport à d'autres prestataires pour des raisons qui nous échapperaient. En effet, comme nous l'avons expliqué, tout référencement implique la priorisation d'une information vis-à-vis d'une autre selon des critères établis. Dans ce cas de figure, les algorithmes sont susceptibles de mettre en œuvre les politiques économiques des opérateurs en ligne. Pour autant, il est souligné par certains auteurs qu'une transparence trop accrue des algorithmes de certaines plateformes pourrait engendrer des ententes sur les prix[612]. D'autres voient également dans ces géants de l'intermédiation, une telle puissance de marché qu'ils s'appropriaient des prérogatives si exorbitantes, normalement réservées aux Etats, qu'elles sont constitutives d'attributs de souveraineté[613]. Ces attributs de souveraineté sont d'autant plus effectifs concernant les entreprises qui sont dépendantes de ces plateformes, et ne pourraient prospérer économiquement indépendamment d'elles. Puisque force est de constater que sans un référencement de leurs offres sur ces plateformes, elles

[609] Il convient par ailleurs d'entendre par professionnel ayant recours aux services d'intermédiation au sens du présent règlement *« tout particulier qui agit dans le cadre de son activité commerciale ou professionnelle ou toute personne morale qui, par le biais de services d'intermédiation en ligne, offre des biens ou services aux consommateurs à des fins liées à son activité commerciale, industrielle, artisanale ou libérale ;* », art. 2 1) Règlement UE 2019/1150 du Parlement Européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne.
[610] *Supra.*, n° 265 et s.
[611] SABRINNI F, « La notion de plateforme au cœur des nouvelles relations entre professionnels : regards croisés entre deux réglementations : P2B vs loi pour une République numérique », *RTD com.*, 2020, p. 215.
[612] RODA J., « L'entente algorithmique », *La Semaine Juridique Edition Générale* n° 28, 15 Juillet 2019, doctr. 785
[613] PASQUALE F., From territorial to functional Sovereignty: The case of Amazon, *lpeblog.com, Blog Law and Political Economy* [en ligne]. 6 décembre 2017 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/

n'existeraient pas aux yeux du consommateur. Mais c'est ici la relation entre le professionnel et la plateforme qui attire notre attention, bien qu'elle conditionne naturellement leurs rapports avec le consommateur.

307. Comme nous l'avons vu, une certaine transparence des plateformes en ligne mettant en relation les professionnels et les consommateurs a été mise en œuvre[614]. Il était donc somme toute logique que des dispositions relatives à la transparence des plateformes en ligne, et donc également de leurs algorithmes, dans les relations entre professionnels voient le jour. L'enjeu n'est plus seulement de protéger le consommateur, mais de permettre aux entreprises dépendantes de l'intermédiation avec des plateformes monopolistiques de connaître le fonctionnement de ces algorithmes. Le Règlement européen du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne[615] est alors notamment intervenu à cette fin.

1 - Les plateformes concernées

308. Les plateformes en ligne concernées par ces nouvelles obligations sont relativement larges bien qu'elles semblent plus restrictives que celles définies par la LRN[616]. Il convient de retenir que les opérateurs de plateforme soumis aux obligations que nous allons étudier sont celles offrant un service d'intermédiation en ligne. Selon le Règlement européen, cela concerne donc les plateformes répondant à trois conditions cumulatives. Premièrement, est qualifié de service de la société de l'information « *tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services* »[617]. Ensuite, ce service doit permettre aux entreprises utilisatrices de la plateforme de proposer des services et des biens à des consommateurs[618]. Enfin, cette intermédiation entre l'entreprise utilisatrice et le fournisseur du service est susceptible de reposer sur une relation

[614] *Supra.*, n° 265 et s.
[615] Règlement UE 2019/1150 du Parlement Européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne.
[616] Sont considérés comme services d'intermédiation en ligne *« les services qui répondent à toutes les conditions suivantes: a) ils constituent des services de la société de l'information au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil (12); b) ils permettent aux entreprises utilisatrices d'offrir des biens ou services aux consommateurs, en vue de faciliter l'engagement de transactions directes entre ces entreprises utilisatrices et des consommateurs, que ces transactions soient ou non finalement conclues; c) ils sont fournis aux entreprises utilisatrices sur la base de relations contractuelles entre le fournisseur de ces services et les entreprises utilisatrices qui offrent des biens ou services aux consommateurs; »*, art. 2 2) du Règlement.
[617] Directive UE 2015/1535 du Parlement Européen et du Conseil du 9 septembre 2015, Art. 1, § 1 b).
[618] Règlement UE 2019/1150 du Parlement Européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, art. 2 b).

contractuelle[619]. Cette vision n'englobe donc pas toutes les plateformes[620], car il suffit qu'une de ces conditions fasse défaut pour qu'elles ne soient pas concernées par les obligations de transparence que nous allons étudier.

2 - La nature de l'obligation

309. Il est à noter que les obligations évoquées s'appliquent aussi bien lors de la phase contractuelle que précontractuelle[621].

310. Les fournisseurs de services d'intermédiation en ligne doivent indiquer dans leurs conditions générales d'utilisation les « principaux paramètres » sur lesquels reposent le classement ainsi que les « *raisons justifiant l'importance relative de ces principaux paramètres par rapport aux autres paramètres* »[622].

311. Concernant les fournisseurs de moteurs de recherche en ligne, les obligations de transparence sont renforcées, notamment car ces outils exercent de par leurs référencements une emprise très importante sur la vie de l'activité professionnelle. Ils doivent être en mesure de préciser les principaux paramètres « *en fournissant une description facilement, et publiquement accessible, énoncée dans une formulation claire et compréhensible, sur les moteurs de recherche en ligne de ces fournisseurs* ». Cette description doit être à jour, ce qui s'explique par le fait que ces outils sont très évolutifs[623]. Qu'il s'agisse de fournisseurs de moteurs de recherche ou d'intermédiation en ligne, dès lors que le classement est susceptible d'être effectué en fonction d'une rémunération directe ou indirecte d'une entreprise utilisatrice ou d'un utilisateur, le fournisseur offre *« une description de ces possibilités et des effets de cette rémunération sur le classement* »[624] . De ce point de vue, nous nous rapprochons donc de la philosophie de la LRN. Toutes ces obligations[625] sont jugées suffisantes pour appréhender le classement à travers

[619] *Ibid*., Art. 2 c).
[620] Pour plus d'informations à ce sujet, voir NOËL E., « Les vulnérabilités entre plateforme en ligne et entreprises utilisatrices », *Les Cahiers de la Recherche sur les Droits Fondamentaux*, n° 18, 2020, p. 112.
[621] Règlement UE 2019/1150 du Parlement Européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, Art. 3.
[622] *Ibid*., art. 5.
[623] *Ibid*., art. 5., § 2.
[624] *Ibid*., art. 5., § 3. Et conformément aux exigences des points 1 et 2 de l'art. 5 précité.
[625] Art. § 1, 2 et 3 précités.

« a) les caractéristiques des biens et services proposés aux consommateurs par le biais des services d'intermédiation en ligne ou des moteurs de recherche en ligne; b) la pertinence de ces caractéristiques pour ces consommateurs; c) en ce qui concerne les moteurs de recherche en ligne, les caractéristiques de conception du site internet utilisé par les utilisateurs de sites internet d'entreprise. »[626].

312. De plus, si les algorithmes d'un moteur de recherche venaient à modifier le classement, voire aboutiraient à son déférencement à cause du signalement effectué par un tiers, *« le fournisseur offre à l'utilisateur de site internet d'entreprise la possibilité de consulter le contenu de cette notification* »[627]. Le principe de la notification du déréférencement est important puisqu'il va conditionner la possibilité d'une plainte[628].

313. Nous retrouvons donc une notion d'intelligibilité des algorithmes dans la mesure où tous les critères ne sont pas connus, et dont l'étendue semble limitée à des notions de clarté. Pour étayer ce propos, le paragraphe 6 de l'article 5 précise que lorsque ces exigences sont satisfaites, les fournisseurs ne sont pas tenus de divulguer leurs algorithmes ou des informations trop précises qui auraient pour conséquence « *de permettre de tromper les consommateurs ou de leur porter préjudice par la manipulation des résultats de recherche* ». Force est de constater que le présent règlement est très favorable aux plateformes saisies par ce dernier. Cette transparence se heurte, comme le précise également ce paragraphe, au secret des affaires[629].

314. Le problème n'est pas tant que les algorithmes ne soient pas communiqués, car le respect de ces obligations permettrait de considérer qu'elles sont satisfaites, mais plutôt qu'une autorité tierce ne garantisse pas que les informations déclarées sont bien celles qui sont appliquées. Les Etats membres sont certes tenus de faire respecter le présent règlement, toutefois ce dernier ne prévoit pas que les autorités de contrôle puissent accéder explicitement à ces algorithmes. Il est également prévu qu'en application des dispositions de « transparence » de l'article 5, des lignes directrices seront édictées par la Commission[630]. Cette transparence n'est donc pas assimilable à des dispositions de conformité stricte.

---

[626] *Ibid*., art. 5, § 5.
[627] *Ibid*., art. 5, § 4.
[628] *Ibid*., art. 11.
[629] Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (Texte présentant de l'intérêt pour l'EEE). Cette directive a de plus fait l'objet d'une transposition dans notre droit national à travers la loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires.
[630] Règlement UE 2019/1150 du Parlement Européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, art. 5, § 7.

315. Il est intéressant de constater que le législateur européen a fait primer l'intérêt des plateformes en ligne au détriment des entreprise utilisatrices. Toutefois, dans la continuité du règlement étudié[631], une nouvelle proposition de la Commission européenne[632] souhaite modifier les rapports de force entre grandes plateformes commerciales et les entreprises utilisatrices, notamment pour que cela soit profitable aux consommateurs. L'objectif « *est de permettre aux plateformes de libérer tout leur potentiel en traitant au niveau de l'UE les cas les plus marquants de pratiques déloyales et la faible contestabilité afin de permettre aux utilisateurs finaux comme aux entreprises utilisatrices de tirer pleinement parti de l'économie des plateformes et de l'économie numérique en général, dans un environnement contestable et équitable* »[633]. Les contrôleurs d'accès[634] de par leur agrégation de puissance et de l'influence qu'ils exercent seraient soumis à d'importants contrôles de la part de la Commission, ce qui va dans le bon sens. Ainsi, elle dispose d'un important pouvoir d'enquête puisqu'elle serait en mesure de demander à des fins de conformité « *l'accès aux bases de données et algorithmes des entreprises, ainsi que des explications les concernant, par simple demande ou par voie de décision* »[635]. Des contrôles sur place pourront être réalisés au sein des locaux de ces entreprises, notamment par le recours à des experts et auditeurs en vue d'étudier les systèmes informatiques, dont les algorithmes[636]. En cas de refus de se soumettre à une telle demande d'accès à une base de données ou aux algorithmes dans le cadre d'une enquête, une importante amende pouvant aller jusqu'à 1% du chiffre d'affaires total réalisé lors de l'année précédente pourrait être prononcée[637]. Des astreintes dissuasives seront également prévues à cet égard. Elles atteindraient jusqu'à 5% du chiffre d'affaires journalier de l'entreprise[638].

[631] *Ibid*.
[632] Proposition de règlement n° 2020/0374 du Parlement européen et du Conseil relatif aux marchés numériques (législation sur les marchés numériques) en date du 15 décembre 2020.
[633] *Ibid*., p. 3.
[634] Sont qualifiés de contrôleur d'accès « *Les fournisseurs de services de plateforme essentiels peuvent être considérés comme des contrôleurs d'accès s'ils : i) ont une incidence importante sur le marché intérieur ; ii) exploitent un ou plusieurs points d'accès majeurs pour les clients ; et iii) jouissent ou sont censés jouir d'une position solide et durable dans leurs opérations* », *ibid*., p. 2 à 3.
[635] *Ibid*., art. 19 § 1.
[636] *Ibid*., art. 21 § 3.
[637] *Ibid*., art. 26 § 2 e).
[638] *Ibid*., art. 27 § 1 c).

B - La transparence des traitements automatisés de données du secteur financier

316. Le déploiement des traitements automatisés de données dans le cadre des transactions financières s'est accentué au cours des dernières décennies. Le *trading algorithmique*[639] est jugé si opaque que sa part dans les échanges financiers n'est qu'estimative. Il représenterait jusqu'à 60 % des transactions aux Etats-Unis d'Amérique et 40% en Europe[640]. Sa démocratisation fait craindre une aggravation de la spéculation, des krachs ainsi que des infractions telles que le délit d'initié entre plusieurs opérateurs économiques. Il constitue donc un enjeu majeur pour les autorités de régulation des marchés financiers qui ont pour compétence de sanctionner les abus de marché et autres manquements. A titre d'exemple, les abus de marché constituent des comportements illicites des acteurs intervenant sur les machés, et qui portent atteinte à leur transparence[641]. Les algorithmes doivent alors être regardés, du fait de leur opacité, comme des perturbateurs de l'intégrité des marchés, justifiant une régulation et une transparence accrue vis-à-vis de l'Etat.

317. Dès 2013, le législateur national, à travers la loi de séparation et régulation des activités bancaires[642], avait introduit une nouvelle section au sein du Code monétaire relative à « l'obligation d'information sur les dispositifs de traitement automatisé », pour notamment y encadrer le négoce à haute fréquence[643]. L'article L. 451-4 du Code monétaire et financier, abrogé depuis[644], disposait déjà que toute personne devait notifier à l'autorité des marchés financiers (AMF) l'utilisation d'un dispositif « *de traitement automatisé générant des ordres de vente ou d'achat de titres de sociétés dont le siège social est localisé en France* »[645]. Chaque ordre de cette nature devait bénéficier d'une traçabilité et d'une conservation « *permettant d'établir le lien entre un ordre donné et les algorithmes ayant permis de déterminer cet ordre,*

---

639 *« la négociation d'instruments financiers dans laquelle un algorithme informatique détermine automatiquement les différents paramètres des ordres, comme la décision de lancer l'ordre, la date et l'heure, le prix ou la quantité de l'ordre, ou la manière de gérer l'ordre après sa soumission, avec une intervention humaine limitée ou sans intervention humaine; ne couvre pas les systèmes utilisés uniquement pour acheminer des ordres vers une ou plusieurs plates-formes de négociation ou pour le traitement d'ordres n'impliquant la détermination d'aucun paramètre de négociation ou pour la confirmation des ordres ou pour exécuter les ordres de clients ou pour le traitement post-négociation des transactions exécutées;* ». Cons. 39 de la Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE Texte présentant de l'intérêt pour l'EEE.

640 LES PARTENAIRES DE CHALLENGES, Le trading haute fréquence en mutation, *Challenges.fr* [en ligne], 30 janvier 2020 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.challenges.fr/entreprise/le-trading-haute-frequence-en-mutation_696509.

641 LASSERRE CAPDEVILLE J., STORCK M., CHEVRIER E., PISONI P., « Code monétaire et financier, annoté & commenté », *Dalloz*, 2020, spec. p. 2403.

642 Loi n° 2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires.

643 *Ibid*., art. 17.

644 Ordonnance n° 2016-827 du 23 juin 2016 relative aux marchés d'instruments financiers, art. 26.

645 *Ibid*., 1°.

conserver tous les algorithmes utilisés pour élaborer les ordres transmis aux marchés et les transmettre à l'Autorité des marchés financiers lorsqu'elle en fait la demande »[646]. Les personnes utilisant ces dispositifs avaient également pour obligation de mettre « *en place des procédures et des mécanismes internes garantissant la conformité de leur organisation* » avec les règles de traçabilité.

318. C'est donc la notification du recours à un traitement automatisé de données qui prévalait auprès de l'AMF. Cette notification est importante, car elle va ensuite conditionner le contrôle par l'autorité. En effet, bien qu'il faille être vigilant vis-à-vis des acteurs qui ne joueraient pas le jeu de la notification, cette dernière permet à l'autorité de contrôle de cibler ses efforts dans le contrôle des opérations de marché.

319. Avec le règlement européen du 16 avril 2014 relatif aux abus de marché[647] et la transposition d'une directive du 15 mai 2014 concernant les marchés d'instruments financiers[648], de nouvelles règles sont venues encadrer le *trading algorithmique*. Ces nouvelles technologies de négociation ne font pas toujours intervenir des humains, et sont souvent purement automatisées. Le volume d'échanges réalisé par ces algorithmes inquiète, notamment parce qu'il est opaque. Afin d'éviter les travers du *trading algorithmique*, l'article 17 de la directive du 15 mai 2014 prévoit également un système de notification de l'entreprise d'investissement qui y a recourt aux autorités compétentes de l'Etat membre ainsi qu'à la plateforme de négociation sur laquelle est déployé un tel système[649]. La réglementation va bien plus loin que la mise en œuvre d'un système de notification dans la mesure où l'autorité de contrôle peut demander à l'entreprise utilisatrice

> « *de façon régulière ou ponctuelle, une description de la nature de ses stratégies de trading algorithmique et des informations détaillées sur les paramètres de négociation ou les limites auxquelles le système est soumis, sur les principaux contrôles de conformité et des risques mis en place pour garantir que les conditions prévues au paragraphe 1 sont remplies et sur les tests conduits sur ses systèmes. L'autorité compétente de l'État membre d'origine de l'entreprise*

[646] *Ibid*., 2°.
[647] Règlement (UE) No 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission.
[648] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE Texte présentant de l'intérêt pour l'EEE et ses règlements délégués n° 2017/591 et 592 de la Commission en date du 1er décembre 2016.
[649] *Ibid*., art. 17 § 2.

d'investissement peut, à tout moment, demander à cette dernière des informations complémentaires sur son trading algorithmique et sur les systèmes utilisés pour celui-ci »[650].

320. La plateforme de négociation sur laquelle officie la société par l'intermédiaire d'un *trading algorithmique* peut solliciter auprès de l'autorité compétente (l'AMF pour la France) dans un délai non excessif les informations que l'entreprise a communiqué au régulateur. Pour que l'autorité de contrôle puisse s'assurer de la conformité du traitement algorithmique aux règles ici présentées, la société doit enregistrer ses activités[651].

321. Concernant spécifiquement le *trading haute fréquence*[652], qui est une des composantes du *trading algorithmique*, l'entreprise utilisatrice doit tenir un registre validé, précis et chronologique de tous les ordres qu'elle passe afin de les mettre à disposition de l'autorité compétente en cas de demande. Ce ne sont donc pas tant les algorithmes qui intéressent l'autorité de contrôle, mais plutôt l'étude des ordres, c'est-à-dire le résultat du traitement.

322. La société qui déploie un tel traitement automatisé doit également mettre en œuvre un système de « *contrôle des risques efficaces* » de ces derniers, notamment afin d'éviter qu'ils soient utilisés à des fins contraire au règlement du 16 avril 2014 ou aux règles d'une plateforme de négociation à laquelle le système est connecté[653]. Ce mécanisme de contrôle du risque doit être adapté à son activité. Pour ce faire, ces systèmes sont soumis à « *des seuils et limites de négociations* », puis doivent prévenir « *l'envoi d'ordres erronés ou tout autre fonctionnement des systèmes susceptible de donner naissance ou de contribuer à une perturbation du marché* ». Pour se prémunir des défaillances, le traitement automatisé est testé et suivi afin de s'assurer de la conformité des dispositions précitées.

---

650 *Ibid.*

651 *Ibid*.

652 Le *« trading haute fréquence est « un système de négociation analyse à grande vitesse les données ou les signaux du marché et envoie ou actualise ensuite une grande quantité d'ordres dans un délai très court en réponse à cette analyse. En particulier, le trading algorithmique à haute fréquence peut comporter des éléments comme l'engagement, la création, l'acheminement et l'exécution d'un ordre, qui sont déterminés par le système sans intervention humaine pour chaque transaction ou ordre, la brièveté de l'échéance pour l'établissement et la liquidation des positions, un taux élevé de rotation quotidienne du portefeuille, un ratio ordre/transaction très élevé sur la journée et une clôture de la journée sur une position proche de la position uniforme. Le trading algorithmique à haute fréquence est caractérisé, entre autres, par un débit élevé de messages sur la journée qui constituent des ordres, des prix ou des annulations »*, (61) de la directive.
Il se caractérise juridiquement par *« a) une infrastructure destinée à minimiser les latences informatiques et les autres types de latence, y compris au moins un des systèmes suivants de placement des ordres algorithmiques: colocalisation, hébergement de proximité ou accès électronique direct à grande vitesse; L 173/384 Journal officiel de l'Union européenne 12.6.2014 FR b) la détermination par le système de l'engagement, la création, l'acheminement ou l'exécution d'un ordre sans intervention humaine pour des transactions ou des ordres individuels; et c) un débit intrajournalier élevé de messages qui constituent des ordres, des cotations ou des annulations;* », art. 4. 40) de la directive.

653 *Ibid*., art. 17 § 1.

323. Si l'entreprise d'investissement déploie un système de *trading algorithmique* permettant un accès direct électronique au marché afin qu'il soit utilisé par des clients sur une plateforme de marché, elle doit contrôler, évaluer et examiner ce dernier afin que l'usage soit conforme au règlement et à la directive[654]. L'objectif est de responsabiliser les prestataires dans le cadre de cet accès direct des clients à la plateforme d'échange. Si une infraction, tel un abus de marché, est constatée par l'entreprise d'investissement, l'autorité compétente doit en être informée et l'entreprise d'investissement demeure responsable.

324. Chaque accès direct est de plus notifié aussi bien à l'autorité compétente qu'à la plateforme de négociation sur laquelle l'accès direct a lieu, et ce afin qu'un contrôle puisse le cas échéant s'opérer. Le but poursuivi par cette obligation de notification est de permettre une fois de plus à l'autorité compétente de surveiller le traitement. Pour ce faire, elle peut demander à la société d'investissement *« de fournir, de façon régulière ou ponctuelle, une description des systèmes et contrôles visés au premier alinéa et la preuve qu'ils ont été appliqués* ». Ladite entreprise tient à ce titre un registre de ses activités afin que l'autorité de contrôle vérifie la conformité des traitements algorithmiques avec les exigences de la directive.

325. Les marchés réglementés doivent également prévoir des coupe-circuits permettant le cas échéant de suspendre ou d'exclure les ordres algorithmiques qui perturberaient le bon ordre du marché. Il s'agit ici d'un certain pragmatisme puisque cela permet de ne pas uniquement se fonder sur les notifications qui ont pu être effectuées par les entreprises aux autorités compétentes. C'est en effet admettre que des ordres irréguliers sont l'œuvre d'une infraction intentionnelle ou bien d'un dysfonctionnement du traitement algorithmique.

326. Les Etats membres requièrent

> *« d'un marché réglementé qu'il dispose de systèmes, de procédures et de mécanismes efficaces, y compris qu'il exige de ses membres ou de ses participants qu'ils procèdent à des essais appropriés d'algorithmes et mettent à disposition les environnements facilitant ces essais, pour garantir que les systèmes de trading algorithmique ne donnent pas naissance ou ne contribuent pas à des conditions de négociation de nature à perturber le bon ordre du marché, et pour gérer les conditions de négociation de nature à perturber le bon ordre du marché qui découlent de ces systèmes de trading algorithmique, y compris de systèmes*

[654] *Ibid*., art. 15 § 5.

permettant de limiter la proportion d'ordres non exécutés par rapport aux transactions susceptibles d'être introduites dans le système par un membre ou un participant, de ralentir le flux d'ordres si le système risque d'atteindre sa capacité maximale ainsi que de limiter le pas minimal de cotation sur le marché et de veiller à son respect. »[655].

327. En tant qu'AAI, l'AMF dispose notamment pour faire respecter la conformité de ces traitements automatisés à la réglementation d'un pouvoir de contrôle, d'enquête et de sanction. Concernant le pouvoir de contrôle et de sanction, d'une part, l'autorité peut se faire communiquer tout document[656], et elle peut sanctionner les comportements illicites d'autre part. Tel a été par exemple le cas lorsque l'AMF a enquêté à partir de 2010 au sujet d'un événement susceptible d'être une manipulation de marché du fait d'un *trading algorithmique*. A défaut de données fiables et complètes sur une longue période, les enquêteurs ont choisi d'analyser une journée entière de transaction sur plusieurs titres et a pu en déduire une manipulation de marché. La société Virtu a alors été condamnée au titre de cette infraction, notamment parce qu'elle a manqué au principe de transparence des marchés, ce qui engendre également un risque pour les autres investisseurs[657]. Toutefois, il convient de nuancer ce cadre juridique puisque des manipulations algorithmiques peuvent avoir lieu à l'étranger, et engendrer des conséquences économiques, y compris sur notre territoire. Tel fut le cas avec le mini krach de Wall Street en 2010 faisant perdre 1000 milliards de dollars en vingt minutes[658].

328. Se pose donc naturellement la question de mettre en place des mécanismes de surveillance des marchés en temps réel[659]. En effet, il est devenu très difficile de contrôler le flux des transactions, lorsque de l'aveu même du directeur des enquêtes de l'AMF, Laurent Combourieu, « *Il y a dix ans, on avait analysé par jour soixante-dix ordres par valeur sur un marché – celui d'Euronext. Aujourd'hui un trader à haute fréquence passe un million d'ordres par jour par valeur sur cinq marchés différents* »[660]. Force est de constater que les ordres de grandeur dépassent désormais l'entendement humain.

---

[655] *Ibid*., art. 48 § 6.
[656] Art. L. 621-10 du Code monétaire et financier.
[657] AMF, déc, du 4 décembre 2015. De plus, selon le Conseil d'Etat, l'enquête de l'AMF au sujet de l'analyse du flux de ces algorithmes a été correctement étayée pour caractériser la manipulation du marché, voir en ce sens, CE, 19 mai 2017, n° 396698.
[658] AIT-KACIMI Nessim., Algorithmes en folie, Krachs en série, Les Echos.fr [en ligne]. 1er juin 2013 (consulté le 27 août 2021). Disponible à l'adresse : http://archives.lesechos.fr/archives/2013/Enjeux/00301-032-ENJ.htm
[659] A la question faudra-t-il des algorithmes pour contrôler d'autres algorithmes, voir CAPITAL, Intelligence artificielle : la Bourse bientôt contrôlée par des boîtes noires ?, *Capital.fr* [en ligne]. 02 décembre 2019 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.capital.fr/entreprises-marches/intelligence-artificielle-la-bourse-bientot-controlee-par-des-boites-noires-1356599 (part. 2).
[660] SIMON D., Bourse, toujours plus vite : la peur du bug, *France Inter.fr* [en ligne]. 8 avril 2016 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.franceinter.fr/emissions/le-zoom-de-la-redaction/le-zoom-de-la-redaction-08-avril-2016

329. L'article L. 621-10 du Code monétaire et financier dote l'AMF d'un important pouvoir d'enquête et de contrôle permettant d'obtenir la communication de « *tous documents, quel qu'en soit le support* ». Cette autorité administrative peut également effectuer des contrôles sur pièce ainsi que procéder à des auditions des personnes susceptibles de fournir des informations. Il est intéressant de relever que l'AMF disposait d'un pouvoir encore plus conséquent puisque les enquêteurs pouvaient obtenir la communication des données « *conservées et traitées par les opérateurs de télécommunications* »[661]. Cette rédaction a toutefois fait l'objet d'une déclaration d'inconstitutionnalité car cette procédure n'offrait pas de garantie suffisante entre le droit au respect de la vie privée et la prévention des atteintes à l'ordre public[662]. Nous comprenons donc parfaitement que la transparence ne peut être absolue, y compris lorsqu'il s'agit d'algorithmes, dans la mesure où d'autres impératifs doivent être conciliés[663], ce qui n'est toutefois pas sans poser la question de l'exclusion des algorithmes dans ce domaine à défaut de pouvoir en obtenir une transparence coûte que coûte[664]. Une autorité européenne des marchés financiers (AEMF) veille également au bon fonctionnement du marché en enquêtant sur le *trading algorithmique*.

330. Enfin, l'ordonnance n° 2016-827 du 23 juin 2016 relative aux marchés d'instruments financiers est venue notamment transposer la directive 2014/65/UE. Elle a introduit cette transparence en droit national aux articles L. 533-10-3 et suivant du Code monétaire et financier.

SECTION 2 - LES AUTRES TENTATIVES INSTAURANT UN REGIME JURIDIQUE DISPARATE DE DROIT PRIVE DE TRANSPARENCE DES ALGORITHMES

331. Tout en étant sources de progrès en permettant l'épanouissement de certains droits et libertés comme la liberté d'expression[665], les plateformes en ligne dont les réseaux sociaux inquiètent par la propagation de certains contenus, ce qui a notamment engendré une loi relative à la lutte contre la manipulation de l'information.

[661] La communication de ces informations s'effectuait dans le cadre *« de l'article L. 34-1 du code des postes et des communications électroniques et les prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et en obtenir la copie »*.
[662] CC, décision n° 2017-646/647 QPC, 21 juillet 2017.
[663] *Infra*., n° 653 et s.
[664] *Infra*., n° 974 et s.
[665] Ce qui leur vaut la qualification de « droit facilitateur », LA RUE F., « Report of the special Rapporteur on the promotion and protection of the right to freedom of opinion and expression », in R*apport des Nations Unies*, mai 2011.

332. Mais au-delà de ces considérations, les réseaux sociaux seraient pour certains un vecteur de haine en ligne, parce que ces plateformes se contenteraient d'héberger des contenus sans y jouer un rôle de régulateur de ces derniers. Le législateur est alors intervenu à de nombreuses reprises pour imposer de nouvelles obligations. Or, compte tenu du nombre d'utilisateurs et des contenus échangés sur ces plateformes en un intervalle de temps très court, la suppression de ces contenus repose sur d'importants algorithmes privés de retrait voire de filtrage des contenus, à défaut de pouvoir humainement tout traiter. Les algorithmes font également leur immixtion sur les plateformes d'intermédiation recourant aux travailleurs du numérique (Paragraphe 1).

333. Les opérateurs de plateforme ne sont pas les seuls à recourir à des algorithmes puisqu'ils sont également utilisés dans le cadre des outils d'aide à la prise de décision privée, ce qui n'est pas sans inquiéter, et ce sans nécessairement faire intervenir un traitement de données à caractère personnel (Paragraphe 2).

PARAGRAPHE 1 – Le cas de la transparence des autres plateformes numériques

334. Les hébergeurs de contenus utilisaient déjà des algorithmes afin d'obtenir la suppression des contenus non conformes à leurs conditions générales d'utilisation, puisque rappelons le, ces plateformes ne sont pas soumises aux règles juridiques s'appliquant à l'espace public : la source de ce droit étant de nature contractuelle. Fort de ce savoir-faire en matière d'algorithmes, que l'Etat ne détient pas, c'est donc sur ces algorithmes privés que le législateur a voulu faire reposer la suppression de nombreux contenus illicites.

335. C'est alors que la censure algorithmique a été considérée comme un outil significatif d'effectivité du droit sur ces plateformes numériques (A), ce qui n'est pas sans interroger sur la transparence de ces dispositifs qui régissent par exemple l'exercice de la liberté d'expression. Il nous semble par ailleurs opportun de retracer l'historique d'une tendance allant vers plus de transparence des plateformes en ligne.

336. Il en est également de même avec les plateformes numériques en droit social. Ces plateformes déterminent en toute opacité les conditions de travail des salariés, mais aussi des indépendants. Derrière l'ubérisation, ce sont les algorithmes qui font droit et n'hésitent pas à concurrencer le droit étatique et les accords collectifs (B).

A - La transparence du retrait des contenus par les traitements algorithmiques des hébergeurs

337. Il est à noter qu'au-delà des dispositions juridiques spécifiques que nous étudions, des normes générales sont susceptibles de concourir à une plus grande compréhension des traitements algorithmiques, en l'occurrence ceux utilisés par les hébergeurs. A titre d'exemple, le Tribunal judiciaire de Paris a ordonné[666] à la société Twitter la communication de tout document contractuel, technique et administratif relatifs notamment aux moyens matériels, ce qui comprend nécessairement les algorithmes utilisés dans la lutte contre la haine en ligne. Cette ordonnance a été prise en application de l'article 145 du Code de procédure civile[667] afin d'évaluer la tenue d'un procès au fond.

1 - La transparence du retrait des contenus par les traitements algorithmiques des hébergeurs

a - De la proposition de loi visant à lutter contre les contenus haineux sur internet…

338. Il s'agit d'une transparence particulière qui se justifie naturellement pour des raisons d'équité et de loyauté, mais également parce que la puissance publique tend à confier de plus en plus à des opérateurs économiques, en l'occurrence aux fournisseurs de service, l'exercice des droits et libertés au sein de cet environnement telle que par exemple la liberté d'expression.

339. Les hébergeurs[668] avaient déjà pour obligation de retirer certains contenus illicites[669] dans un délai de 24h. Il s'agissait d'obtenir la suppression ou le déférencement administratif, et donc sans l'intervention préalable d'un juge, des propos[670] portant incitation d'actes terroristes

---

666 Tribunal Judiciaire de Paris, n° 20/53181 du 6 juillet 2021.

667 L'article 145 du Code de procédure civile dispose que « *s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé* ».

668 Les hébergeurs de contenus visés par l'article 6-1 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique sont « *les personnes dont l'activité est d'éditer un service de communication au public en ligne mettent à disposition du public* » ainsi que « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* »

669 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, transposant la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »). Selon l'article 6-1 de ladite loi, il s'agit des contenus terroristes, c'est-à-dire les propos portant sur une incitation à des « *actes terroristes » ou faisant l'« apologie de tels actes* » prévus à l'article 421-2-5 du Code pénal, mais également pédopornographique, c'est-à-dire « *la diffusion des images ou des représentations de mineurs relevant* » de l'art. 227-23 du Code pénal.

670 Selon l'article 6-1 de ladite loi, il s'agit des contenus terroristes, c'est-à-dire les propos portant sur une incitation à des « *actes terroristes » ou faisant l'« apologie de tels actes* » prévus à l'article 421-2-5 du Code pénal, mais également

ou à leur apologie ainsi que les contenus dits pédopornographiques. Par l'intermédiaire de la loi dite « cyberhaine »[671], le législateur français avait toutefois souhaiter porter cette obligation de retrait initialement de 24h à 1h[672] à compter de la notification par l'autorité administrative.

340. De plus, la proposition de loi visant à lutter contre les contenus haineux sur internet voulait imposer par ailleurs aux opérateurs de plateforme en ligne définis à l'article L. 111-7 du Code de la consommation, c'est-à-dire à « *toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public* », de retirer ou de rendre inaccessibles[673] « *tout contenu contrevenant manifestement* » à une liste conséquente d'infractions[674] dans un délai de 24h à compter de la notification de dénonciation des propos par une ou plusieurs personnes[675]. Il était convenu que cette obligation soit étendue aux moteurs de recherche, à savoir aux activités reposant sur le classement ou le référencement de contenus proposés ou mis en ligne par des tiers aux moyens de traitement algorithmiques[676]. Cependant, seules les plateformes dépassant un certain seuil d'activités

pédopornographique, c'est-à-dire « *la diffusion des images ou des représentations de mineurs relevant* » de l'art. 227-23 du Code pénal.

[671] Loi visant à lutter contre les contenus haineux sur internet.

[672] Art. 1er de la proposition de loi visant à lutter contre les contenus haineux sur internet, modifiant l'art. 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[673] *Ibid*., art. 1 II.

[674] Au titre de l'article 6-2 de la loi de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique telle que modifié par la loi visant à lutter contre les contenus haineux sur internet, il s'agit des propos renvoyant à l'apologie des crimes d'atteinte volontaire à la vie ou les atteintes volontaires à l'intégrité de la personne ainsi que les agressions sexuelles, l'apologie « *des crimes de guerre, des crimes contre l'humanité, des crimes en réduction en esclavage ou d'exploitation d'une personne réduite en esclavage ou des crimes et délits de collaborations avec l'ennemi, y compris si ces crimes n'ont pas donné lieu à la condamnation de leurs auteurs* », art. 24 al. 5 de la loi du 29 juillet 1881 sur la liberté de la presse ; la provocation « *à la discrimination, à la haine ou à a violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée* », art. 24 al. 7 ; la provocation à « *la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap ou auront provoqué, à l'égard des mêmes personnes, aux discriminations prévues par les articles 225-2 et 432-7 du code pénal* », art. 24 al. 8 ; la contestation de « *l'existence d'un ou plusieurs crimes contre l'humanité* » ou encore nier, minorer ou banaliser de façon outrancière *« l'existence d'un crime de génocide (…), d'un autre crime contre l'humanité, d'un crime de réduction en esclavage ou d'exploitation d'une personne réduite en esclavage ou d'un crime de guerre* », art. 24 bis ; l'injure commise « *envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée* », art. 33 al. 3 ; l'injure commise « *envers personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap* », art. 33 al. 4 ; le harcèlement sexuel tel que prévu par l'article L 222-33 du code pénal ; « *le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique » ou encore « le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter* » et « *le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou représentation* », art. 227-23 du code pénal ; La provocation « *à des actes de terrorisme ou de faire publiquement l'apologie de ces actes* », art. 421-2-5 du code pénal ; ou lorsque le contenu porte « *sur le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le supporte un message à caractère violent, incitant au terrorisme, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineur à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message* », art. 227-24 du code pénal.

[675] *Ibid.*

[676] Selon l'article 1 al. 10 de la proposition de loi précitée, est considéré comme moteur de recherche les activités fixées à l'article L. 111-7 I 1° du Code de la consommation, *Supra*., n° 269.

auraient été soumises à ces obligations[677]. Compte tenu des millions de contenus qui s'échangent chaque jour sur les plateformes, cette mission ne peut être effectuée exclusivement par des êtres humains. De telles obligations incitent nécessairement ces opérateurs à recourir à de nombreux programmes informatiques permettant d'analyser et d'identifier les contenus manifestement illicites, et ce afin d'éviter une condamnation[678]. La loi indiquait notamment que les procédures et les moyens technologiques mis en œuvre devaient être proportionnés afin « *de garantir le traitement dans les meilleurs délais des notifications reçues et l'examen approprié des contenus notifiés ainsi que de prévenir les risques de retrait injustifié* »[679]. Cette disposition illustre parfaitement une méconnaissance technique du législateur dans la mesure où nous voyons difficilement comment il serait pensable d'attendre d'un algorithme un traitement proportionné de tels contenus, et encore moins qu'il est possible pour ces outils de prévenir des risques de retraits injustifiés. En effet, les algorithmes n'ont nullement la capacité d'étudier le contexte dans lequel certains propos ont pu être tenus puisqu'ils sont dénués de sens commun. A ce titre, dans une porte étroite transmise au Conseil constitutionnel, plusieurs syndicats et associations ont souligné *« qu'un contenu qui pris isolément peut s'analyser comme manifestement illicite, peut tout de même bénéficier de la protection accordée à la liberté d'expression, à l'aune du contexte dans lequel ce contenu a été publié* »[680].

341. Ce ne sont pas les maigres garde-fous prévus par ce texte, tels que la possibilité de contester la suppression d'un contenu devant un juge[681] ou encore le fait qu'il ait été donné compétence au Conseil Supérieur de l'Audiovisuel (CSA) de « *prendre en compte l'application inadéquate par l'opérateur des procédures et des moyens humains et, le cas échéant, technologiques* » afin de prévenir les retraits excessifs[682], qui aurait rassuré. Un observatoire de la haine en ligne, sous l'autorité du CSA, assurait notamment le suivi de l'application de ces obligations[683].

[677] Ce seuil aurait dû être fixé par un décret pris en Conseil d'Etat
[678] Bien que la « surcensure » de ces plateformes puissent également faire l'objet d'une condamnation, le fait pour ces opérateurs de ne pas procéder au retrait des contenus signalés dans les délais imposés par la loi les exposent également à une condamnation. Voir en ce sens art. 7 II de la proposition de loi précitée.
[679] Art. 4 de la proposition de loi visant à lutter contre les contenus haineux sur internet
[680] SYNDICAT DE LA MAGISTRATURE, SYNDICAT DES AVOCATS DE FRANCE, LIGUE DES DROITS DE L'HOMME, AIDES, Contribution extérieure du Syndicat de la magistrature, du Syndicat des avocats de France, de la Ligue des Droits de l'Homme et de AIDES, sur la loi visant à lutter contre les contenus haineux sur internet (affaire n° 2020-801 DC), *syndicat-magistrature.org* [en ligne]. 29 mai 2020, [Consulté le 12 juin 2020]. Disponible à l'adresse : http://www.syndicat-magistrature.org/IMG/pdf/porte_ouverte_loi_avia_saf_sm_aides_ldh-2.pdf
[681] Art. 1 III de la proposition de loi visant à lutter contre les contenus haineux sur internet.
[682] *Ibid*., Art. 7 II.
[683] *Ibid*., Art. 16.

342. Les utilisateurs devaient également être informés de manière « *claire et détaillée, facilement accessible et visible, présentant à leurs utilisateurs les modalités de modération des contenus illicites* »[684], ce qui implique à notre sens une intelligibilité des algorithmes utilisés à leur égard. A ce titre, le CSA avait pour mission de préciser par la voie de délibérations publiques, et dans le respect du secret des affaires, les dispositifs technologiques déployés dans le cadre du retrait des contenus par les plateformes, tout en fournissant par ailleurs des indicateurs chiffrés[685]. Il s'agissait donc pour les utilisateurs d'une transparence s'exerçant *a minima* et essentiellement par un tiers de confiance, alors que l'intervention de ces algorithmes était une volonté de la puissance publique.

343. Nous ne pouvons que contester une fois de plus que des mécanismes de gouvernance prennent le pas sur une régulation d'ordre étatique effectuée par la justice, surtout lorsque certains réseaux sociaux, comme Facebook, n'hésitent pas à instituer une « Cour suprême » des contenus relevant ou non de l'acceptable en fonction des conditions générales d'utilisation de sa plateforme[686]. Le risque étant que Facebook se permette par exemple d'interpréter ce qu'elle entend être un contenu illicite au regard du droit français.

344. Comme a pu le signaler la Commission nationale consultative des droits de l'homme (CNDH) « *c'est au juge, et à lui seul, d'apprécier le caractère abusif de l'exercice de la liberté d'expression* »[687]. Toutefois, force est de constater que dans le cadre de cette proposition, ce n'était finalement pas au juge qu'il revenait d'apprécier les contenus devant être supprimés, mais bien à des algorithmes développés par des acteurs non étatiques pour les raisons que nous avons évoquées. Et quand bien même il serait admissible, dans le cadre d'un autre paradigme, de déléguer l'appréciation de contenus manifestement illicites à des plateformes privées, le législateur semble être assez peu préoccupé par la transparence de ces outils, car seul compte le résultat, à savoir le retrait de ces contenus. En effet, l'article 5 7° du texte prévoyait que les opérateurs rendent compte « *des actions et moyens qu'ils mettent en œuvre et des résultats obtenus dans la lutte et la prévention contre les contenus* » manifestement illicites au CSA, mais sans préciser la nature et le degré de la transparence à réaliser aussi bien auprès de l'Etat que des individus. La CNDH précisait d'ailleurs dans son avis que

[684] *Ibid*., Art. 5.
[685] *Ibid.*
[686] LETTERON R., Facebook crée sa « Cour Suprême », *Liberté, Libertés chéries. Veille juridique sur les droits de l'homme et les libertés publiques* [en ligne]. 9 mai 2020 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://libertescheries.blogspot.com/2020/05/facebook-cree-sa-cour-supreme-rien-que.html
[687] CNDH, Avis relatif à la proposition de loi visant à lutter contre la haine sur internet, 9 juillet 2019.

« *les opérateurs devraient être en mesure de fournir au régulateur leur mode de fonctionnement et d'en expliquer les « choix » a posteriori. Cette exigence d'explicabilité et d'intelligibilité impliquerait d'étendre également les pouvoirs du régulateur à la possibilité de procéder aux audits des algorithmes utilisés par les plateformes en ligne et d'apprécier les moyens humains mis en œuvre par le régulateur pour contrôler le traitement réservé aux résultats issus des systèmes algorithmiques* ».

345. Mais force est de constater que le CSA ne disposerait pas pour l'heure des moyens humains et technologiques pour s'assurer de cette conformité, ne serait-ce car elle n'a pas été instituée initialement pour cela[688], alors que la proposition de loi envisageait que

les « *opérateurs mentionnés aux premier et deuxième alinéas du I de l'article 6-2 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, toutes les informations nécessaires au contrôle des obligations mentionnées à l'article 6-3 de la même loi, y compris l'accès aux principes et méthodes de conception des algorithmes ainsi qu'aux données utilisées par ces algorithmes pour se conformer à ces obligations ;* »[689]

346. Il est intéressant de constater que de nombreux représentants politiques, souvent critiques à l'égard des géants du numérique, y compris pour des raisons de souveraineté numérique, se sont empressés de voter le retrait de contenus par les plateformes en ligne. C'est la force de frappe algorithmique de ces géants, que l'Etat ne détient pas, qui permet de faire appliquer la réglementation, et ce de manière automatisée, afin d'obtenir l'apparente effectivité de cette dernière. Comme nous l'avons déjà abordé, le recours aux traitements algorithmiques est d'apparence séduisant, mais déforme notre tradition juridique[690] et il n'est pas sans heurts du fait des erreurs de traitement ou encore de faux négatifs par exemple sur l'appréciation des contenus qui devraient normalement relever du juge. Il s'agit d'un exemple frappant du fait que les Etats ne se donnent pas les moyens de connaître le fonctionnement de ces algorithmes, qui plus est propriétaires, alors qu'ils conditionnent dans ce cas de figure l'exercice de droits et libertés, comme si seul importait le résultat, à savoir la suppression des contenus, tout en ne s'immisçant pas dans les architectures techniques qui seraient susceptibles d'y parvenir. Bien

[688] *Ibid.*
[689] *Ibid.*, Art. 7 II.
[690] DUCLERCQ J-B., « Les algorithmes en procès », *op. cit.*

que le Conseil constitutionnel ait censuré les propositions abordées[691], dont de tous les mécanismes de transparence des algorithmes qui y étaient associés par voie de conséquence, à l'exception de la création d'un observatoire de la haine en ligne, elles reviennent en partie par l'intermédiaire du droit européen.

b - … au règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne

347. A l'instar des obligations de retrait des contenus terroristes par les plateformes instaurées par le droit national, et précédemment étudiée, la Commission européenne souhaitait que les hébergeurs recourent au déploiement d'outils automatisés afin d'identifier, empêcher la diffusion et supprimer ce type de contenu[692]. Des obligations de vigilance[693] imposaient à ces plateformes en ligne de prévenir la diffusion de tels contenus, ce qui indique une reconnaissance des contenus en amont de leur publication, bien qu'il ne devrait pas s'agir d'une surveillance généralisée même si on imagine difficilement comment cela n'aurait pas été le cas. Ces opérateurs devaient également se soumettre à des injonctions[694] de retrait ou d'en bloquer l'accès sur demande de l'autorité compétente[695], après notification, dans un délai d'une heure. Concernant les signalements des contenus par l'autorité compétente, l'hébergeur aurait dû mettre en place des mesures, y compris techniques, permettant d'évaluer rapidement le contenu, ce qui inclut l'utilisation d'algorithmes[696]. Quant aux mesures proactives, elles comprenaient le filtrage, c'est-à-dire la faculté d'empêcher la publication d'un contenu à caractère terroriste *a priori*, mais également la mise en œuvre d'outils numériques pour « *détecter, d'identifier et de supprimer sans délai les contenus à caractère terroriste, ou de bloquer l'accès à ceux-ci* »[697] ou empêcher leur remise en ligne[698], *a posteriori*.

348. Une fois de plus, la puissance publique ne prend pas part à l'élaboration de ces outils. La seule exigence est que ces algorithmes doivent être efficaces et proportionnés pour ne pas

[691] CC, décision n° 2020-801 DC, 18 juin 2020, *Loi visant à lutter contre les contenus haineux sur internet*.
[692] Proposition de Règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne. Une contribution de la Commission européenne à la réunion des dirigeants à Salzbourg les 19 et 20 septembre 2018 COM/2018/640 final.
[693] *Ibid*., art. 3.
[694] *Ibid*., art. 4.
[695] *Ibid.*, art. 5, « L'autorité compétente ou l'organe compétent de l'Union peut adresser un signalement à un fournisseur de services d'hébergement ».
[696] *Ibid.*
[697] *Ibid.*, art. 6 § 2 (b).
[698] *Ibid.*, art. 6 § 2 (a).

nuire à « *l'importance fondamentale de la liberté d'expression et d'information dans une société ouverte et démocratique* »[699]. De plus, lorsque la plateforme en ligne recourt à des procédés numériques dans le cadre de cette mission, elle prévoit « *des garanties efficaces et adéquates pour assurer l'exactitude et le bien-fondé des décisions prises au sujet de ces contenus, en particulier les décisions relatives à la suppression de contenus considérés comme terroristes ou au blocage de l'accès à ces derniers* »[700], et le cas échéant une intervention humaine lorsque cela est nécessaire afin de procéder à des vérifications[701].

349. Afin d'assurer une certaine transparence de ces outils, dans l'hypothèse où l'opérateur a fait l'objet d'une demande de retrait d'un contenu par l'autorité compétente, il était prévu la transmission d'un rapport dans les trois mois suivant la notification, puis ensuite une fois par an sur les mesures proactives prises, et donc sur la mise en œuvre de la détection et le retrait automatisé[702].

350. Au titre de la transparence de ces outils vis-à-vis de l'utilisateur de la plateforme, leur politique de prévention des contenus à caractère terroriste aurait dû être présentée dans les conditions générales d'utilisation de la plateforme, *« et y joignent, le cas échéant, une explication pertinente du fonctionnement des mesures proactives, y compris le recours à des outils automatisés. »*[703]. Des rapports relatifs à la transparence de la politique de ces outils devaient également être publiés chaque année. Fait intéressant, la proposition précisait le contenu minimal de ce rapport parmi lesquels il aurait été possible de retrouver des explications sur les dispositifs automatisés déployés pour la reconnaissance des contenus, mais aussi les mesures prises par le fournisseur afin de bloquer ou encore de supprimer les contenus.

351. Néanmoins, le règlement (UE) 2021/784 du Parlement européen et du Conseil adopté le 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne ne reprend plus les obligations proactives des hébergeurs, et donc la transparence qui aurait été afférente aux outils déployés pour ce faire. Toutefois, les hébergeurs ne sont nullement empêchés de recourir à des algorithmes pour supprimer de nombreux contenus assimilés au terrorisme, et ce conformément à leur condition générale d'utilisation. La nouvelle règlementation s'est donc finalement cantonnée à assurer une transparence des outils

[699] *Ibid.*
[700] *Ibid.*, art. 9.
[701] *Ibid.*
[702] *Ibid.*, Art. 6 § 2.
[703] *Ibid.*, Art. 8.

automatisés lorsque les fournisseurs de service d'hébergement en utilisent en imposant une « *explication pertinente du fonctionnement des mesures spécifiques, y compris s'il y a lieu, du recours à des outils automatisés* » par l'intermédiaire des conditions générales[704]. Il s'agit d'une transparence limitée pour l'utilisateur qui devrait cependant être plus précise par la publication d'un rapport annuel explicitant le recours à de telles mesures[705].

c - Une transparence générale en construction au plan européen

352. C'est de manière plus générale, comme nous l'avons vu, que la proposition de règlement relatif au marché unique numérique[706] accompagnant un autre projet portant sur le marché intérieur des services numériques[707] est amenée à imposer de nouvelles obligations de transparence des algorithmes et plus largement des traitements. Il s'agit d'un texte ambitieux qui envisage de réguler de manière générale l'intermédiation « *dont le lieu d'établissement ou de résidence se situe dans l'Union, quel que soit le lieu d'établissement des fournisseurs de ces services* »[708]. Les réseaux sociaux sont par exemple concernés et pèsent sur ces plateformes des obligations particulières en fonction des risques. Les fournisseurs devront indiquer les *« mesures et outils utilisés à des fins de modération des contenus, y compris la prise de décision fondée sur des algorithmes et le réexamen par un être humain. Ils sont énoncés clairement et sans ambiguïté et sont publiquement disponibles dans un format facilement accessible* »[709].

353. Des dispositions nommément désignées comme étant relatives à la transparence sont également prévues au sujet des activités de modération. Nous y retrouvons la publication d'au moins un rapport annuel dans des termes clairs et aisément compréhensibles. Devrait par ailleurs figurer dans ce rapport de manière détaillés « *les éventuelles activités de modération de contenu auxquelles ils se sont livrés au cours de la période concernée* », ce qui est amené le cas échéant à renseigner sur les traitements algorithmiques utilisés[710]. En effet, l'article 23 §1 (c) précise que le rapport doit également intégrer des informations sur « *tout recours à des moyens automatisés à des fins de modération de contenus, y compris une spécification des*

[704]Art. 7 § 1 règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.
[705] *Ibid*., § 2 et 3.
[706] Proposition de Règlement n° 2020/0374 du Parlement européen et du Conseil relatif aux marchés numériques (législation sur les marchés numériques) en date du 15 décembre 2020.
[707] Proposition de Règlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, 15 décembre 2020.
[708] *Ibid*., art. 1.
[709] *Ibid*., art. 12 § 1.
[710] *Ibid*., art. 13.

objectifs précis, des indicateurs de la précision des moyens automatisés pour atteindre ces objectifs et des éventuelles mesures de sauvegarde appliquées ». Il s'agit donc d'une transparence cumulative et plus aboutie que celle prévue par le règlement relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

354. Des obligations complémentaires sont prévues pour « les fournisseurs de services d'hébergement, y compris aux plateformes en ligne ». Afin d'appréhender le traitement des signalements de contenus illicites opérés par les utilisateurs, les fournisseurs devront communiquer sur les moyens automatisés permettant de traiter ces demandes, y compris dans l'accusé de réception suivant cette notification[711]. Dans l'hypothèse où un fournisseur retire un contenu ou empêche un utilisateur d'accéder à un service, il a pour obligation d'informer par un « *exposé clair et spécifique* » les motifs. Cette information doit comprendre notamment ce qui est relatif *« à l'utilisation de moyens automatisés pour prendre la décision, y compris lorsque cette dernière concerne des contenus détectés ou repérés par des moyens automatisés* »[712]. Compte tenu de leur caractère systémique, les très grandes plateformes en ligne, c'est-à-dire dont le nombre d'utilisateurs actif est égal ou supérieur à 45 millions[713], devront en plus se soumettre à la tenue d'audit d'indépendant portant y compris sur toutes les obligations de transparence précitées[714]. Enfin, afin de s'assurer de la conformité de ces opérateurs économiques à la réglementation, il est prévu que la Commission puisse, notamment par l'intermédiaire d'experts et d'auditeurs, contrôler sur place le système informatique, les algorithmes ainsi que leurs données[715].

355. Par anticipation du droit européen, et compte tenu de la censure du Conseil constitutionnel des dispositions relatives à la transparence des outils automatisés pour satisfaire les obligations de la proposition de loi visant à lutter contre les contenus haineux sur internet, le législateur national a souhaité intégrer de nouvelles obligations de transparence des outils utilisés par les plateformes en ligne dans la lutte contre les contenus haineux. Telle a été l'ambition de la loi confortant le respect des principes de la République[716]. Au regard des nouvelles obligations de ces opérateurs économiques devant être accomplies[717], y compris par l'intermédiaire de moyens technologiques proportionnés[718], les utilisateurs seront informés de

[711] *Ibid*., art. 14 § 6.
[712] *Ibid*., art. 15 § 2.
[713] *Ibid*., art. 25 § 1.
[714] *Ibid*., art. 28 § 1 a).
[715] *Ibid*., art. 54 § 3 et 57.
[716] Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.
[717] *Ibid*., art 42.
[718] *Ibid*.

manière facilement accessible par le truchement des conditions générales d'utilisation du service les moyens automatisés utilisés à des fins de modération[719]. De la même manière, la personne concernée par le retrait ou l'inaccessibilité d'un contenu se voit notifier par une mention explicite que la décision repose sur un traitement algorithmique[720]. Le recours contre une telle décision ne doit pas quant à lui reposer que sur un moyen automatisé[721].

356. Quant au CSA il se voit confier d'importantes prérogatives de contrôle tel que l'

> « *accès aux principes de fonctionnement des outils automatisés auxquels ils ont recours pour répondre à ces obligations, aux paramètres utilisés par ces outils, aux méthodes et aux données utilisées pour l'évaluation et l'amélioration de leur performance ainsi qu'à toute autre information ou donnée lui permettant d'évaluer leur efficacité, dans le respect des dispositions relatives à la protection des données personnelles. Le conseil peut leur adresser des demandes proportionnées d'accès, par l'intermédiaire d'interfaces de programmation dédiées, à toute donnée pertinente pour évaluer leur efficacité, dans le respect de ces mêmes dispositions. Dans le respect de ces dispositions et aux mêmes fins, il peut mettre en œuvre des méthodes proportionnées de collecte automatisée de données publiquement accessibles afin d'accéder aux données nécessaires, y compris lorsque l'accès à ces données nécessite la connexion à un compte* »[722].

357. La constitutionnalité de ces dispositions n'a toutefois pas été contrôlée par le Conseil constitutionnel[723] dans la mesure où sa saisine ne portait pas sur ces éléments, ce qui aurait pu être l'occasion d'aborder la conciliation de la transparence de ces algorithmes avec les libertés économiques. Nous regrettons par ailleurs que le législateur aussi bien national qu'européen préfère profiter de la puissance algorithmique des géants du numérique pour faire respecter le droit en se contentant simplement d'une transparence des outils utilisés, alors qu'il devrait prendre part à leur conception.

[719] *Ibid*.
[720] *Ibid*.
[721] *Ibid*.
[722] *Ibid*.
[723] CC, décision n° 2021-823 DC, 13 août 2021, *Loi confortant le respect des principes de la République*.

2 - Le droit d'auteur et les droits voisins dans le marché unique numérique

358. La directive sur le droit d'auteur et les droits voisins dans le marché unique numérique[724] comporte une disposition relative à l'immixtion des algorithmes dans la régulation de ces contenus par les hébergeurs. De nombreuses plateformes utilisaient déjà des détections automatisées de contenus contrevenant au droit d'auteur, à l'image de Content ID pour Youtube[725]. L'article 17 de la présente directive repose sur cette philosophie. Le degré de transparence de ces outils numériques n'a pas encore été déterminé, et ce malgré l'ordonnance la transposant en droit national[726]. Il est déjà intéressant de constater, par la voie de la remise d'un rapport du ministère de la Culture, que l'Etat inventorie les méthodes de reconnaissance des contenus afin d'imposer aux plateformes les techniques les plus adéquates[727]. Il est donc à noter que le législateur se soucie davantage de l'architecture technique à retenir afin de parvenir au respect du droit d'auteur qu'à celui de l'exercice de la liberté d'expression. Paradoxalement, une Commission du Parlement européen a récemment eu l'occasion de souligner qu'« *en l'état actuel de la technique, aucune technologie n'est en mesure d'évaluer, selon le niveau requis par la loi, si le contenu qu'un utilisateur souhaite téléverser porte atteinte au droit d'auteur ou relève d'une utilisation légitime* »[728]. Malgré ce constat, l'Union ne souhaite pas imposer aux hébergeurs des moyens techniques particuliers pour parvenir à la conformité des obligations à ladite réglementation.

359. S'agissant du droit privé, les algorithmes ne jouent pas qu'un rôle dans la détection des contenus en ligne, il est également possible de les retrouver dans d'innombrables usages du droit du travail.

---

[724] Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (Texte présentant de l'intérêt pour l'EEE.)

[725] Selon YouTube « *Content ID est un outil (...) développé pour aider les titulaires de droits d'auteur à identifier et à gérer en toute facilité leur contenu sur YouTube. Les vidéos mises en ligne sur YouTube sont comparées à une base de données de fichiers fournis par les propriétaires de contenu. Ce sont eux qui décident de la procédure à suivre lorsqu'une correspondance est établie entre une vidéo mise en ligne sur YouTube et leur propre contenu. Dans ce cas de figure, la vidéo en question fait l'objet d'une revendication Content ID.* », AIDE YOUTUBE, Fonctionnement de Content ID, *Support.google.com* [en ligne]. [Consulté le 12 juin 2020]. Disponible à l'adresse : https://support.google.com/youtube/answer/2797370?hl=fr

[726] Ordonnance n° 2021-580 du 12 mai 2021 portant transposition du 6 de l'article 2 et des articles 17 à 23 de la directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE.

[727] MOCHON, J-P., Rapport, Vers une application effective du droit d'auteur sur les plateformes numériques de partage : Etat de l'art et propositions sur les outils de reconnaissance des contenus, *Site du ministère de la Culture et de la Communication* [en ligne]. 28 novembre 2019 [Consulté le 12 juin 2021]. Disponible à l'adresse : https://www.culture.gouv.fr/content/download/262441/file/Synth%C3%A8se%20Rapport%20CSPLA%20Hadopi%20CNC%20Outils%20de%20reconnaissance.pdf?inLanguage=fre-FR

[728] COMMISSION EUROPEENNE, Orientations relatives à l'article 17 de la directive 2019/790 sur le droit d'auteur dans le marché unique numérique, in *eur-lex.europa.eu* [en ligne]. 04 juin 2021. [Consulté le 21 juin 2021]. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1625142238402&uri=CELEX%3A52021DC0288

B - Transparence des algorithmes en droit social

1 - Les dispositions relatives aux salariés hors cadre des plateformes

360. Indépendamment de la question des plateformes, il serait intéressant que les employeurs aient également pour obligation de signaler le fonctionnement des algorithmes qui ont une incidence sur les travailleurs. Le chronométrage des cadences a été remplacé, dans certaines entreprises, par la modélisation algorithmique du temps de travail, ce qui n'est pas sans conséquence sur le bien-être des travailleurs[729]. Bien que des dispositions déjà existantes, qui n'ont pas été initialement pensées pour le numérique, puissent permettre la communication d'informations au sujet de ces algorithmes, la difficulté réside dans le fait qu'aucun texte ne fixe préalablement la liste précise des documents qui seraient nécessaires à leur compréhension, laissant une marge d'appréciation importante à l'employeur pour ne pas révéler l'étendue du traitement, qui, une fois de plus, ne repose pas toujours sur des données personnelles.

361. Tel est par exemple le cas de La Poste qui utilise un logiciel informatique dénommé « METOD » afin de réaliser la modélisation des tâches à effectuer par les facteurs, alors qu'il a des conséquences sur leurs conditions de travail. Sous l'empire de l'ancien article L. 4614-12 du Code du travail, le Comité d'hygiène, de sécurité et des conditions de travail [730] pouvait recourir à l'expertise, ce qui a été fait, afin d'obtenir la transparence de cet outil de gestion. Pour permettre de recourir à l'expertise, il a été demandé à La Poste de fournir les documents relatifs au fonctionnement dudit logiciel, ce que La Poste n'a pas été capable de communiquer, notamment parce qu'elle n'aurait pas conservé ces informations, la loi ne l'y obligeant pas. Cette affirmation est troublante puisque les logiciels reposent sur des données et des paramétrages qui sont consultables dans le programme. En l'absence de transparence de ces données, il n'est pas possible de savoir pour l'expert si l'outil constitue une menace grave pour les salariés. Par une ordonnance de référé rendue le 13 juin 2017, le TGI de Paris n'a pas hésité à enjoindre La Poste à transmettre une liste de documents limitative au cabinet d'expertise afin de faire toute la lumière sur le fondement du logiciel[731].

362. Les traitements algorithmiques s'immiscent également dans le monde du travail aussi bien dans la phase de recrutement que d'évaluation des salariés, alors qu'ils ne sont pas toujours

[729] En ce sens, voir JOUNIN N., « Le caché de La Poste. La genèse de temps virtuels pour organiser le travail des facteurs », *La revue de l'IRES*, n° 93, 2017, p. 25 à 50.
[730] Remplacé depuis le 1er janvier 2020 par le Comité social et économique (CSE). En ce sens, LOISEAU G., « Le comité social et économique », *Droit social*, 2017, p. 1044.
[731] TGI de Paris, ordonnance de référé du 13 juin 2017, RG 17/51830.

transparents et/ou intelligibles, et parfois ils n'hésitent pas à venir concurrencer le droit du travail[732]. La transparence de ces dispositifs est un enjeu majeur, car ils sont susceptibles de rendre inopérant, du fait de leur opacité, de leur architecture technique ou encore des données qu'ils analysent, des principes comme celui de non-discrimination[733]. Il a par exemple déjà été démontré que Amazon avait un temps fait reposer l'étude des candidatures à un emploi par des algorithmes, aboutissant à des discriminations[734]. C'est la raison pour laquelle ce projet a pour le moment été abandonné. Bien entendu, la transparence des algorithmes ne fera pas disparaître les biais qui émanent également de comportements humains, mais elle permet de s'assurer que ces outils, lorsqu'ils sont déployés, sont conformes au droit aussi bien dans leur conception que lors de leur fonctionnement.

363. Certaines dispositions du Code du travail s'adaptent très bien aux outils algorithmiques. En effet, l'article L. 1221-8 du Code du travail dispose qu'en plus d'être pertinente au regard des finalités poursuivies, « *le candidat à un emploi est expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard* ». Il en va de même après le recrutement, si des méthodes et techniques sont utilisées lors de son évaluation professionnelle[735]. A ce titre, quelles que soient les méthodes et techniques déployées, « *lorsque la notation a pour effet de justifier des différences de traitement c'est à la condition que les critères d'évaluation soient objectifs et transparents.* »[736]. Pour les méthodes et techniques utilisées dans le cadre des candidatures[737] ou de l'évaluation du salarié[738], aucune information concernant la candidature ou un emploi **«** *ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* ». A notre sens, le fait de porter préalablement à connaissance de tels dispositifs permet le cas échéant de pouvoir contester ces outils. C'est donc aussi un devoir de loyauté qui recouvre un enjeu probatoire. En effet, comment serait-il possible de démontrer, et donc de contester l'utilisation d'un algorithme lorsque le salarié ignore son existence ?

---

[732] ROSENBLAT A., *Uberland : How Algorithms are Rewriting the Rules of Work, University of California Press*, 2018, 296 p.
[733] Art. L. 1132-1 du Code du travail.
[734] Il est apparu que ce système discriminait les femmes par rapport aux hommes. LES ÉCHOS, Quand le logiciel de recrutement d'Amazon discrimine les femmes, *Les Echos.fr* [En ligne]. 13 octobre 2018 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.lesechos.fr/industrie-services/conso-distribution/quand-le-logiciel-de-recrutement-damazon-discrimine-les-femmes-141753
[735] Art. L. 1222-4 du Code du travail.
[736] En ce sens, voir TGI Nanterre, 5 sept. 2008 et note de LYON-CAEN A, « L'évaluation des salariés », *Recueil Dalloz*, 2009, p. 1124.
[737] Art. L. 1221-9 du Code du travail.
[738] Art. L. 1222-4 du Code du travail.

364. A cela s'ajoutent naturellement les dispositions relatives à la transparence offertes par le RGPD[739] dans la mesure où ces outils manipulent des données à caractère personnel. Le droit à l'information relatif aux traitements automatisés de données s'applique également en plus des dispositions précitées. A défaut, le fait pour l'employeur de procéder à tout traitement de données à caractère personnel sans avoir respecté ces formalités préalables est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende[740]. Afin de faciliter la mise en œuvre de ces principes, la CNIL a publié le 15 avril 2020 un référentiel relatif à la gestion des ressources humaines[741].

2 - Les travailleurs des plateformes numériques

365. Se pose de plus en plus la question des travailleurs des plateformes numériques, notamment du fait de l'« ubérisation » de la société, c'est-à-dire le recours à une main d'œuvre indépendante et non plus essentiellement salariée. Afin de répondre à cette nouvelle problématique, le législateur est intervenu, y compris pour permettre une meilleure transparence des algorithmes utilisés. C'est en effet d'une part un problème relatif à la loyauté de la plateforme vis-à-vis des travailleurs qui sont captifs de cette dernière, et d'autre part, de transparence, car il convient de considérer que ces travailleurs acceptent d'effectuer des prestations conformes à ce qui est annoncé. La transparence permettrait également de connaître le statut réel du travailleur, en l'occurrence, est-il véritablement indépendant vis-à-vis de la plateforme ? L'algorithme permet-il de refuser des propositions de prestation sans que ce dernier ne le sanctionne par moins de courses à l'avenir ? La façon d'attribuer des commandes constitue-t-il un lien de préposition entre la plateforme et l'indépendant ? Auquel cas il conviendrait de requalifier le contrat.

366. La loi du 24 décembre 2019 d'orientation des mobilités[742] a introduit plusieurs dispositions à cette fin. Ces nouvelles obligations concernent les plateformes d'intermédiation[743] pour les travailleurs indépendants exerçant une activité de « Conduite d'une

[739] Conformément aux articles 12, 13, 14, 15 et 22 du RGPD. Ces dispositions sont traitées dans le premier chapitre de cette thèse, *Supra*., n° 80 et s.
[740] Art. 226-16 du Code pénal.
[741] CNIL, Délibération n° 2019-160 du 21 novembre 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel.
[742] Loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités.
[743] Selon les articles L. 7341-1 du Code du travail et L. 242 bis du Code des impôts. Voir également l'article D. 1326-1 du Code des transports.

voiture de transport avec chauffeur » ainsi que de « Livraison de marchandises au moyen d'un véhicule à deux ou trois roues, motorisé ou non »[744].

367. Ces plateformes *« (…) communiquent aux travailleurs, lorsqu'elles leur proposent une prestation, la distance couverte par cette prestation et le prix minimal garanti dont ils bénéficieront, déduction faite des frais de commission »*[745].

368. Bien que la mise en œuvre de cette obligation d'information soit précisée par décret, cette disposition pose d'une certaine manière la transparence des algorithmes, y compris à des fins de loyauté. L'objectif étant par exemple qu'une course puisse être suffisamment détaillée pour qu'un chauffeur décide ou non de la refuser. Le CNn s'était par ailleurs prononcé en faveur d'une « *une obligation légale d'informer de façon claire et compréhensible les travailleurs du fonctionnement de l'algorithme et des conditions d'utilisations de la plateforme.* **»,** ce qui n'a pas été retenu en ces termes par le législateur[746].

> « *La plateforme mentionnée à l'article L. 1326-1 est tenue de publier sur son site internet, de manière loyale, claire et transparente, des indicateurs relatifs à la durée d'activité et au revenu d'activité au titre des activités des travailleurs en lien avec la plateforme, au cours de l'année civile précédente* »[747].

369. Il est toutefois à noter une immixtion du législateur dans l'architecture technique de la plateforme puisque cette dernière ne doit pas pénaliser le travailleur s'il refuse une proposition de prestation[748]. Mais une fois de plus, il ne s'agit pas d'un contrôle des algorithmes à proprement parler afin de s'assurer que ces obligations seront bien respectées par la plateforme[749]. La preuve est donc bien difficile à apporter pour l'indépendant même si afin de pallier ces difficultés, la Cour de cassation n'hésite plus à requalifier ces relations contractuelles en contrat de travail du fait d'un lien de préposition[750]. Il est alors intéressant de constater que d'autres techniques juridiques, en l'occurrence, la requalification du contrat, permettent

---

[744] Art. L. 1326-1 du Code des transports.
[745] Art. L. 1326-2 du Code des transports. Voir pour plus de précisions, art. D. 1326-2 et D. 1326-3 du Code des transports.
[746] CONSEIL NATIONAL DU NUMERIQUE, Position du CNNum sur les dispositions de la LOM relatives au travail des plateformes, *Cnnumerique.fr* [en ligne], 03 juin 2019, [Consulté le 12 juin 2020]. Disponible à l'adresse : https://cnnumerique.fr/position-du-cnnum-sur-les-dispositions-de-la-lom-relatives-au-travail-des-plateformes
[747] Art. L. 1326-3 du Code des transports. Cette obligation entrera finalement en vigueur le 1er mars 2022. Voir en ce sens, Décret n° 2021-501 du 22 avril 2021 relatif aux indicateurs d'activité des travailleurs ayant recours à des plateformes de mise en relation par voie électronique. Ces indicateurs sont calculés en fonction des critères fixés à l'article R1326-5 du Code des transports « *à partir des données issues de la période qui débute le 1er septembre 2021 et se termine au 31 décembre 2021* ».
[748] Art. L. 1326-3 al. 2 du Code des transports.
[749] Il s'agit de l'Autorité de régulation des transports (ART).
[750] Cour de cassation, 4 mars 2020, chambre sociale, n° 19-13.316.

d'obtenir des résultats probants dans la lutte contre ces algorithmes opaques. Ces plateformes concurrencent le droit parce que l'Etat ne s'est pas doté de la force suffisante dans le domaine du contrôle de la conformité de ces algorithmes à la réglementation. Ce mouvement s'inscrit notamment dans les affirmations du Conseil d'Etat qui s'oppose à la reconnaissance d'un principe de transparence des algorithmes, justifié de prime abord par la complexité de la compréhension de ces derniers, mais surtout parce qu'un tel principe *« nuirait en outre au respect du secret industriel et pourrait potentiellement freiner l'innovation* »[751].

370. Pour aller plus loin, et partant du postulat que les plateformes reposent sur des architectures algorithmiques susceptibles de concurrencer le droit du travail, une proposition de loi relative au statut des travailleurs des plateformes numérique a été déposée le 11 septembre 2019[752], mais elle a été rejetée le 4 juin 2020. Elle prévoyait notamment pour les plateformes une « *l'obligation d'intelligibilité* » des algorithmes. La proposition posait un principe de prise en charge complète par la plateforme des frais permettant d'expertiser lesdits algorithmes. Les représentants des travailleurs auraient également pu solliciter de la documentation en cas de doute sur le changement des algorithmes de la plateforme dès lors qu'ils affectent « *les conditions de travail, l'organisation du travail et des temps d'attente, la modalité de la mise en relation, la modalité et le montant des rémunérations* ». A cette fin, il était question que les représentants des travailleurs sollicitent les services d'un expert sur ces questions à la charge de la plateforme. Comme le souligne Barbara Gomes, les membres du comité social et économique sont soumis au secret professionnel, ce qui aurait pu offrir des garanties à la plateforme tout en permettant d'évaluer des algorithmes ou plutôt les résultats de ces derniers sur l'organisation et la santé au travail[753].

371. Enfin, récemment la même problématique a été soulevée en Italie par le Tribunal de Bologne[754]. Une discrimination indirecte opérée par une plateforme à l'encontre d'un livreur a pu être retenue grâce à une charge de la preuve allégée propre à ce type de procédure par la simple production devant le juge d'éléments factuels par le requérant. Ainsi, le juge a pu retenir par l'intermédiaire des critères de l'algorithme communiqués à la juridiction par la plateforme

[751] CONSEIL D'ETAT, Rapport « Étude annuelle 2017 - Puissance publique et plateformes numériques : accompagner « l'ubérisation » », p. 116, *Conseil-Etat.fr* [en ligne]. 28 septembre 2018 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2017-puissance-publique-et-plateformes-numeriques-accompagner-l-uberisation

[752] SAVOLDELLI P., GAY F., APOURCEAU-POLY C et al., proposition de loi n° 717 relative au statut des travailleurs des plateformes numérique, Sénat, Session extraordinaire de 2018-2019, enregistrée à la Présidence du Sénat le 11 septembre 2019, *Sénat.fr* [en ligne]. 11 septembre 2019 [Consulté le 12 juin 2020]. Disponible à l'adresse : http://www.senat.fr/leg/ppl18-717.html

[753] GOMES B., *Le droit du travail à l'épreuve des plateformes numériques*, thèse soutenue le 3 décembre 2018 à l'Université Paris X Nanterre, p. 138.

[754] Tribunal ordinaire de Bologne (Italie), 27 novembre 2020, RG 2949/2019.

que la participation par un livreur à une grève, aboutissant à ce qu'il n'accepte pas des commandes, avait engendré un classement inférieur de celui-ci par rapport aux livreurs n'ayant pas participer à ce mouvement social[755], était constitutive d'une discrimination indirecte.

PARAGRAPHE 2 - La transparence des outils d'aide à la prise de décision ou de délégation privée

372. En dehors des plateformes numériques les outils d'aide à la prise de décision privée sont de plus en plus nombreux et ont des incidences juridiques sur les personnes et les institutions malgré parfois l'absence de données à caractère personnel. Une transparence de ces outils est déjà saisie par le droit : tout d'abord concernant la justice prédictive et privée (A), mais également en matière médicale (B). Enfin, en contrepartie d'une immixtion toujours plus importante de l'informatique en matière de délégation de conduite des véhicules, un nouveau régime juridique de transparence est apparu, notamment pour assurer la sécurité des personnes (C).

A - Justice prédictive privée et arbitrage

1 - Les algorithmes utilisés dans le cadre de la médiation et l'arbitrage privé

373. Les services en ligne de médiation ou de conciliation[756] ne peuvent reposer sur le seul fondement d'un « *traitement algorithmique ou automatisé de données à caractère personnel* »[757], ce qui n'est pas sans rappeler une symétrie avec l'article 47 de LIL qui dispose qu'« *aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne* ».

[755] Comme l'indique Luca Ratti et Marie Peyronnet au sujet de cette affaire transalpine, « *le juge examine attentivement le fonctionnement de l'algorithme de la plateforme et en particulier le fait que la possibilité pour les livreurs d'accéder au système de réservation des créneaux de travail dépend de deux indices : l'indice de fiabilité, qui mesure le nombre de fois où le livreur ne s'est pas connecté à la plateforme, d'une part l'indice de participation, qui mesure la volonté du livreur de travailler pendant les heures de pointe, d'autre part. De l'analyse du fonctionnement de ces deux indices, le tribunal aboutit au constat que les livreurs qui ne participent pas au travail réservé sans en informer préalablement la plateforme (annulation tardive) se voient attribuer un score (classement) inférieur aux autres livreurs* », RATTI L., PEYRONNET M., « Controverse : algorithmes et risque de discrimination : quel contrôle du juge ? », *Revue de droit du travail*, 2021, p. 81.

[756] Il convient d'entendre par service de médiation et de conciliation, les services définis à l'article L. 21 de la loi n° 95-125 du 8 février 1995 relative à l'organisation des juridictions et à la procédure civile, administrative et pénale.

[757] Art. 4 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

374. Toutefois, lorsque des traitements automatisés interviennent dans le cadre d'un service en ligne de médiation ou de conciliation, le service doit en informer les parties et s'assurer de leur consentement. Concernant la transparence de ces dispositifs, elle est calquée sur le modèle de la transparence du droit des algorithmes publics[758]. L'article 4-3 de la loi programmation 2018-2022 et de réforme pour la justice dispose que

> « *les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par le responsable de traitement à toute partie qui en fait la demande. Le responsable de traitement s'assure de la maîtrise du traitement et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la partie qui en fait la demande la manière dont le traitement a été mis en œuvre à son égard* »[759].

2 - La transparence des outils de justice prédictive développés par des sociétés privées

375. Indépendamment de l'arbitrage, la multiplication des outils d'analyse juridique n'est pas sans poser des interrogations. Ces outils sont essentiellement développés par des sociétés privées qui souhaitent également pouvoir réutiliser les données de justice qui seront prochainement disponibles[760] en *open data*[761] afin de proposer des services de plus en plus pertinents, voire prédictifs pour les professionnels du droit. En ce sens, cette ouverture constituerait également l'apanage du principe de publicité de la justice[762]. Mais cela n'est pas sans risque d'atteinte à la vie privée des parties, mais également du droit au respect à la vie privée des magistrats et des membres du greffe.

376. Le législateur, craignant de voir émerger comme aux Etats-Unis d'Amérique des statistiques précises par juridiction ou par juge ainsi que par type de contentieux, l'article L. 111-13 du Code de l'organisation judiciaire dispose que, « *les données d'identité des magistrats*

---

[758] *Infra.*, n° 435 et s.
[759] Art. 4-3 loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice**.**
[760] Au regard de l'arrêté du 28 avril 2021 pris en application de l'article 9 du décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives, le calendrier de mise en ligne des décisions de justice en open data s'échelonne jusqu'en 2025 en fonction des juridictions et des contentieux
[761] L'*open data* des décisions de justice ne comporte pas que l'ouverture des données, mais également un principe d'utilisation et de réutilisation des données par tout acteur. Voir en ce sens, art. L. 111-13 al. 1er pour les décisions de l'ordre judiciaire et art. 10 al. 2 du Code de Justice administrative et décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives.
[762] PERROUD T., BOURDON P., CLUZEL-METAYER L., RENAUDIE O., « L'open data ou comment accomplir (enfin !) la promesse de publicité de la justice », *Dalloz actualité*, 12 octobre 2020.

et des membres du greffe ne peuvent faire l'objet d'une réutilisation ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées ». Bien que cette disposition soit critiquée par une majorité de la doctrine[763], car elle contreviendrait notamment à la publicité des décisions de justice ou encore par exemple à l'accès au droit, elle a été déclarée conforme à la Constitution dans la mesure où « *le législateur a entendu éviter qu'une telle réutilisation permette, par des traitements de données à caractère personnel, de réaliser un profilage des professionnels de justice à partir des décisions rendues, pouvant conduire à des pressions ou des stratégies de choix de juridiction de nature à altérer le fonctionnement de la justice* »[764]. Ce positionnement, qui heurte des principes du droit, n'est pas si problématique qu'il n'y parait dans la mesure où la loi du papier ne peut pas être dans un certain cas la loi du cyberespace puisqu'il ne s'agit pas que d'une problématique de dématérialisation d'un support physique. Les décisions de justice comportent des données nominatives sur les personnes pouvant paraître anodines sur un format physique, mais lorsqu'elles sont compilées dans des logiciels afin d'en obtenir une analyse à grande échelle, elles constituent un risque majeur pour le droit des personnes, voire pour les institutions, en l'occurrence la bonne administration de la justice.

377. Afin de s'assurer de la conformité de ces outils au respect de la vie privée des professionnels de justice et des parties, le législateur a prévu *« une régulation des algorithmes qui exploitent les données issues de décisions, afin d'assurer une transparence sur les méthodologies mises en œuvre »*[765]. La Cour de cassation, en collaboration avec le Ministère de la Justice, ont lancé un projet permettant de « *développer des techniques d'apprentissage automatique afin d'identifier les données à anonymiser dans les décisions de justice avant de les rendre accessibles et réutilisables* »[766]. L'enjeu est que ce processus ne soit pas effectué sans le moindre contrôle. Quant au Conseil d'Etat, il n'a pour l'heure développé qu'un outil de pseudonymisation des décisions de justice de l'ordre administratif[767].

---

[763] En ce sens, voir notamment PERROUD, T., « L'anonymisation des décisions de justice est-elle constitutionnelle ? Pour la consécration d'un principe fondamental reconnu par les lois de la République de publicité de la justice », in *JP blog* [en ligne]. 11 mars 2019 [Consulté le 12 juin 2020]. Disponible à l'adresse : http://blog.juspoliticum.com/2019/03/11/lanonymisation-des-decisions-de-justice-est-elle-constitutionnelle-pour-la-consecration-dun-principe-fondamental-reconnu-par-les-lois-de-la-republique-de-publicite-de-la-justice/

[764] CC, décision n° 2019-778 DC, 21 mars 2019, Loi de programmation 2018-2022 et de réforme pour la justice, § 93.

[765] Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice**,** rapport annexé.

[766] COUR DE CASSATION, Open justice & L.A.B.E.L. : l'innovation technologique au service de l'anonymisation et de la diffusion de la jurisprudence, *Cour de cassation.fr* [en ligne]. [Consulté le 15 juin 2020]. Disponible à l'adresse : https://www.courdecassation.fr/institution_1/open_data_dematerialisation_7985/open_data_decisions_justice_7821/l.a.b.e.l._innovation_9130/

[767] ETALAB, Guide : comment pseudonymiser des documents grâce à l'IA, *Guides.etalab.gouv.fr* [en ligne]. [Consulté le 15 juin 2020]. Disponible à l'adresse : https://guides.etalab.gouv.fr/pseudonymisation/#a-quoi-sert-ce-guide

378. Le décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives ne semble pas aller dans le sens d'une uniformisation des techniques d'anonymisation des décisions de justice. En effet, il prévoit une occultation minimale obligatoire des noms et prénoms[768], et le cas échéant, si cette occultation est toujours « *de nature à porter atteinte à la sécurité ou au respect de la vie privée des personnes physiques mentionnées au jugement ou de leur entourage* », le Président de la formation du jugement ou le magistrat qui a rendu la décision, peut décider d'occulter d'autres éléments d'identification[769]. Une demande peut par ailleurs être introduite par la personne concernée à cet effet[770]. La CNIL craignait pourtant des disparités entre juridictions, voire entre magistrats, et ce notamment compte tenu d'une absence d'harmonisation des occultations complémentaires[771] alors qu'il aurait été plus judicieux d'instaurer un service public des données de justice afin de tempérer les travers de l'*open data*.

379. Quand bien même ces données seraient anonymisées, il n'en demeure pas moins un risque de ré-identification[772] des parties et des professionnels de justice de la part du réutilisateur de ces décisions. Comme l'indique Lucie Cluzel-Métayer, « *surtout, la possibilité d'établir des liens entre les données anonymisées constitue la principale faiblesse de l'ensemble de ces dispositifs, puisqu'il suffit de croiser les informations pour qu'elles redeviennent identifiantes* », même si l'intégration de techniques d'anonymisation dès la conception permettrait de réduire ce risque[773].

380. Si la démarche de ré-identification d'un réutilisateur aboutirait à un traitement illicite de données à caractère personnel, elle pourrait être irréversible pour certaines parties, même des années après, voire menacerait leur intégrité physique comme cela pourrait être le cas en matière de droit des étrangers. Il serait donc opportun de prévoir une transparence supplémentaire des outils algorithmiques des opérateurs économiques disposant de la capacité technologique d'effectuer de telles opérations ainsi que des logiciels procédant à cette anonymisation comme c'est aujourd'hui le cas sur ce dernier point avec les outils développés

[768] Art. L. 10 du CJA et Art. L. 111-13 du CJO.
[769] Art. R. 741-14 CJA et art. R. 111-12 du CJO.
[770] Art. R. 741-15 CJA et art. R. 111-13 du CJO.
[771] CNIL, Délibération n° 2020-021 du 6 février 2020 portant avis sur un projet de décret relatif à la mise à disposition du public des décisions des juridictions judiciaires et administratives (demande d'avis n° 19022713).
[772] Selon le RGPD, art. 4, 5, il convient d'entendre par pseudonymisation « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ;* »
[773] CLUZEL-METAYER L., « Les limites de l'*open data* », *AJDA*, 2016, p. 102.

par Etalab[774]. Au-delà de la transparence, et à des fins préventives, il pourrait même être envisagé, sur le fondement du risque, de communiquer ces bases de données qu'à des opérateurs économiques agrées par l'Etat[775] pour qu'elles ne soient pas réutilisées à des fins malveillantes. Le rapport de Loic Cadiet évoquait déjà en 2017 à ce sujet que « *les enjeux d'accès à l'information du public débordent le seul cadre de la diffusion des décisions de justice et doivent s'appliquer aux outils qui en assureront l'exploitation* »[776].

B - Les outils d'aide à la prise de décision en matière médicale

381. Bien que les données de santé soient une ressource permettant d'alimenter le progrès scientifique, voire d'améliorer les soins en les personnalisant davantage, il convient cependant d'admettre que la manipulation de ces données sensibles nécessite une attention particulière, y compris dans le domaine de la transparence de ces traitements[777], ne serait-ce pour s'assurer que les garanties prévues par le droit sont bien effectives. Il en va par exemple du droit au secret médical ou encore de principes comme le consentement éclairé aux soins le cas échéant.

382. Dans la droite ligne du rapport de la CNIL[778] visant à garder la main en matière d'algorithmes et d'IA, l'enjeu est d'assurer que les spécialistes eux-mêmes, c'est-à-dire les professionnels de santé, ne perdent pas le contrôle au sujet du fonctionnement de ces algorithmes[779], alors même que ces derniers sont susceptibles de les surpasser dans certains cas.

383. En effet, les traitements algorithmiques sont également de plus en plus utilisés dans le domaine médical. Cette multiplication est rendue possible par l'importante production de données de santé, de leur stockage ainsi que du traitement de ces informations par de puissants

---

[774] Voir en ce sens, GUIDES ETALAB, Pseudonymisation, *github.com* [en ligne]. 06 novembre 2020. [Consulté le 09 juin 2021]. Disponible à l'adresse : https://github.com/etalab/guides.etalab.gouv.fr/tree/master/pseudonymisation

[775] Cet agrément pourrait être octroyés aux *legaltechs* ou aux éditeurs juridiques traditionnels, ainsi qu'aux projets publics d'accessibilité au droit souhaitant mettre en œuvre des techniques d'exploration de ces bases de données anonymisées. Un service public des données de justice pourrait être créé à cette fin.

[776] CADIET L., Rapport remis à Madame la garde des Sceaux, ministre de la Justice, *l'open data* des décisions de justice, mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, 2017, p. 24.

[777] Il est à noter que ces traitements sont appréhendés de manière très large puisqu'ils englobent également la question de la robotique qui sont dans ce domaine considérés comme des dispositifs médicaux. Nous avons toutefois décidé de nous intéresser qu'aux logiciels d'aide à la prise de décision en matière médicale qui nous semblent être aujourd'hui le régime juridique de transparence le plus représentatif en la matière. Voir néanmoins en ce sens, NEVEJANS N., « Les problématiques juridiques et éthiques posées par les robots en santé mentale », *in* TISSERON S., TORDO F (dir.)., *Robots, de nouveaux partenaires de soins psychiques*, *Erès*, 2018, p. 43.

[778] CNIL, ETHIQUE NUMERIQUE, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », *CNIL.fr* [en ligne]. Décembre 2017 [Consulté le 2 juillet 2020]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

[779] NEVEJANS N., « L'influence des logiciels d'aide à la décision sur le processus décisionnel médical à la lumière du droit et de l'éthique », *in* HERVE C., STANTON-JEAN M. (dir.)., *Innovations en santé publique, des données personnelles aux données massives (BIG DATA). Aspects cliniques, juridiques et éthiques*, *Dalloz*, 2018, spec. p. 120 et ss.

calculateurs. Leur multiplication, couplée à une opacité de ces traitements, est par exemple susceptible de renfermer des fraudes. Les techniques d'auto-apprentissages sont par ailleurs un véritable défi, car quand bien même les obstacles juridiques à leurs compréhensions seraient levés, cette transparence est difficilement réalisable techniquement aussi bien du point de vue des données traitées que des algorithmes les traitants.

384. Cette absence de transparence, particulièrement sensible dans ce domaine, ouvre la voie à des vulnérabilités, même si ces méthodes constituent également une meilleure prise en charge du patient dans le diagnostic dans de nombreux cas. Mais la vigilance doit être de rigueur puisqu'à titre d'exemple, un éditeur de logiciel américain a reconnu avoir favorisé les intérêts d'une société pharmaceutique spécialisée dans la filière des opioïdes par un outil d'aide à la prise décision recommandant aux médecins leur prescription[780]. Le risque de vulnérabilité peut alors concerner le patient comme le professionnel de santé qui parfois ne comprend plus le fonctionnement des recommandations. Néanmoins, le régime juridique étudié ne constitue pas une obligation d'information au service du principe de consentement éclairé aux soins puisque le patient ne pourra pas s'opposer au recours des algorithmes par le professionnel de santé[781].

385. Même s'il existait déjà dans le Code de déontologie médicale un devoir général d'information loyale et claire auprès du patient sur les investigations et les soins que le médecin lui propose, notamment en prenant compte de la personnalité afin de s'assurer que les explications soient compréhensibles[782], il convenait toutefois pour le législateur de réagir spécifiquement à la question des outils d'aide à la prise de décision dans ce domaine.

386. En s'inspirant de la LIL et du RGPD[783], conformément à l'étude d'impact[784], le projet de loi relatif à la bioéthique prévoyait dans une de ses versions[785] à l'article 11 qu'aucune décision médicale ne pouvait être prise sur le seul fondement d'un traitement algorithmique. Le recours au programme informatique impliquait donc qu'il ne devait s'agir que d'un outil d'aide

[780] DEPARTMENT OF JUSTICE, Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations, *The United States, Department of Justice* [en ligne]. 27 Janvier 2020 [Consulté le 13 mars 2020]. Disponible à l'adresse : https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0

[781] BEVIERE-BOYER B., « Numérique en santé : le projet de loi relatif à la bioéthique a accouché d'une souris », NEVEJANS N. (dir.), *Données et technologies numériques. Approches juridique, scientifique et éthique*, *mare & martin*, 2021, p. 243.

[782] Art. R. 4127-35 du Code de la santé publique.

[783] Les données de santé sont des données à caractère personnel sensibles qui sont déjà soumises à un régime juridique particulier de transparence prévu par le RGPD, *Supra.*, n° 148 et s.

[784] Projet de loi relatif à la bioéthique, art. 11 « Préserver une garantie humaine dans l'interprétation des résultats », *Assemblée Nationale.fr* [en ligne]. [Consulté le 18 juin 2020]. Disponible à l'adresse : http://www.assemblee-nationale.fr/dyn/15/textes/l15b2187_etude-impact#_Toc14771004

[785] Art. 11 du projet de loi relatif à la bioéthique du texte n° 371 modifié et adopté par le Sénat en deuxième lecture.

à la prise de décision, ce qui ne figure plus dans le texte final. Quel que soit la rédaction, il était assez peu probable que le professionnel de santé vérifie pour chaque situation le bien-fondé de ces recommandations algorithmiques pour les actes à visée « *préventive, de diagnostique ou thérapeutique* ».

387. La nature et le degré de la transparence de l'outil a également fortement évolué au fil des débats parlementaires. La formulation initiale du projet de loi bioéthique était ambiguë quant à l'existence et l'étendue d'un droit à l'information vis-à-vis du patient puisque le professionnel de santé devait communiquer à celui-ci que les résultats de cette utilisation ainsi que les modalités d'action du traitement[786]. Cette situation pouvait s'expliquer par le fait que le gouvernement prévoyait la maitrise de l'outil par le professionnel. Ce dernier était susceptible de modifier le paramétrage du traitement algorithmique tout en bénéficiant d'un accès aux opérations et données utilisées[787], ce qui lui permettait d'agir comme un tiers de confiance le cas échéant vis-à-vis de son patient. A cet égard, le Conseil d'Etat[788] n'a pas cette fois-ci craint pour le secret industriel et commercial de ces logiciels. L'institution, dans son étude relative à la révision de la loi bioéthique[789], s'était déjà prononcé sur la nature de cette transparence et avait qualifié d'insuffisant le fait de communiquer le code source du programme utilisé au médecin et au patient *« parce qu'il ne contribuerait que marginalement à la compréhension par les médecins, et par les patients, des logiques à l'œuvre dans les dispositifs d'intelligence artificielle »*[790], plaidant donc davantage pour cette logique d'intelligibilité.

388. Le Sénat a modifié le texte afin de préciser ce droit à l'information vis-à-vis des patients. Il en résultait que

> « *lorsque, pour des actes à visée préventive, diagnostique ou thérapeutique, le professionnel de santé envisage de recourir à un traitement algorithmique, il en informe préalablement le patient et lui explique sous une forme intelligible la manière dont ce traitement serait mis en œuvre à son égard. Seules l'urgence et l'impossibilité d'informer peuvent y faire obstacle »*[791].

[786] Projet de loi n° 2187 relatif à la bioéthique du 24 juillet 2019, art. 11.
[787] *Ibid.*
[788] CONSEIL D'ETAT, avis sur un projet de loi relatif à la bioéthique, séance du 18 juillet 2019.
[789] CONSEIL D'ETAT, Rapport « Révision de la loi de bioéthique : quelles options pour demain ? », *vie-publique.fr* [en ligne], 7 juillet 2018 [Consulté le 2 juillet 2020]. Disponible à l'adresse : https://www.vie-publique.fr/rapport/37442-revision-de-la-loi-de-bioethique-quelles-options-pour-demain
[790] *Ibid*., p. 206.
[791] Art. 11 du projet de loi relatif à la bioéthique.

389. Après de nombreux désaccords, dont en commission mixte paritaire, la loi n° 2021-1017 du 2 août 2021 a finalement introduit à l'article L. 4001-3 du Code de la santé publique une nouvelle disposition relative à la transparence de ces nouveaux dispositifs médicaux[792]. Même si la mention d'une information par une forme intelligible a été retirée par le législateur, la personne concernée par le traitement reste informée de l'intervention non pas d'un simple traitement algorithmique, mais d'« *un traitement de données algorithmique dont l'apprentissage a été réalisé à partir de données massives* », ce qui vise donc spécifiquement les méthodes d'IA. Le champ d'application de la transparence est donc restreint par rapport à l'ambition initiale.

390. Les professionnels de santé jouent un rôle considérable dans le fonctionnement de ces outils puisque les saisies de données au sein du traitement algorithmique sont effectuées sous son contrôle pour assurer la traçabilité des données de santé traitées du patient par les algorithmes, ainsi que les interprétations qui vont en résulter[793]. Enfin, afin notamment que le personnel de santé ne perde pas la main sur ces outils numériques, il est prévu que les concepteurs de ces logiciels « *s'assurent de la transparence du fonctionnement de l'outil pour ses utilisateurs* »[794]. Bien que cette disposition paraisse de bon sens d'un point de vue juridique, les techniques d'IA sont pour l'heure difficilement compréhensibles, y compris pour les chercheurs, ce qui heurte la réalité technique. Nous comprenons donc difficilement comment la transparence exigée pourrait être effective. C'est en effet tout le paradoxe des techniques d'apprentissage qui sont prometteuses, mais reposent sur de nombreuses données dont l'origine et le paramétrage ont également des incidences considérables sur le résultat sans que nous identifiions parfaitement la cause. Ainsi, en l'état de l'art, l'exigence d'une transparence absolue de ces outils consisterait en réalité à y renoncer. La précision des dispositifs médicaux concernés par ces nouvelles obligations et quant à leurs modalités de mise en œuvre devra faire l'objet d'un arrêté du Ministre chargé de la Santé après un avis de la CNIL et de la HAS[795]. La HAS est compétente pour autoriser et vérifier la conformité les dispositifs médicaux, dont les outils d'aide à la prise de décision[796]. Elle établit également à cette fin des procédures de certification de ces logiciels[797].

[792] Art. L. 4001-3 I du Code de la santé publique.
[793] Art. L. 4001-3 II du Code de la santé publique.
[794] Art. L. 4001- 3 III du Code de la santé publique.
[795] Art. L. 4001- 3 IV du Code de la santé publique.
[796] Art. L. 161-38 et art. 161-39 du Code de la sécurité sociale.
[797] Art. L. 161-38 du Code de la sécurité sociale.

C - La transparence des systèmes de délégation de conduite

391. La directive 2006/42/CE[798] comportait déjà par exemple de manière générale une obligation d'information des fabricants au sujet des machines puisqu'ils doivent constituer une documentation technique à disposition des autorités de contrôle compétentes, et ce afin d'éclairer sur leur fonctionnement. Depuis des décennies les logiciels exercent un rôle de plus en plus significatif dans le domaine de l'aviation notamment à travers le pilotage automatique des appareils, ce qui explique par ailleurs l'existence d'une règlementation sectorielle.

392. Qu'il s'agisse de la certification des aéronefs civils[799] avant leur mise sur le marché ou de leur contrôle de conformité *a posteriori*, il existait déjà un régime juridique à cet égard afin d'assurer la sécurité des personnes[800]. Il en est désormais de même au sujet des aéronefs sans pilote à bord[801] en attendant une règlementation sur le transport fluvial automatisé. Il s'agit ni plus ni moins que d'une automatisation de la prise de décision humaine dont la transparence est surtout au service de la sécurité des personnes.

393. En revanche depuis quelques années ce sont les véhicules terrestres à moteur qui font l'objet d'une attention toute particulière puisque le recours à la délégation de conduite automatisée a été autorisé, ce qui n'est pas sans poser des questions d'ordre éthique[802]. C'est la raison pour laquelle nous avons décidé d'illustrer spécifiquement ce point dans la mesure où le législateur tant européen que national est venu préciser cette avancée technologique en reprenant des techniques juridiques déjà utilisées dans les régimes juridiques précédemment

[798] La directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (refonte). Elle devrait prochainement être abrogée par un règlement actuellement en projet qui prévoit des obligations de transparence particulières des logiciels à des fins de sécurité. Le logiciel est à ce titre considéré comme un composant de sécurité immatériel afin d'assurer la traçabilité de la sécurité des machines. Ainsi, les machines doivent être conçues notamment afin d'être surveillées à distance si elles sont mobiles et autonomes. Concernant le dépôt du dossier technique des machines, le fabricant doit de plus communiquer au régulateur des informations démontrant sa conformité aux nouvelles exigences. Plusieurs techniques juridiques comme l'accès à un registre des données généré par la machine ou encore la communication du code source sont prévus. Voir particulièrement les annexes III et IV de la proposition de règlement n° 2021/0105 du Parlement européen et du Conseil sur les machines et produits connexes en date du 21 avril 2021.

[799] Au niveau européen, l'Agence européenne de la sécurité aérienne est compétente pour certifier les aéronefs. Il en est de même en France par l'intermédiaire de la direction générale de l'aviation civile.

[800] En ce sens voir notamment Règlement 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) no 2111/2005, (CE) no 1008/2008, (UE) no 996/2010, (UE) no 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) no 552/2004 et (CE) no 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) no 3922/91 du Conseil.

[801] Voir notamment Règlement délégué (UE) 2019/945 de la Commission du 12 mars 2019 relatif aux systèmes d'aéronefs sans équipage à bord et aux exploitants, issus de pays tiers, de systèmes d'aéronefs sans équipage à bord.

[802] NEVEJANS N., *in* SIDO B., Rapport d'information n° 570 les robots et la loi du Sénat, session ordinaire 2015-2016, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, enregistré à la Présidence du Sénat le 3 mai 2016, *Senat.fr [en ligne]*. [Consulté le 3 mars 2021]. Disponible à l'adresse : https://www.senat.fr/rap/r15-570/r15-570.html

évoqués[803]. Un nouveau règlement européen[804] régit le contrôle de ces logiciels ainsi que leur autorisation de mise sur le marché. Enfin, très récemment, le législateur français[805] est intervenu afin de les autoriser.

394. Bien qu'une certaine information doive être communiquée au titre du droit de la consommation, cet enjeu de transparence conditionne en réalité la sécurité des personnes mais aussi la responsabilité en cas de dommage. Cette transparence se réalise donc par des dispositions du Code des transports. Ainsi, en tant que consommateur le conducteur se voit seulement communiquer par le professionnel les conditions d'utilisation du système automatisé de conduite intégré au véhicule[806]. Néanmoins, c'est par la voie règlementaire que les modalités de fournitures des informations seront précisées.

395. C'est surtout au regard des autorités de contrôle tant nationales qu'européenne que sera assurée la transparence de ces logiciels puisqu'elles « *exigent des opérateurs économiques qu'ils mettent à leur disposition la documentation, les informations et toute autre spécification technique, y compris l'accès aux logiciels et aux algorithmes, que les autorités jugent nécessaires pour mener leurs activités de surveillance du marché* »[807]. Cette technique juridique n'est pas nouvelle puisque depuis 2020[808], et ce conformément aux dispositions du Code de la route issues de l'affaire du *Dieselgate*[809], une autorité administrative dénommée Service de Surveillance du Marché des Véhicules et des Moteurs (SSMVM) est compétente pour contrôler la conformité des véhicules terrestres à moteur et de leurs composants à la réglementation. Cette autorité est donc également amenée à jouer un rôle significatif dans le contrôle des algorithmes puisqu'elle peut d'ores et déjà effectuer des contrôles sur pièce et accéder, sans que le secret des affaires ne lui soit opposé[810], à toutes les informations nécessaires à ses enquêtes. Cela

[803] *Supra*., n° 392.
[804] Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) no 715/2007 et (CE) no 595/2009 et abrogeant la directive 2007/46/CE.
[805] Loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités.
[806] Art. L. 224-68-1 du Code de la consommation créé par l'ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation.
[807] Art. 8 § 8 du Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) no 715/2007 et (CE) no 595/2009 et abrogeant la directive 2007/46/CE.
[807] Loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités.
[808] Ordonnance n° 2020-701 du 10 juin 2020 relative à la surveillance du marché des véhicules à moteur ; Arrêté du 10 juin 2020 portant création du service à compétence nationale dénommé service de surveillance du marché des véhicules et des moteurs (SSMVM).
[809] *Supra*., n° 31.
[810] Art. L. 329-17 du Code de la route.

inclut l'accès aux systèmes informatiques des constructeurs[811], et le cas échéant l'« *accès aux logiciels, aux données stockées et aux algorithmes et peuvent solliciter l'assistance de l'opérateur économique afin d'être en mesure de les exploiter* »[812].

396. Dans ce nouveau régime juridique, le mandataire du constructeur[813] est par ailleurs soumis à des obligations particulières puisqu'il doit communiquer au régulateur tous les documents permettant d'assurer la conformité du constructeur dont l'accès aux logiciels et algorithmes[814]. Le dépôt du dossier par le constructeur auprès de l'autorité de contrôle comporte également ces éléments[815]. Les services techniques du régulateur peuvent demander des compléments d'information afin de « *développer un niveau de compréhension approprié des systèmes, y compris du processus d'élaboration et du concept des systèmes, ainsi que des fonctions du logiciel et des algorithmes nécessaires aux fins de la vérification de la conformité aux prescriptions du présent règlement, pour prendre une décision concernant les essais requis ou pour en faciliter la réalisation* »[816]. Enfin, à des fins de conformité, l'autorité peut accéder au logiciel et aux algorithmes du véhicule une fois celui-ci réceptionné. Il s'agit de vérifier que le traitement correspond bien aux éléments qui avaient été communiqués lors du dépôt du dossier par le constructeur[817]. En cas d'attaque informatique remettant en cause la sécurité du véhicule, l'autorité de contrôle se voit communiquer par le constructeur ou son mandataire les données techniques « *permettant d'analyser les modalités de ces attaques* »[818].

397. Sans que ne soit exigé le consentement de l'utilisateur du véhicule, lorsque celui-ci dispose d'un moyen de communication, il est prévu un accès aux données « *strictement nécessaires à la détection d'accidents, d'incidents ou de conditions génératrices d'accidents situés dans l'environnement de conduite du véhicule, à l'exclusion des données destinées aux systèmes de communications aux centres d'appels d'urgence* »[819]. Ces données doivent être

[811] Art. L. 329-14 du Code de la route.
[812] Art. L. 329-15 du Code de la route.
[813] Il convient d'entendre par mandataire « *toute personne physique ou morale établie dans l'Union qui est dûment mandatée par le constructeur pour le représenter auprès de l'autorité compétente en matière de réception ou de l'autorité chargée de la surveillance du marché et agir en son nom dans le domaine régi par le présent règlement* », art. 3 § 41 du Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) no 715/2007 et (CE) no 595/2009 et abrogeant la directive 2007/46/CE.
[814] *Ibid*., art. 15 § 1 b).
[815] *Ibid*., art. 25.
[816] *Ibid*., art. 25 § 4.
[817] *Ibid*., art. 31 § 5.
[818] Art. L. 1514- 8 du Code des transports créé par l'ordonnance n° 2021-442 du 14 avril 2021 relative à l'accès aux données des véhicules.
[819] Art. L. 1514- 1 du Code des transports créé par l'ordonnance n° 2021-442 du 14 avril 2021 relative à l'accès aux données des véhicules.

anonymisées et leur accès est assuré par les forces de l'ordre et les gestionnaires d'infrastructures routières[820].

398. Il est intéressant de noter que le constructeur ou son mandataire sont par ailleurs autorisés à accéder aux données du système automatisé pendant qu'il circule afin d'étudier son comportement pour améliorer le cas échéant la sécurité de la délégation de conduite. La transparence du traitement est alors prévue vis-à-vis du constructeur puisque ces systèmes sont amenés à générer des erreurs qui auraient échappé aux concepteurs[821].

399. Enfin, à l'instar d'une boîte noire dans le domaine de l'aviation, si le véhicule est impliqué dans un accident, est prévu l'accès au système d'enregistrement d'état des données de la délégation de conduite[822] par « *les fonctionnaires du corps de commandement et d'encadrement de la police nationale* »[823] ou à des enquêteurs du bureau d'enquêtes sur les accidents de transport terrestres (BEATT)[824], et le cas échéant l'assureur[825].

400. Parallèlement, le Code des transports fixera les règles pour les systèmes de transport routier automatisés qui entreront en vigueur au plus tard le 1er septembre 2022 une fois précisées par la voie réglementaire[826].

CONCLUSION DU CHAPITRE I

401. L'immixtion des algorithmes dans les différentes branches du droit est inévitable en plus d'être théoriquement infinie. Nous assistons donc logiquement en réponse à ce fait juridique à l'émergence d'un droit privé des algorithmes très sectoriel et sans véritable cohérence dans la

[820] *Ibid.*
[821] Art. L.1514-7 du Code des transports.
[822] Conformément à l'article 6 du règlement (UE) 2019/2144 du Parlement européen et du Conseil relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, ces enregistreurs seront par ailleurs installés dans tous les véhicules à moteur. Il est précisé que « *les données qu'ils sont capables d'enregistrer et de mémoriser en ce qui concerne l'intervalle de temps peu avant, pendant et immédiatement après une collision comprennent la vitesse du véhicule, le freinage, la position et l'inclinaison du véhicule sur la route, l'état et le taux d'activation de tous ses systèmes de sécurité, le système eCall embarqué fondé sur le service 112, l'activation des freins et tout autre paramètre d'entrée pertinent des systèmes embarqués de sécurité active et d'évitement des accidents, ces données présentant un haut niveau de précision et leur préservation étant assurée* ».
[823] Art. L. 123-3 du Code de la route créé par l'ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation.
[824] Art. L. 1515- 4 du Code des transports créé par l'ordonnance n° 2021-442 du 14 avril 2021 relative à l'accès aux données des véhicules.
[825] Art. L. 1515-5 du Code des transports créé par l'ordonnance n° 2021-442 du 14 avril 2021 relative à l'accès aux données des véhicules.
[826] Art. 7, ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation.

mise en œuvre de la transparence, alors qu'il s'agit des mêmes technologies. Le droit européen ambitionne néanmoins d'y remédier à travers de nombreuses propositions allant pour certaines dans le bon sens, notamment par l'intermédiaire d'une approche plus générale par les risques[827].

402. Mais l'intervention des algorithmes n'est pas toujours l'œuvre des puissances privées, mais également une volonté de la puissance publique, comme nous l'avons vu avec la régulation de certains contenus. En incitant à certains usages, la puissance publique n'a pas jugé opportun d'instituer des obligations de transparence satisfaisantes, ajoutant de fait une opacité supplémentaire aux algorithmes déjà déployés par les opérateurs économiques.

403. De manière générale, la nature de cette transparence n'est ni du même degré ni de même nature, non pas pour des raisons de conciliations entre divers impératifs qui pourraient l'expliquer, mais parce que le législateur ne dispose pas d'une cohérence dans ce domaine, ce qui engendre une confusion et une pluralité de régimes juridiques. Le plus souvent, la transparence est faible vis-à-vis de l'utilisateur, alors qu'elle est renforcée auprès des autorités de contrôle qui ont la charge de cette régulation. Mais force est de constater qu'en plus d'être trop nombreuses, et donc divisées, ces autorités ne sont ni dotées des moyens humains et techniques suffisants pour jouer un rôle de tiers de confiance efficace.

[827] *Infra*, n° 946 et s.

CHAPITRE II - L'EMERGENCE D'UN DROIT PUBLIC DES ALGORITHMES : LA TRANSPARENCE DES TRAITEMENTS ALGORITHMIQUES

404. Pour reprendre les propos de Jean-François Kerléo, la transparence en droit public constitue une nouvelle culture juridique. Il s'agit d'un ensemble de techniques juridiques, mais ne reposant pas sur une unité conceptuelle[828]. Dans le cadre de ce chapitre nous nous intéresserons cependant à ce qui va concourir à la meilleure compréhension des traitements algorithmiques publics. La transparence étudiée s'inscrit dans l'accomplissement de la démocratie administrative[829] et plus largement de la vie démocratique.

405. Comme nous l'avons vu, la LIL de 1978[830] s'applique aussi bien aux acteurs privés que publics dès lors qu'ils recourent à un traitement automatisé de données à caractère personnel. Or, l'administration recourt de plus en plus à des traitements ne manipulent pas nécessairement que des données personnelles, alors qu'ils peuvent avoir des effets juridiques sur les administrés : tel est le cas par exemple des décisions administratives individuelles fondées sur des traitements algorithmiques. Il était devenu urgent de venir compléter le régime juridique existant afin de prendre en compte ces nouvelles situations. Ce régime juridique encore en construction est intervenu non pas pour limiter l'usage des algorithmes utilisés dans le cadre de l'action administrative, mais afin d'assurer une tentative de transparence de ces derniers (Section 1).

406. Toutefois, les algorithmes ne font pas seulement leur immixtion au sein de l'action administrative puisqu'ils influencent également la vie démocratique, ce qui est susceptible d'avoir des incidences sur les choix politiques et la participation des citoyens. C'est donc par l'intermédiaire du droit dur, et surtout du droit souple, qu'une transparence de ces outils tend à s'opérer (Section 2).

---

828 KERLEO J-F., *La transparence en droit, Recherche sur la formation d'une culture juridique, op. cit.*

829 Comme l'indique Julie Arroyo « *la transparence constitue une condition de réalisation de la démocratie administrative. Sa promotion répond à la crise du système démocratique fondé sur le système représentatif. La légitimité de l'administration apparaît désormais moins fondée sur le principe de séparation des pouvoirs, l'élection et le « mythe » de la représentation reposant sur la concordance des volontés des gouvernés et des gouvernants que sur le pluralisme et le contrôle exercé directement par les citoyens sur le processus politique et administratif. Cette vision renouvelée de la démocratie impose de substituer au modèle administratif classique reposant sur la hiérarchie, le secret et l'assujettissement de l'administré, un modèle d'administration plus ouvert, rééquilibré au profit de l'administré, fondé sur l'information, le dialogue et sa participation. La mise en place de la transparence administrative participe à la réalisation de ces nouvelles exigences démocratiques en assurant l'information des administrés, cette information leur permettant de se livrer à une forme de contrôle du pouvoir ainsi que, dans une certaine mesure, d'y participer.* », ARROYO J., Un droit à l'oubli dans le champ des documents administratifs ?, *op. cit.*

830 *Supra.*, n° 80 et s.

SECTION 1 - TRANSPARENCE ET RECOURS AUX TRAITEMENTS ALGORITHMIQUES DANS LE CADRE DE L'ACTION ADMINISTRATIVE

407. L'administration, dans le cadre de son action, recourt depuis les années soixante-dix[831] aux traitements algorithmiques. Le Conseil d'Etat avait par ailleurs consacré une étude sur les incidences de l'informatique sur les libertés publiques et les décisions administratives individuelles automatisées dès 1970[832]. Les lois de 1978[833] et 1979[834] s'inscrivaient également dans ce mouvement de transparence administrative.

408. Ce phénomène s'est accentué avec la démocratisation de l'informatique, et notamment grâce aux améliorations techniques telles que la vitesse de calcul des ordinateurs ou encore l'amélioration des capacités de stockage des données, ce qui a ouvert la voie à des outils d'aide à la prise de décision algorithmiques de plus en plus performants, mais aussi à la possibilité qu'un traitement automatisé fonde exclusivement une décision administrative individuelle.

409. Certains administrés ne pouvant pas obtenir d'explication auprès de l'administration sur ces traitements, dans la mesure où ces outils ne faisaient pas toujours intervenir de données à caractère personnel, ils n'ont pas eu d'autres choix que de contourner cet angle mort juridique. La liberté d'accès aux documents administratifs est apparue comme une solution naturelle pour obtenir des informations à ce sujet (Paragraphe 1), avant que le législateur ne prenne conscience de cette difficulté, et ne décide enfin d'intervenir en définissant la nature et le degré de transparence des traitements algorithmiques ayant fondés des décisions administratives individuelles (Paragraphe 2).

PARAGRAPHE 1 - Le droit d'accès aux documents administratifs

410. La transparence telle que prévue par le législateur, consiste dans la genèse de la LRN, à s'assurer notamment que les choix politiques ne sont pas remis en cause par cette automatisation, et ce d'autant plus que les programmeurs informatiques ignorent parfois l'état

[831] En effet, comme nous l'avons vu, le projet de « Système automatisé pour les Fichiers Administratifs et le Répertoire des Individus » (SAFARI) datait de 1974. *Supra.*, n° 22.
[832] CONSEIL D'ETAT, Rapport, « Les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives : notes, comptes-rendus d'entretiens, notes manuscrites, projet de plan, projets intermédiaires », 20050574/18, n° 2, *Archives nationales*, 1970.
[833] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.
[834] Loi n° 79-587 du 11 juillet 1979 relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public.

du droit dans les domaines pour lesquels ils sont amenés à créer des logiciels. La consécration de l'étendue de l'accès à ces documents administratifs permet de s'assurer que l'administration n'utilise pas des traitements automatisés illégaux, qu'elle n'est d'ailleurs pas toujours à même de comprendre au regard de la complexité de certaines opérations. C'est donc par la voie de la liberté d'accès aux documents administratifs que la transparence a été amenée à s'opérer dans un premier temps.

411. Bien qu'il existe des efforts allant dans le sens d'une meilleure transparence des traitements algorithmiques utilisés par l'administration, il n'existe cependant pas un véritable principe juridique de transparence en droit administratif[835]. Ce que nous appelons transparence, c'est-à-dire toute action contribuant à comprendre le fonctionnement des algorithmes, repose sur des principes juridiques différents. Cette transparence n'est de plus pas absolue et se heurte à bien des exceptions. Nous ne traiterons pas de la question des conditions de la réutilisation des codes sources, car nous focalisons notre réflexion sur les dispositifs permettant de s'assurer que les traitements algorithmiques sont conformes au droit positif.

412. Le code source est en quelque sorte l'ADN du programme informatique. Sa connaissance permet de connaître par exemple quels sont les critères ou encore les calculs qu'il mettent en œuvre. L'enjeu a été dans un premier temps de savoir si le code source pouvait être assimilable à un document administratif communicable afin qu'il soit étudié (A). Cependant, lorsqu'il est communiqué par l'administration, sa compréhension demeure technique et difficile dans certains cas, y compris pour des raisons juridiques (B).

A - Le code source : un document administratif communicable

413. Les dispositions relatives à la liberté d'accès aux documents administratifs sont des « *garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* »[836] et il ne paraissait pas illogique que les codes sources des logiciels deviennent communicables, même dans l'hypothèse où ces traitements n'ont pas d'effets juridiques sur les tiers, parce qu'ils seraient exclusifs à une mission de service public. A ce titre, toute personne, qu'elle soit physique ou morale, peut demander la communication d'un tel code source, et ce indifféremment de ses prétentions[837].

[835] GRABIAS F., « La transparence administrative, un nouveau principe ? », *La Semaine Juridique Administrations et Collectivités territoriales*, n° 50, 17 décembre 2018, p. 2340.
[836] CE, 29 avril 2002, *Ulmann*, req. n° 228830.
[837] Art. L. 300-1 du CRPA.

414. En premier lieu, la transparence va trouver sa source dans la liberté de communication des documents administratifs. En l'occurrence, grâce à la reconnaissance par la CADA du code source comme document administratif communicable. La CADA définit le code source comme étant « *un ensemble de fichiers informatiques qui contient les instructions devant être exécutées par un micro-processeur* »[838]. Il s'agit donc de l'algorithme ou des algorithmes implantés dans un langage de programmation permettant à ordinateur de l'exécuter.

415. Le législateur a entériné[839] un mouvement que la CADA avait déjà opéré à travers plusieurs affaires relatives à une demande de communication du code source d'un logiciel. Dans une première affaire, un enseignant-chercheur avait demandé à la Direction générale des finances publiques, la transmission du code source du logiciel permettant le calcul de l'impôt sur les revenus des personnes physiques afin de pouvoir le réutiliser dans le cadre de ses recherches[840]. En effet, pour la CADA, la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, est suffisamment générale pour permettre la communication des codes sources[841]. Cet exercice interprétatif ne fut donc pas difficile à réaliser de la part de la CADA. La communication des codes sources utilisés par l'administration, dans le cadre d'une mission de service public, se fonde donc sur le régime juridique de la liberté d'accès aux documents administratifs.

416. Puis, dans une autre affaire bien plus polémique, une association de lycéens demandait à ce que l'éducation nationale lui communique le code source de la plateforme *APB* relatif à la préinscription des lycéens dans les établissements de l'enseignement supérieur[842]. L'association arguait que l'algorithme avait notamment pour finalité le tirage au sort des lycéens souhaitant intégrer des filières dont les demandes excèdent les capacités d'accueil. Elle accusait le programme de procéder à cette sélection. A défaut d'obtenir la communication de ce document, il n'était pas possible de lever l'opacité qui entoure cet algorithme. La CADA avait émis un avis favorable à ce que ces documents administratifs soient communiqués aux intéressés. Il est intéressant de constater que cette affaire a permis de mettre en exergue le fait que la communication des codes sources est devenue un enjeu majeur d'intelligibilité des algorithmes. En effet, dans ce cas de figure, n'était plus en jeu la volonté initiale des demandeurs, qui

[838] CADA, avis n° 20161989 du 23 juin 2016.
[839] Art. L. 300-2 du CRPA.
[840] CADA, avis n° 20144578 du 8 janvier 2015.
[841] *Ibid.*, et rappelé par la CADA dans son conseil n° 20155079 du 19 novembre 2015.
[842] CADA, avis n° 20161989 du 23 juin 2016.

consistaient à pouvoir réutiliser un logiciel utilisé par l'administration, mais bien de comprendre la motivation des décisions administratives individuelles s'imposant aux lycéens.

417. Les codes sources sont désormais communicables dans les mêmes conditions que les autres documents administratifs[843]. Cette doctrine de la CADA a été entérinée par le juge administratif dans un jugement du Tribunal administratif de Paris le 10 mars 2016[844], puis par le législateur en 2016 par l'intermédiaire de la LRN[845] en ajoutant les codes sources à la liste des documents administratifs communicables[846], y compris par défaut dans leur version actualisée[847]. L'obligation de mise en ligne par défaut des codes sources, c'est-à-dire sans qu'une demande ne soit adressée par un administré, ne concerne que les administrations[848] d'au moins cinquante agents ou salariés équivalents temps plein[849], dont les collectivités territoriales d'au moins 3 500 habitants. A l'instar de toute communication effectuée sous former électronique, le document doit être mis à disposition « *dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé* »[850].

418. Bien que la liberté d'accès aux documents administratifs porte sur *« les documents produits ou reçus, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission »*[851], il ne s'agit pas d'un droit absolu.

419. Conformément au régime juridique général de la communication des documents administratifs[852], ne peuvent toutefois pas être transmis tous les codes sources utilisés dans le cadre de l'action administrative. Ne sont donc pas communicables les documents qui ne seraient pas achevés, ni les documents préparatoires[853]. Les codes sources non achevés ne pourront donc faire l'objet de cette communication.

420. En outre, dans l'hypothèse où les codes sources comportent des données à caractère personnel, le CRPA précise qu'ils

[843] Voir CRPA, Livre III.
[844] TA de Paris, 10 mars 2016, M. X, n° 1508951.
[845] Loi n ° 2016-1321 du 7 octobre 2016 pour une République numérique.
[846] Art. L. 300-2 du CRPA.
[847] Art. L. 312-1-1 du CRPA.
[848] Est considérée comme administration toute personne morale dont la mission de service public effectuée par l'Etat, les collectivités territoriales, « *ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission* ». Voir en ce sens, art. L. 300-2 du CRPA.
[849] Art. D. 312-1-1-1 du CRPA.
[850] Art. L. 300-4 du CRPA.
[851] *Ibid*.
[852] Voir CRPA, Livre III.
[853] Art. L. 311-2 du CRPA.

« […] ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement permettant de rendre impossible l'identification de ces personnes. Une liste des catégories de documents pouvant être rendus publics sans avoir fait l'objet du traitement susmentionné est fixée par décret pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés » [854].

421. Toutefois, toute personne ne pourra pas se voir transmettre les codes sources dans les hypothèses où la communication porte atteinte au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif, au secret de la défense nationale, à la conduite de la politique extérieure de la France, à la sureté de l'Etat, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations, à la monnaie ou au crédit public, au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente, à la recherche et à la prévention, par les services compétents, d'infractions de toute nature, ou sous réserve de l'article L. 124-4 du Code de l'environnement, et aux autres secrets protégés par la loi[855]. Il en va de même si la communication va à l'encontre des droits de propriété littéraire et artistique[856], à la vie privée, au secret médical ou encore au secret des affaires[857].

422. Or, comme nous l'avons rappelé, l'enjeu de la communication du code source n'est pas uniquement l'éventualité de la réutilisation du logiciel utilisé par l'administration, mais également de s'assurer que ces outils sont conformes aux obligations législatives et réglementaires. Par conséquent, sous couvert du secret de la défense nationale, ne pourra pas être divulgué le code source des programmes mis en œuvre dans le cadre de la loi renseignement qui est destiné par exemple à détecter les connexions susceptibles de révéler une menace terroriste. En la matière, il conviendra donc de se contenter de la CNCTR, qui est garante de la bonne mise en œuvre des techniques de surveillances, y compris lorsqu'elles sont réalisées numériquement[858].

---

[854] Art. L. 312-1-2 du CRPA.
[855] Art. L. 311-5 du CRPA.
[856] Art. L. 311-4 du CRPA.
[857] En effet, dans l'hypothèse où la demande d'accès au document administratif porte sur la vie privée, le secret médical ou le secret des affaires, ils ne sont communicables qu'aux intéressés. En ce sens, voir art. L. 311-6 1° du CRPA. Concernant le secret des affaires, pour plus de précisions, DOUVILLE T., « Parcoursup et le secret des algorithmes », *Dalloz IP/IT*, 2019, p. 700. Lire également à ce sujet, DOUVILLE T., « Parcoursup à l'épreuve de la transparence des algorithmes », *Dalloz IP/IT*, 2019, p. 390.
[858] Nous nous intéresserons spécifiquement à cette question dans la seconde partie de cette thèse, *Infra*., n° 707 et s.

423. Selon la doctrine de la CADA, le fait que la communication d'un code source se heurte à sa non-réutilisation en raison de difficultés techniques, voire à une impossibilité purement matérielle, ne peut justifier un refus[859]. Le code source « *doit être communiqué, au choix du demandeur et dans la limite des possibilités techniques de l'administration, par la délivrance d'une copie sur un support compatible avec celui qu'elle utilise, aux frais du demandeur, ou par courrier électronique et sans frais* »[860].

424. Enfin, sont communicables les documents administratifs qui s'inscrivent dans un processus décisionnel à la condition qu'ils aient perdu leur caractère préparatoire[861]. La diffusion du code source peut également être différée le temps que soit occulté, pour des raisons techniques, du code « *les mentions qui portent atteinte à la sécurité des systèmes d'informations* »[862]. Ainsi, afin de lutter contre la pandémie de SARS-COV-2 de nombreux traitements et applications ont été développés à cette fin[863]. Dans ce cadre, la mise en ligne du code source de ces programmes a nécessité des occultations afin d'assurer la sécurité de ces systèmes, empêchant la compréhension globale de ces derniers[864]. Par ailleurs, l'actualisation de la publication de ces codes a parfois eu lieu plusieurs mois après leur entrée en fonctionnement, ce qui a nui au contrôle effectif de ces outils par la société civile notamment.

425. Ce régime juridique est inadapté faute d'AAI susceptible de vérifier sur pièce l'existence des documents administratifs et leur véracité, excepté la présence d'un traitement automatisé de données à caractère personnel[865]. Se pose donc naturellement la question d'un administré qui soupçonnerait un traitement automatisé de données sans preuve, comme ce fut le cas au lancement de la plateforme *APB*. Il n'était pas possible de démontrer le recours à un tel traitement alors que la suspicion a par la suite été confirmée. Saisie d'une demande d'accès au code source d'*APB* le 23 juin 2016 à la suite d'un refus de l'administration, la CADA avait émis un avis favorable à la communication *« des documents sollicités s'ils existent »*[866]. Fort heureusement, la CNIL, lors d'un contrôle sur pièce, a pu constater l'ampleur et les critères du traitement[867]. Mais dans l'hypothèse d'un traitement algorithmique fondant une décision

[859] CADA, avis n° 20144578 du 8 janvier 2015.
[860] CADA, avis n° 20161989 du 23 juin 2016.
[861] En ce sens, CADA, avis n° 20180276 du 19 avril 2018.
[862] CADA, avis n° 20182682 du 6 septembre 2018.
[863] CLUZEL-METAYER L., « La datasurveillance de la Covid-19 », *op. cit.*, p. 918.
[864] Pour plus de précisions à ce sujet, *Infra*., n° 842.
[865] En effet, concernant les traitements de données à caractère personnel, la CNIL peut agir en tant qu'autorité de contrôle : art. 19 de la Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*.
[866] CADA, avis n° 20161989 du 23 juin 2016.
[867] CNIL, déc. n° MED-2017-053 du 30 août 2017 *mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation.*

administrative individuelle ne portant pas sur des données à caractère personnel, l'administration pourrait tout à fait faire le choix de ne pas reconnaître l'existence d'une telle documentation, ce qui met en exergue les carences en matière de contrôle de la CADA.

B - La difficile compréhension des codes sources

1 - L'absence de documentation afférente et l'exigence d'un public averti à la compréhension

426. Bien que le code source soit pour la grande majorité des personnes inintelligible faute de connaissance technique, il n'en demeure pas moins que même pour un spécialiste, la communication du code source, dans certaines conditions, est insuffisante à sa compréhension.

427. Comme nous l'avons vu précédemment, la doctrine de la CADA, qui a été depuis codifiée dans le CRPA, assimile les codes sources à des documents administratifs communicables. Toutefois, la communication d'un code source ne se suffit pas à lui-même pour le comprendre. Certes, en fonction du langage informatique utilisé, il est possible d'identifier des éléments communs à ce langage, ce qui permet d'identifier certaines logiques. Mais la compréhension du logiciel sans la documentation afférente à son élaboration, à son explication, ne peut être atteinte. Afin de connaître la documentation associée au code source, il est nécessaire de faire une demande spécifique à cette communication. La simple demande de la communication d'un code source n'entraîne pas *de facto* la communication de la documentation permettant de comprendre le fonctionnement dudit programme. Nous nous heurtons donc à des contraintes supplémentaires, à savoir qu'en plus des exceptions qui existent déjà à la communication du code source[868], la documentation peut très bien ne pas être communiquées à cause des secrets protégés par la loi tels que vus précédemment, ce qui rendrait la compréhension du code source difficile, voire impossible.

428. Dans le cadre d'une demande adressée à la CADA[869], un requérant demandait à ce que soient communiqués les codes sources et la documentation afférente d'un logiciel dont l'objet est de simuler certains projets de réforme. La demande portait sur tous les documents accompagnant le code source tels que « *les documentations, les calibrations, les scénarios prospectifs simulés* » et « *les évaluations de réformes ex ante et ex post* ». Pour le Ministère, la

[868] *Supra.*, n° 421.
[869] CADA, avis n° 20180276 du 19 avril 2018.

communication de ces documents, à l'exception des codes sources, « *porte atteinte au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif* ». La CADA a toutefois émis un avis favorable sur ce point dans la mesure où les documents s'inscrivant dans un processus décisionnel sous réserve qu'ils aient perdu leur caractère préparatoire et qu'ils n'ont pas déjà fait l'objet d'une diffusion publique. Sur ce point, nous estimons que la doctrine de la CADA n'est pas adaptée. En effet, lorsque le code source a déjà fait l'objet d'une diffusion publique, il n'est pas possible d'obtenir par cette voie la communication d'un code source. Cela est tout à fait compréhensible dans le cadre d'une demande de communication d'un document papier. Mais dans l'hypothèse d'un code source, il conviendrait de présumer qu'entre la publication du code source et une nouvelle demande, le code source a évolué dans la mesure où, par nature, l'intérêt d'un programme est qu'il évolue au fil du temps. En refusant d'émettre un avis favorable dans une telle situation, c'est prendre le risque de se retrouver avec une version du code source mise en ligne désuète, voire qui ne s'applique plus dans les faits. D'où la nécessité également que les dispositions de la mise en ligne des traitements algorithmiques mis en œuvre par l'administration s'appliquent strictement conformément aux dispositions L. 312-1-3 du CRPA. L'autre difficulté soulevée par cette affaire est que l'un des codes source a dû être converti dans un format libre parce qu'il a été programmé dans un langage propriétaire[870]. Lors de la conversion, des erreurs ont pu très bien intervenir. Il est impératif d'éviter que l'administré se retrouve avec des codes sources modifiés ne correspondant pas à la réalité du traitement.

429. Toutefois, ces documents ne sont pas communicables parce que soumis au secret des délibérations, dans les hypothèses où ils s'inscrivent dans un processus décisionnel indissociable d'une initiative politique du Gouvernement. Les codes sources ont finalement été diffusés publiquement sur le site internet de la Direction générale du Trésor le 5 septembre 2018[871], mais la documentation s'y afférant, comme l'avait prévu le Gouvernement, n'a pas été communiquée, ce qui rend la compréhension des codes sources difficile[872]. Tel a également le

[870] En effet, la programmation s'effectue possiblement dans une multitude de langages informatiques. Nombreux de ces langages sont propriétaires. Ainsi, l'un des codes sources publié par le ministère était en langage TROLL, ce qui nécessite l'achat d'une licence pour toute personne souhaitant étudier ce dernier. Voir en ce sens, BERNE X., Sous pression, Bercy ouvre les codes sources des modèles Mésange, Opale et Saphir, *Next-Impact* [en ligne]. 06 septembre 2018 [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.nextinpact.com/news/107001-sous-pression-bercy-ouvre-codes-sources-modeles-mesange-opale-et-saphir.htm

[871] TRESOR DIRECTION GENERALE, La DG Trésor met à la disposition du public les codes sources des modèles Mésange, Opale et Saphir, *Trésor-Info [en ligne]*. 5 septembre 2018 [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.tresor.economie.gouv.fr/Articles/2018/09/05/la-dg-tresor-met-a-la-disposition-du-public-les-codes-sources-des-modeles-mesange-opale-et-saphir

[872] BERNE X., Sous pression, Bercy ouvre les codes sources des modèles Mésange, Opale et Saphir, *op. cit.*

cas de l'ancêtre de *Parcoursup*, le logiciel *APB*. Ce dernier avait été communiqué de manière incomplète et sans documentation[873]. Fort heureusement, le code source national de la plateforme *Parcoursup* a quant à lui été publié avec la documentation nécessaire par le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation (MESRI). Le communiqué de presse du Ministère précise d'ailleurs que « *la publication du code permettra à chacun de vérifier que le fonctionnement de la plateforme est conforme au droit* »[874]. Indépendamment de la question de la non-communication des algorithmes dits « locaux » de *Parcoursup*, cet épisode démontre que la transparence de ces logiciels est avant tout une volonté politique, et ne repose aucunement sur la doctrine de la CADA ou des Tribunaux administratifs, qui s'accommodent de la communication de code source parcellaire et/ou sans documentation permettant de les comprendre. Cette logique illustre que la communication de ces documents a été rattachée à un régime juridique pensé que pour le papier ou sa dématérialisation, sans prendre en compte les spécificités de l'environnement numérique.

430. L'absence de documentation s'y afférant pour les expliquer, les rend le plus souvent inintelligible, et nuance la portée d'un tel régime juridique. La transparence ne peut se limiter à la question des codes sources. Car la communication d'un document en langue française peut-être, par nature, compris par tous, ce qui n'est pas le cas des langages informatiques.

431. Pourtant, la transparence des codes informatiques, bien que peu compréhensible par la plupart des personnes, est précieuse, dans la mesure où elle permet à des associations ou à des personnes compétentes de les étudier. C'est une garantie collective de la bonne conformité de ces systèmes au droit, mais à la condition que les codes sources communiqués soient ceux qui sont réellement en fonctionnement. Elle permet également d'inclure ces éléments dans le débat public, voire de les améliorer. Nous aborderons toutefois ces points que dans la seconde partie de cette thèse[875].

[873] GRAVELEAU S., APB : les questions que soulève le code source, *Le Monde* [en ligne]. 25 octobre 2016, mis à jour le 25 octobre 2016. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.lemonde.fr/campus/article/2016/10/25/apb-les-questions-que-souleve-le-code-source_5020076_4401467.html

[874] VIDAL F., Parcoursup, la plateforme d'admission dans l'enseignement supérieur, *Site du ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation* [en ligne]. 21 mai 2018 [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.enseignementsup-recherche.gouv.fr/cid130453/parcoursup-publication-du-code-informatique-des-algorithmes.html

[875] *Infra.*, n° 791 et s.

2 - Le code informatique et absence de communication des données d'apprentissage utilisées par les algorithmes

432. Bien que la LRN ait clarifié le régime juridique de la communication des codes sources, il n'en demeure pas moins que ce régime est insuffisant, et reste muet quant à la question des données d'apprentissage[876]. Si nous reprenons la définition donnée par le Conseil Constitutionnel, les algorithmes auto-apprenants sont les algorithmes susceptibles de réviser les règles par eux-mêmes en fonction des données qu'ils analysent[877]. Ils ont donc la particularité de s'émanciper des critères initialement déterminés par les concepteurs du programme. Pour les algorithmes non soumis aux secrets protégés par la loi, l'intérêt est de connaître les données sur lesquelles se fondent les algorithmes auto-apprenants ou faisant intervenir d'autres techniques d'IA. Cette approche est primordiale pour s'efforcer à comprendre les résultats de ces algorithmes qui peuvent, comme nous le verrons, être utilisés comme aide à la prise de décision publique, voire fonder exclusivement des décisions administratives individuelles[878]. Nous ne pouvons que recommander qu'une demande de communication d'un code informatique, sous réserve des secrets protégés par la loi, devrait emporter automatiquement la communication des données d'apprentissage.

433. Il peut exister des hypothèses dans lesquelles le code source serait public, alors que les données d'apprentissage ne le seraient pas, et ce quand bien même les données proviendraient initialement de l'*open data*. En effet, si ces données ont été retravaillées, notamment par un tiers, des droits de propriété intellectuelle sont susceptibles de s'appliquer à ces bases de données. Ainsi, sans connaissance des paramétrages de ces données, le code informatique est un élément insuffisant à la compréhension global d'un tel outil. Compte tenu de l'usage de ces outils, et de leur absence de communication d'informations précises à ce sujet pour les rendre plus intelligibles pour des raisons juridiques, il conviendrait de les exclure pour les cas où ils exerceraient une incidence trop importante sur les personnes, voire la société[879].

434. La communication des codes informatiques, bien qu'incomplète, est une nécessité. Mais les secrets protégés par la loi empêchent une transparence juridique de ces systèmes. Et lorsque cette transparence a lieu, elle n'est pas intelligible pour les administrés. La LRN a donc pris en compte ce phénomène en prévoyant des obligations supplémentaires d'explicabilité des

[876] BOURCIER D., DE FILIPPI P., « Transparence des algorithmes face à l'Open Data : Quel statut pour les données d'apprentissage ? », *Revue française d'administration publique*, 2018, p. 525.
[877] CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*.
[878] *Infra*., n° 439 et s.
[879] *Infra*., n° 959 et s.

traitements algorithmiques incombant à l'administration, notamment parce que les décisions administratives individuelles prises sur le fondement de traitement algorithmique s'imposent sans le consentement des intéressés[880].

PARAGRAPHE 2 - La communication des principales caractéristiques et les règles définissant un traitement algorithmique ayant fondé une décision administrative individuelle

435. Force est de constater que l'administration recourt de plus en plus aux algorithmes pour fonder des décisions administratives individuelles (A). Devant cet état de fait, le législateur n'a pas eu d'autres choix que d'imposer de nouvelles règles de transparence (B). Mais il s'avère que des exceptions et de nombreuses autres limites viennent mettre à mal ce nouveau régime juridique (C).

436. Même si aucune décision administrative ne pouvait être prise « *sur le seul fondement d'un traitement automatisé de donnée* », comme le rappelait le Conseil d'Etat dans son avis sur le projet de la LRN[881], puisque tout traitement automatisé devait faire intervenir un humain dans le processus[882], le législateur a su profiter de l'adoption du RGPD et des marges de manœuvre substantielle qui lui ont été laissées[883], pour autoriser l'administration à recourir à des décisions administratives individuelles exclusivement fondées sur un traitement algorithmique.

A - Le recours aux traitements algorithmiques

1 - Les décisions administratives individuelles fondées sur un traitement algorithmique

437. Comme nous l'avons vu[884], il est important de rappeler que l'article 10 de la LIL de 1978[885] disposait qu'« *aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité* ». Toutefois,

[880] DUCLERCQ J-B., « Le droit public à l'ère des algorithmes », *RDP*, 2017, p. 1401.
[881] CE, avis n° 390741 sur le projet de loi pour une République numérique, 3 décembre 2015, § 24.
[882] Loi n° 78-17 du 6 janvier 1978 préc. modifiée par la loi n° 2004-801 du 6 août 2004, art. 10.
[883] CLUZEL-METAYER L., DEBAETS E., « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA*, 2018, p. 1101.
[884] *Supra.*, n° 148.
[885] Loi n° 78-17 du 6 janvier 1978 préc. modifiée par la loi n° 2004-801 du 6 août 2004, art. 10.

conformément à la même disposition de la LIL, des décisions administratives individuelles pouvaient être prises sur le fondement d'un traitement algorithmique dès lors qu'il existe une intervention humaine[886]. C'est notamment pour cette raison que le MESRI avait été mis en demeure par la CNIL[887] au sujet de la plateforme *APB,* ce qui aboutit à son remplacement par une autre plateforme, *Parcoursup*.

438. En 2015, le gouvernement est confronté à une défiance entourant la plateforme APB. Il prend conscience de l'enjeu d'un droit à l'explicabilité des décisions administratives individuelles prises sur le fondement d'un traitement algorithmique. Selon l'étude d'impact de la LRN, « *de nombreux programmes utilisant des traitements algorithmiques traitent des données qui ne sont pas toujours à caractère personnel, et qui – sans constituer l'unique fondement d'une décision – fournissent des éléments sur lesquels s'appuie la restitution finale des résultats du traitement* »[888]. Il s'agit donc d'un régime juridique qui se superpose aux dispositions prévues par la LIL et profite notamment aux personnes morales faisant l'objet de telles décisions.

2 - Les décisions administratives individuelles exclusivement automatisées

439. Il convient de dissocier les décisions administratives individuelles fondées sur un traitement algorithmique des décisions de même nature qui seraient exclusivement automatisées puisque les dernières ne font jamais l'objet d'une intervention humaine.

440. Lors de son adoption, le RGPD[889], était accompagné d'une directive du même jour[890], laissant aux Etats membres des marges de manœuvre substantielles dans l'application de ce dernier. Cette opportunité a été saisie par le législateur, lui permettant d'autoriser le recours à des décisions administratives individuelles exclusivement automatisées sauf si elles portent sur

---

[886] *Ibid.*, « *(…) Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité ».*
Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée. »

[887] CNIL, déc. n° MED-2017-053 du 30 août 2017 *mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation.*

[888] Projet de loi pour une République numérique, étude d'impact, 9 décembre 2015, p.10.

[889] 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* ; OJ L 119, 4.5.2016, p. 1 à 88.

[890] Directive (UE) 2016/680 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.

des données sensibles ou s'il s'agit de « *se prononcer sur un recours administratif mentionné au titre Ier du livre IV du Code des relations entre le public et l'administration* »[891].

441. En l'occurrence, il convient d'entendre par donnée personnelle sensible au regard de la LIL, les données qui

> « *(…) révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* »[892].

442. Malgré ces exceptions, le champ des possibles est relativement étendu pour l'administration, et la LIL ne semblait pas exclure explicitement le recours aux algorithmes auto-apprenants pour ces décisions.

443. Par une décision du 12 juin 2018, le Conseil constitutionnel a notamment été amené à contrôler la conformité de cette nouvelle disposition avec la Constitution[893]. Les requérants estimaient[894] que l'existence de ces décisions individuelles prises sur le fondement exclusif de traitements algorithmiques équivaudrait à un renoncement du pouvoir d'appréciation de l'administration concernant les situations individuelles, ce qui méconnaîtrait la garantie des droits et l'article 21 de la Constitution. Tel serait particulièrement le cas pour les algorithmes d'apprentissage automatique, qui sont *« susceptibles de modifier eux-mêmes les règles* »[895]. Ces algorithmes empêcheraient également l'administration de connaître les véritables règles fondant ces décisions administratives. Autre interrogation soulevée par les requérants : en acceptant ce type de décision automatisée, le législateur porterait atteinte *« aux principes de valeur constitutionnelle régissant l'exercice du pouvoir réglementaire* » puisque d'une part, l'administration abandonnerait son pouvoir réglementaire à des algorithmes capables de modifier les règles par eux-mêmes, et d'autre part, le recours à ces algorithmes ne permettrait pas de s'assurer que ces derniers appliquent bel et bien le droit existant. De plus, en ce qui concerne le recours aux algorithmes auto-apprenants, dans la mesure où ils sont susceptibles de

[891] Art. 47 2° de la LIL modifiée.
[892] Art. 6 de la LIL modifiée.
[893] CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*.
[894] *Ibid.*, § 66.
[895] *Ibid.*

réviser les règles qu'ils appliquent eux-mêmes, il en résulterait une imprévisibilité méconnaissant le principe de publicité des règlements. Il ressort du dernier moyen soulevé par les requérants sur ce fondement que la disposition contestée manquerait de portée normative, ou qu'à défaut, « *elles seraient contraire, par leur complexité, à l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi* »[896]. Mais selon le Conseil Constitutionnel, le législateur a prévu des garanties suffisantes de transparence que nous étudierons dans le cadre de la motivation, et ce afin de se prémunir contre un « *coup de data permanent* »[897].

B - La motivation

444. La motivation participe, comme le décrivait si bien René Chapus, à trois exigences

> « *celle de la démocratie, car il est conforme à ses principes que les administrateurs rendent comptent aux administrés des raisons pour lesquels ils se sont déterminés ; celle d'une bonne administration, car l'obligation de motiver contraint les autorités administratives à examiner attentivement le bien-fondé des décisions qu'elles projettent […] ; celle enfin d'un bon contrôle de l'Administration : la connaissance des motifs des décisions permet aux intéressés de mieux apprécier s'il y a pour eux matière à réclamation ou à recours, tandis que le travail du juge, s'il est saisi, est facilité* »[898].

445. Nous pouvons comprendre aisément que la motivation est également au service de la transparence des algorithmes lorsque ces derniers prennent des décisions ou interviennent comme simple aide. Toutefois, comme le rappelle Jean Waline[899], l'administration française a très longtemps été dominée par la culture du secret, ce qui n'était plus acceptable compte tenu des exigences démocratiques. C'est notamment dans ce mouvement général de transparence que la LIL de 1978 et la loi du 11 juillet 1979[900] relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public se sont inscrites. Malgré des

---

[896] *Ibid*.
[897] L'expression *« coup de data permanent »* que nous reprenons est issue de l'article de BARRAUD B., « Le coup de data permanent : la loi des algorithmes », *Revue des droits et libertés fondamentaux*, 2017.
[898] CHAPUS R., *Droit administratif général*, tome 1, 15e éd., 2001, Montchrestien, p. 1131 (cité par PAPADAMAKI I., « L'obligation de motivation en droit administratif français sous l'influence du droit de l'Union européenne », *RDP*, 2017, p. 1245.).
[899] WALINE J., *Droit administratif*, *Dalloz*, 27e édition, p. 473.
[900] Loi n° 79-587 du 11 juillet 1979 *relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public.*

améliorations, force est de constater que l'administration connaît encore bien des zones d'ombre[901].

446. Mais la possibilité de prendre des décisions administratives individuelles fondées sur des traitements algorithmiques sans que les administrés n'aient à donner leur consentement[902] du fait de prérogatives de puissances publiques, ajoute à notre sens une dimension opaque à une transparence déjà imparfaite, parce que non reconnue[903].

447. Si le traitement algorithmique fondant la décision administrative individuelle manipule des données à caractère personnel, l'intéressé doit se voir communiquer « *les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre* »[904]. Mais il existe des cas dans lesquels des décisions administratives individuelles font intervenir des traitements algorithmiques ne manipulant pas de données à caractère personnel. Dans ce cas de figure, il était impossible pour un administré ayant fait l'objet d'une décision administrative individuelle d'être informé ou de connaître les principales caractéristiques des traitements algorithmiques intervenus dans la prise de décision, et ce de manière intelligible, car non soumis au régime juridique de la LIL. Le législateur est donc intervenu à cette fin par l'intermédiaire de la LRN de 2016.

448. Bien que ces dispositions ne figurent pas dans le livre du CRPA relatif à la motivation des actes administratifs, mais dans le livre III de ce dernier relatif à l'étendue de la communication des documents administratifs, nous constatons que ces nouvelles dispositions concourent à la motivation des décisions administratives individuelles. Selon nous, cela s'explique par le fait qu'en 2016, les décisions administratives individuelles devaient nécessairement faire intervenir un humain. D'une part, l'algorithme intervenait donc soit en tant qu'aide à la prise de décision, auquel cas, il existait une possibilité de ne pas suivre ses recommandations, et d'autre part, le fait qu'un humain intervienne dans la prise de décision faisait écran par rapport à l'algorithme. Dans cette situation, connaître les principales caractéristiques du traitement algorithmique ne pouvait être synonyme de motivation, ne serait-ce parce qu'en tout hypothèse un agent public pouvait ne pas suivre cet outil. Alors que pour

[901] CHEVALLIER J., « Le mythe de la transparence administrative », *op. cit*., p. 244.
[902] Art. 47 2° de la LIL modifiée.
[903] Il n'existe pas à ce jour un principe général de transparence des décisions administratives comme l'a affirmé le Conseil d'Etat dans sa décision du 23 février 2005, req. n° 241796.
[904] Art. 47 1° de la LIL modifiée.

les décisions administratives individuelles exclusivement automatisées, connaître les principales caractéristiques de l'administration, revient à disposer de la motivation de l'acte.

1 - La mise en ligne par défaut des principales caractéristiques des algorithmes utilisées par l'administration pour fonder les décisions administratives individuelles

449. L'article L. 312-1-3 du CRPA précise que les administrations « *publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles* »[905].

450. Le mécanisme est intéressant, car nous sortons d'une logique individuelle de la demande pour aboutir à une logique d'automaticité de la mise en ligne des principales caractéristiques des traitements algorithmes fondant des décisions administratives individuelles sous réserve des exceptions que nous avons déjà évoquées[906]. Nous constatons toutefois que cette disposition est subordonnée à un seuil qui nous semble discutable. En effet, cette obligation ne concerne que les administrations d'au moins cinquante agents ou salariés équivalents temps plein[907]. Ce seuil exclue donc de nombreuses administrations qui seraient susceptibles de recourir à ces outils.

451. Fort heureusement, le législateur a prévu des obligations supplémentaires incombant à l'administration[908].

2 - Les décisions administratives individuelles prises sur le fondement d'un traitement algorithmique

a - La mention explicite et la communication des principales caractéristiques

452. Comme nous l'avons vu précédemment, l'étendue du droit à la communication aux codes sources est une avancée majeure, même s'il existe encore bien des exceptions à ce droit[909]. Toutefois, la communication du code source ne se suffit pas à lui-même et n'est pas intelligible pour un administré profane en programmation informatique, surtout lorsque ce

[905] Art. L. 312-1-3 du CRPA.
[906] Voir en ce sens, art. L.311-5 du CRPA, *supra*., n° 421.
[907] Art. D. 312-1-4 du CRPA.
[908] Est considérée comme administration toute mission de service public effectuée par l'Etat, les collectivités territoriales, « *ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission* ». Voir en ce sens, art. L. 300-2 du CRPA.
[909] *Supra*., n° 410 et s.

dernier fait l'objet d'une décision administrative individuelle. Ce nouveau régime juridique met donc en place une logique d'intelligibilité des algorithmes et non plus une simple communication des codes informatiques sans la moindre explication. L'intéressé, qu'il s'agisse d'une personne physique ou morale[910], pourra alors demander, même si la décision lui est favorable, à ce que lui soit communiquée de manière intelligible les principales caractéristiques du programme, notamment appliqués à sa situation. C'est aussi une façon de s'assurer que le traitement algorithmique ne comporte pas de discrimination par exemple, et est bien conforme au droit.

453. Sous réserve des secrets protégés par la loi[911], l'article L. 311-3-1 du CRPA dispose que

> *« […] une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande ».*

454. La décision administrative individuelle doit mentionner, au titre de la mention explicite, la finalité poursuivie par le traitement algorithmique qui fonde la décision[912] ainsi que rappeler le droit *« d'obtenir la communication des règles définissant ce traitement et des principales caractéristiques de sa mise en œuvre, ainsi que les modalités d'exercice de ce droit à communication et de saisine, le cas échéant, de la commission d'accès aux documents administratifs, définies par le présent livre »*[913].

455. Si l'intéressé souhaite connaître les règles définissant le traitement ainsi que les principales caractéristiques de l'algorithme, sous réserve de ne pas porter atteinte à des secrets protégés par la loi, l'administration doit lui communiquer ces éléments sous une forme intelligible comprenant le degré et le mode de contribution du traitement algorithmique à la prise de décision, les données traitées et leurs sources, les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ainsi que les opérations effectuées par le traitement[914].

---

[910] En effet, le fait que les personnes morales soient concernées par ce droit est une avancée majeure, dans la mesure où la LIL ne s'applique qu'aux traitements de données à caractère personnel, c'est-à-dire aux données permettant d'identifier des personnes physiques.
[911] *Supra.*, n° 421.
[912] Art. R. 311-3-1-1 du CRPA.
[913] *Ibid.*
[914] Art. R. 311-3-1-2 du CRPA.

456. La CNIL souhaitait pourtant dans son avis[915] sur le projet de décret d'application (actuel Article R. 311-3-1-2 du CRPA) qu'une liste des obligations de transparence de ces traitements soit plus précise afin d'empêcher que l'administration ne dispose d'une marge d'appréciation trop importante sur les catégories d'informations communicables. Elle a donc proposé une série de catégories sous forme d'exemple à ajouter audit décret telles que

> *« (…) par exemple, la méthode ayant servi à développer l'algorithme et les contraintes ou les besoins qui ont été définis par l'administration ou, si une évaluation a été menée, le taux d'erreur de l'algorithme et les types d'erreurs par catégorie de données ou encore les critères précis selon lesquels l'algorithme a été testé et évalué »*[916].

457. Malheureusement, cette proposition n'a pas été retenue par le gouvernement. Puisqu'il n'existe pas de symétrie entre la liberté d'accès aux traitements automatisées de données à caractère personnel et la communication des principales caractéristiques des traitements algorithmiques fondant une décision administrative individuelle, nous ne pouvons que regretter un régime juridique confus pour les demandeurs. En outre, comme Jean-Baptiste Duclercq, un encadrement général des algorithmes aurait été plus approprié, notamment pour plus d'intelligibilité des personnes juridiques[917].

458. Toutefois, l'intéressé ignorera que la décision administrative individuelle a été prise sur le fondement d'un traitement algorithmique dans les hypothèses où la communication porte atteinte aux secrets protégés par la loi[918]. L'absence de mention explicite qu'un algorithme est intervenu dans la prise décision est à déplorer dans la mesure où l'administré ne pourra pas soupçonner l'utilisation d'un algorithme, et donc ne pourra le contester.

b - Une obligation de transparence renforcée pour les décisions administratives individuelles exclusivement automatisées

459. Comme nous l'avons vu, autrefois interdit par la loi, le législateur a finalement autorisé le recours aux décisions administratives exclusivement automatisées à la seule condition qu'elles soient explicables. Cette obligation d'explicabilité va au-delà du régime juridique

[915] CNIL, Délibération n° 02017-023 du 16 février 2017 portant avis sur un projet de décret relatif aux modalités de communication des règles et caractéristiques des traitements algorithmiques.
[916] *Ibid*.
[917] DUCLERCQ J-B., « Le droit public à l'ère des algorithmes », *op. cit.*, p. 1401.
[918] Art. L. 311-5 2° du CRPA.

prévu pour les décisions privées exclusivement automatisées[919] puisque le « *le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard* »[920].

460. Pour les sages de la rue de Montpensier[921], ces dispositions ne sont pas contraires à la Constitution en ce que le législateur a défini « *des garanties appropriées pour la sauvegarde des droits et libertés des personnes soumises aux décisions administratives individuelles prises sur le fondement exclusif d'un algorithme* »[922].

461. Toutefois, le Conseil vient préciser les conditions du recours par l'administration aux traitements algorithmiques auto-apprenants. Il rappelle que l'adoption de décisions administratives individuelles prises sur le fondement exclusif d'un traitement algorithmique ne peut être effectuée que si les règles et critères sont définis à l'avance par le responsable du traitement. Ces algorithmes n'autorisent pas l'administration à fonder « *des décisions sans base légale, ni à appliquer d'autres règles que celles du droit en vigueur* »[923]. Il en résulte que le recours à ces algorithmes ne peut être perçu comme une renonciation au pouvoir réglementaire.

462. Le Conseil rappelle que ces décisions automatisées sont par ailleurs soumises au respect de trois conditions sous peine d'illégalité[924]. Premièrement, elles doivent respecter les obligations précisées par l'article L. 311-3-1 du CRPA[925]. Le Conseil précise toutefois que dans les hypothèses où les principales caractéristiques de l'algorithme ne peuvent être communiquées pour des raisons de secrets ou intérêts énoncés au 2° de l'article L. 311-5 du même Code, « *aucune décision ne peut être prise sur le fondement exclusif de cet algorithme* »[926]. Il apparaît donc que la transparence de ces algorithmes est pour le Conseil la condition *sine qua non* au recours à des décisions prises exclusivement sur le fondement de traitements algorithmiques, et ce conformément au souhait du législateur. Deuxièmement, ces décisions doivent être susceptibles d'un recours administratif ou contentieux[927]. En cas de tel recours, l'administration doit être susceptible de se prononcer sur la décision « *sans pouvoir se*

[919] *Supra*., n° 147 et s.
[920] Art. 47 2° de la LIL modifiée.
[921] CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*.
[922] *Ibid*., § 72.
[923] *Ibid*., § 69.
[924] *Ibid*., § 70.
[925] *Supra*., n° 453.
[926] *Ibid*.
[927] Conformément au chapitre 1er titre 1er du livre IV du CRPA.

fonder exclusivement sur l'algorithme »[928]. Ensuite, si le juge administratif est saisi d'un recours contre cette décision, l'administration doit être en capacité de communiquer à la juridiction les caractéristiques de l'algorithme. Troisièmement, un traitement algorithmique ne peut fonder exclusivement une décision s'il porte sur des données à caractère personnel sensibles conformément à la règlementation[929].

463. Enfin, concernant le responsable du traitement, il doit avoir la maîtrise du traitement[930] et ses évolutions, afin d'expliquer au demandeur, sous une forme intelligible, la façon dont le traitement a été mis en œuvre à son égard. Par ailleurs, en l'absence de contrôle et de validation des algorithmes d'apprentissage automatique par le responsable de traitement, ces algorithmes auto-apprenants, susceptibles de modifier les règles eux-mêmes, ne pourront fonder exclusivement une décision administrative individuelle. Cela revient finalement à considérer qu'une décision individuelle ne peut être exclusivement fondée sur des algorithmes auto-apprenants, car en l'état des sciences informatiques, nous ne sommes pas encore capables d'expliquer les résultats de ces algorithmes et leurs processus.

464. Ce régime juridique semble pour l'heure complexe à mettre en œuvre et relativement méconnu des administrations comme le souligne un Rapport de l'ENA[931] alors même que ces obligations sont entrées en vigueur depuis le 1er septembre 2017. C'est sans doute pour cette raison que le législateur, dans la modification de la LIL en 2018[932], a considéré qu'à partir du 1er juillet 2020, les décisions administratives individuelles reposant exclusivement sur des traitements algorithmiques comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du CRPA.

[928] CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*, § 70.
[929] Art. 47 2° de la LIL modifiée.
[930] CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*, § 71.
[931] CHIGNARD S., Algorithmes publics : des élèves de l'ENA formulent une série de recommandations sur les enjeux d'éthique et de responsabilité, *Le blog d'Etalab* [en ligne]. 20 janvier 2020 [Consulté le 30 janvier 2020]. Disponible à l'adresse : https://www.etalab.gouv.fr/algorithmes-publics-des-eleves-de-lena-formulent-une-serie-de-recommandations-sur-les-enjeux-dethique-et-de-responsabilite
[932] DOUVILLE T., « Parcoursup et le secret des algorithmes », *op. cit.*, p. 700. Lire également à ce sujet, DOUVILLE T., « Parcoursup à l'épreuve de la transparence des algorithmes », *op. cit.*, p. 390.

C - Vers des exceptions à la transparence toujours plus nombreuses et critiques diverses

1 - L'exception introduite par la loi n° 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants

465. Indépendamment des exceptions déjà prévues par le CRPA, le législateur a été amené à dénaturer de manière significative l'esprit de la LRN[933] qui avait pourtant vocation à contribuer à une plus grande transparence des décisions administratives individuelles fondées sur un traitement algorithmique, notamment en rétrécissant le champ des données « secrètes »[934].

466. A la suite de l'abandon de la plateforme *APB*[935], une nouvelle plateforme a vu le jour par arrêté[936], dénommée *Parcoursup*. Il s'agit cette fois-ci non pas d'un traitement illégal[937] exclusivement automatisé, effectuant un tirage au sort entre les candidats dès lors que *« le nombre de candidats remplissant les mêmes critères reste supérieur au nombre de places disponibles »*[938], mais d'une aide à la prise de décision, faisant donc intervenir des humains dans l'étude des dossiers.

467. Le MESRI, conformément à l'article L. 612-3 II du Code de l'éducation, a décidé de rendre public le code source du traitement automatisé de la plateforme nationale ainsi que le cahier des charges synthétiques[939]. Mais les algorithmes, dits *locaux*, utilisés par certaines équipes pédagogiques universitaires chargées de l'examen des candidatures dans les établissements, n'ont pas fait l'objet à ce jour d'une quelconque publicité. Or, pour reprendre les propos de Thibault Douville, « *un algorithme est secret dès lors que celui qui l'a créé ou le met en œuvre ne le communique pas* »[940].

468. En effet, la loi n° 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants est venue modifier l'article L. 612-3 du Code de l'éducation, précisant qu'

[933] La loi n° 2016-1321 préc. avait introduit les dispositions relatives à la transparence des traitements algorithmiques dans le CRPA.
[934] CLUZEL-METAYER L., « L'ouverture des données publiques », *in Le droit administratif au défi du numérique*, *AFDA*, 2019, p. 19.
[935] *Supra.*, n° 437.
[936] Arrêté du 28 mars 2018 *autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Parcoursup »*, JORF n° 0074 du 29 mars 2018, abrogé depuis par l'arrêté du 31 décembre 2020 portant création d'un traitement automatisé de données à caractère personnel dénommé « *Parcoursup* ».
[937] CNIL, déc. n° MED-2017-053 du 30 août 2017 *mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation.*
[938] *Ibid*.
[939] VIDAL F., Parcoursup, la plateforme d'admission dans l'enseignement supérieur, *op. cit.*
[940] DOUVILLE T., « Parcoursup et le secret des algorithmes », *op. cit.*, p. 700.

« [a]fin de garantir la nécessaire protection du secret des délibérations des équipes pédagogiques chargées de l'examen des candidatures présentées dans le cadre de la procédure nationale de préinscription prévue au même deuxième alinéa, les obligations résultant des articles L. 311-3-1 et L. 312-1-3 du code des relations entre le public et l'administration sont réputées satisfaites dès lors que les candidats sont informés de la possibilité d'obtenir, s'ils en font la demande, la communication des informations relatives aux critères et modalités d'examen de leurs candidatures ainsi que des motifs pédagogiques qui justifient la décision prise »[941].

469. La CADA est même allée jusqu'à déplorer ce régime spécial d'accès[942]. Il est intéressant de noter qu'en contrepartie de cette absence de communication individuelle des principales caractéristiques des traitements algorithmiques aux candidats, un comité d'éthique et scientifique a été institué en tant que tiers de confiance afin de garantir le bon fonctionnement de la plateforme[943]. Dans le second rapport annuel adressé au Parlement rendu par ce Comité, il est considéré que la transparence

« englobe la transparence au sens strict – dire ce que l'on fait –, la loyauté – faire ce que l'on dit (i.e. ne faire que ce que l'on dit) –, l'intelligibilité – ce que l'on fait doit être compréhensible –, ainsi que la confidentialité des données personnelles. On peut préciser que la loyauté implique l'absence de biais et en particulier l'équité algorithmique, qui impose que deux personnes devant être traitées de la même façon le soient effectivement »[944].

470. Bien que l'idée de ce comité soit intéressante, c'est désormais la transparence de ce dernier qui interroge, et ce d'autant plus qu'il n'étudie pas tous les algorithmes *locaux* utilisés par les équipes pédagogiques qui cristallisent la défiance.

---

941 Code de l'éducation, art. L. 612-3, I, al. 5.

942 CADA, avis n° 20184400 du 10 janvier 2019.

943 « *Il s'assure que les règles informatiques qui régissent son fonctionnement sont strictement claires, conformes aux normes en vigueur et transparentes. A ce titre, il est chargé : 1) D'émettre un avis sur toute évolution substantielle des règles de fonctionnement de la plateforme Parcoursup ; 2) D'analyser le fonctionnement de la plateforme et de faire toute proposition au ministre chargé de l'enseignement supérieur afin de l'améliorer ; 3) D'examiner les conditions d'ouverture du code source des traitements automatisés utilisés pour le fonctionnement de la plateforme Parcoursup ; 4) De veiller au respect des principes juridiques et éthiques qui fondent l'examen des candidatures réalisé par les établissements dispensant des formations initiales du premier cycle de l'enseignement supérieur*. », art. 1, arrêté du 9 mars 2018 relatif aux missions, à la composition et aux modalités de fonctionnement du comité éthique et scientifique de la plateforme *Parcoursup*.

944 FALQUE-PIERROTIN I., BERRY G., CYTERMANN J-R. et al., *Comité éthique et scientifique de Parcoursup, Rapport au parlement* [en ligne]. Janvier 2020 [Consulté le 30 janvier 2020]. Disponible à l'adresse : https://cache.media.enseignementsup-recherche.gouv.fr/file/2020/28/9/Rapport_du_CESP_2019_(janvier_2020)_1227289.pdf

471. Le Défenseur des droits a été saisi de nombreuses demandes allant dans le sens d'une transparence des algorithmes dits *locaux* utilisés par les Universités dans la sélection des candidatures, notamment car ces traitements algorithmiques opaques risquaient d'ouvrir la voie à l'existence de pratiques discriminantes dans l'évaluation des dossiers. Par une décision en date du 18 janvier 2019[945], le Défenseur des droits considère que « *le secret des délibérations ne s'oppose pas à l'information des candidats sur le contenu exact et la manière précise d'évaluation des candidatures* »[946]. En effet, selon lui, une transparence des critères sur lesquels les dossiers sont examinés ne porte pas atteinte aux principes de souveraineté du jury et du secret des délibérations dans la mesure où la publication de ces informations « *ne vise pas à dévoiler le contenu de l'appréciation portée sur chaque candidature, mais uniquement les critères pris en compte dans cette appréciation ainsi que leur méthode d'application* »[947].

472. Dans le même temps, le Tribunal administratif de Guadeloupe a été saisi par un syndicat étudiant d'une demande de communication des procédés algorithmiques utilisés par l'Université des Antilles dans le cadre de la sélection des candidatures *Parcoursup*. Par un jugement en date du 4 février 2019[948], le tribunal annule la décision implicite de rejet refusant la transmission des procédés algorithmiques *locaux* au syndicat et décide d'enjoindre l'Université de procéder à ladite communication au motif que cette dernière ne porte pas atteinte au secret des délibérations. En effet, cette diffusion ne porte que sur la nature des critères pris en compte dans le traitement des candidatures, c'est-à-dire leur pondération ou encore leur hiérarchisation, et aucunement sur « *l'appréciation portée par la commission sur les mérites de chacune de ces candidatures* »[949]. De plus, pour le juge administratif, puisque la demande n'émane pas d'un candidat, mais d'un tiers, la communication des procédés algorithmiques ainsi que des codes sources de ces programmes est fondée. En effet, le législateur n'a pas écarté dans l'article L. 612-3 I du Code de l'éducation la disposition de l'article L. 311-1 du CRPA permettant notamment à toute personne qui en fait la demande d'obtenir la communication des documents administratifs qui sont détenus par l'administration[950].

473. Par une décision en date du 12 juin 2019[951], le Conseil d'Etat annule le jugement du Tribunal administratif de Guadeloupe au motif que ce dernier a commis une erreur de droit.

[945] Défenseur des droits, déc. n° 2019-021 du 18 janvier 2019.
[946] *Ibid.*, § 39.
[947] *Ibid*.
[948] TA Guadeloupe, 4 février 2019, *UNEF c. Université des Antilles*, n° 1801094.
[949] *Ibid.*, cons. 11.
[950] Sauf s'il s'agit de secrets protégés par la loi, *Supra*., n° 421.
[951] CE, 12 juin 2019, *Université des Antilles*, n° 427919.

Dans une motivation lapidaire[952], les juges constatent que le législateur a également entendu déroger par des dispositions spéciales aux dispositions de l'article L. 311-1 du CRPA alors que le texte ne prévoit déroger qu'aux articles L. 311-3-1 et L312-1-3 du CRPA. Certes, le législateur a dérogé à ces dispositions dans l'article L. 612-3 I du code de l'éducation, et comme nous l'avons déjà expliqué, cet article ne concerne pas les tiers, mais les candidats. Concernant les candidats, cette demande peut être fondée. Elle serait d'autant plus fondée que ces procédés algorithmiques, une fois communiqués, ne portent pas atteinte au secret des délibérations. Il est important de souligner qu'entre le jugement du Tribunal administratif de Guadeloupe du 4 février 2019[953] et l'arrêt du Conseil d'Etat, un décret en date du 26 mars 2019[954] est venu préciser l'article D. 612-1-5 du Code de l'éducation afin que soit portée à la connaissance des candidats *« les critères généraux encadrant l'examen des candidatures par les commissions d'examen des vœux* ». La communication de ces critères généraux aux candidats est alors présentée comme étant un bon compromis visant à pallier l'absence de communication des principales caractéristiques de l'algorithme. Or, comme nous l'avons développé tout au long de cette partie, la transparence, et donc l'acceptabilité de ces algorithmes, ne peut être tolérée que par la mise en œuvre de dispositifs de conformité, c'est-à-dire de règles qui en l'espèce viseraient à ce que les critères généraux servant à l'étude des candidatures par les commissions d'examen des vœux qui sont communiquées, correspondent bien aux critères appliqués dans la réalité. C'est d'ailleurs l'esprit de la LRN de se voir communiquer les principales caractéristiques d'un algorithme ayant fondés une décision administrative individuelle afin de s'assurer qu'il a bien été appliqué à sa situation. Nous regrettons que cette décision confirme une certaine opacité alors qu'il existait un autre chemin : celui préconisée par le Défenseur des droits Jacques Toubon et le Tribunal administratif de Guadeloupe qui opérait une meilleure garantie. Car si on admet que la communication des principales caractéristiques des algorithmes et code source porte atteinte au secret des délibérations, cela revient à reconnaître que la décision d'affectation dans un établissement repose exclusivement sur un traitement automatisé de données, ce qui est illégal en l'absence de transparence absolue comme a pu l'affirmer le Conseil constitutionnel, et ce quand bien même il ne s'agirait pas d'un algorithme auto-apprenant[955].

[952] *Ibid.*, § 8.
[953] TA Guadeloupe, 4 février 2019, *UNEF c. Université des Antilles*, n° 1801094.
[954] Décret n° 2019-231 du 26 mars 2019 *relatif à la procédure nationale de préinscription pour l'accès aux formations initiales du premier cycle de l'enseignement supérieur et modifiant le code de l'éducation*.
[955] CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*.

474. Dans sa critique de l'arrêt du Conseil d'Etat du 12 juin 2019, Roseline Letteron[956] considère que le décret en date du 26 mars 2019 instaure une transparence des délibérations locales à travers la publication des « *critères généraux encadrant l'examen des candidatures (...)* ». Nous ne partageons pas cet avis. S'il est vrai que le décret du 26 mars 2019 impose la publication des critères généraux encadrant l'examen des candidatures, il ne s'agit pas du même niveau garanti de transparence administrative. En effet, l'article L. 311-3-1 du CRPA a, comme nous l'avons rappelé, été exclu par le législateur dans le cas de ces délibérations. Il en va de même de l'article L 311-1 par le Conseil d'Etat sur le fondement des travaux préparatoires. Sauf qu'un traitement algorithmique peut mettre en œuvre des critères qui ne sont pas ceux déclarés, y compris des critères illégaux. Il ne s'agit pas d'ailleurs d'incriminer les équipes pédagogiques, car elles pourraient être susceptibles d'être assistées par des traitements algorithmiques qui appliquent des critères qu'ils n'ont peut-être même pas voulu mettre en place. A ce titre, l'esprit de l'article L311-3-1 est justement de pouvoir s'assurer que le traitement algorithmique appliqué à la situation du candidat est bien celui qui a été déclaré par l'établissement. En se contentant du décret du 26 mars 2019 comme unique garantie, l'opacité des traitements algorithmiques est omniprésente et n'est pas levée. En effet, comment un candidat pourrait-il prouver que les critères avancés par les équipes pédagogiques chargées de l'examen des candidatures correspondent à la réalité des traitements algorithmiques dès lors que l'on ne se soucie plus de leur contrôle ? Par sa décision, le Conseil d'Etat n'arrive pas en retard, à la suite du décret du 26 mars 2019, mais il scelle au contraire l'absence de transparence dans ce domaine. La crainte est même de se voir multiplier des exceptions à cette transparence alors que les secrets protégés par la loi sont déjà nombreux.

475. Enfin, dans un arrêt en date du 15 janvier 2020, le Conseil d'Etat a transmis au Conseil constitutionnel une question prioritaire de constitutionnalité[957]. Les sages se sont prononcés[958] sur la conformité des exceptions prévues par le Code de l'éducation, notamment par rapport à l'article 15 de la DDHC de 1789 relatif au « *droit de demander compte à tout Agent public de son administration* ». Malgré la reconnaissance à valeur constitutionnelle d'un principe d'accès aux documents administratifs, le Conseil a considéré que « *la restriction d'accès à certains documents administratifs relatifs aux traitements algorithmiques éventuellement utilisés par*

[956] LETTERON R., Parcoursup devant le Conseil d'Etat, *Liberté, Libertés chéries. Veille juridique sur les droits de l'homme et les libertés publiques* [en ligne]. 18 juin 2019 [Consulté le 18 janvier 2020]. Disponible à l'adresse : https://libertescheries.blogspot.com/2019/06/parcoursup-devant-le-conseil-detat.html?fbclid=IwAR1Wk-y44fInC6nRP_pghPwW6i-0hRDvhUJlOu-Zkt1X8-igyA3HDPWu75Y

[957] CE, 15 janvier 2020, req. n° 433296.

[958] CC, décision n° 2020-834 QPC, 3 avril 2020.

l'établissement ne prive pas d'effectivité les recours contre une décision de refus d'inscription »[959] alors pourtant que l'absence de transparence ne permet pas de s'assurer que le traitement est conforme au droit, ce qui nuit à sa contestabilité.

476. L'action administrative, telle qu'imaginée par le législateur et la juridiction administrative et constitutionnelle, ne peut que jeter une défiance entre l'administration et les administrés. Or, la confiance, assurée notamment par une transparence des algorithmes, est fondamentale dans l'acceptabilité de ces derniers.

2 - Les faiblesses d'un régime juridique en construction : les outils d'aide à la prise de décision

477. Dans le cadre des décisions que nous étudions, la communication des principales caractéristiques des outils d'aide à la prise de décision n'a finalement que très peu d'intérêt si nous ne pouvons pas prouver que l'administration est dans une situation de compétence liée. En effet, si l'administration dispose dans son champ de compétences d'un pouvoir discrétionnaire, contester l'outil d'aide à la prise de décision ne permettra pas de remettre en cause la décision puisqu'un agent fait écran. Or, il serait raisonnable de penser que même dans l'hypothèse où l'administration disposerait d'un pouvoir discrétionnaire, l'agent serait potentiellement influencé par le logiciel d'aide à la prise de décision qu'il utilise[960]. De plus, dans certaines circonstances les programmeurs peuvent être considérés comme les véritables auteurs de l'acte lorsque le logiciel est suivi, parce qu'ils retranscrivent la législation ou la réglementation sous forme d'algorithmes, et opèrent les arbitrages nécessaires afin que l'informatisation du processus décisionnel soit possible.

478. Afin d'éviter qu'un agent fasse écran systématiquement entre la décision individuelle et le programme utilisé, ce qui empêche la « contestabilité » de ces algorithmes[961], nous proposons que la mention explicite fasse apparaître les statistiques de suivi de ces outils par les agents dudit service dans les conditions similaires. Ces statistiques, qui devraient être tenues par l'administration et contrôlées par une autorité indépendante que nous développerons dans le cadre de la seconde partie de cette thèse[962], permettrait de connaître si l'agent est dans une

[959] CC, décision n° 2020-834 QPC, 3 avril 2020, § 20.
[960] CLUZEL-METAYER L., « L'influence des algorithmes sur l'édiction des décisions administratives », in *Méthodes en droit administratif*, Thèmes et commentaires, *AFDA*, 2018, p. 243.
[961] BARBIN E., « Le contrôle juridictionnel de l'outil numérique d'aide à la décision administrative », *RFDA*, 2021, p. 491.
[962] *Infra.*, n° 694 et s.

situation de compétence liée[963] vis-à-vis de l'outil. A ce titre, les services recourant à ces technologies seraient dans l'obligation de tenir un registre précis du nombre de décisions édictées, d'une part par l'algorithme, dans le cas des traitements exclusivement automatisés, et d'autre part, communiquer les statistiques de suivi des algorithmes par les agents pour les simples outils d'aide à la prise de décision algorithmique. Ces informations doivent être communicables car elles informent les intéressés sur les critères de la motivation, facilitant de fait un éventuel recours pour excès de pouvoir par exemple. C'est ici la dimension quantitative de l'application de ces algorithmes qui éclaire sur leur implication réelle sur la situation des administrés. C'est par le truchement de cette dimension collective, qu'il convient de connaître les effets de la multiplication des algorithmes dans l'action administrative. Il s'agit d'une approche moins individualisée, mais plus collective, qui informe. Dans l'hypothèse d'une circulaire impérative, les agents en connaissent la portée normative. En effet, c'est parce qu'elle est impérative qu'elle va être suivie. Mais les algorithmes nous enseignent qu'à défaut d'être suivi parce qu'une norme l'exige, c'est la façon dont l'algorithme est appliqué qui qualifie l'algorithme ou non d'impératif. Or, cette dimension n'a pas encore été appréhendée par le législateur.

479. Si l'administration dispose d'un pouvoir discrétionnaire, et que l'outil est suivi en permanence dans les recommandations qu'il effectue, le juge pourrait alors requalifier la décision administrative individuelle de purement automatisée, appliquant de ce fait les règles de transparence absolue inhérente au régime juridique tel que dessiné par le Conseil constitutionnel et la règlementation en vigueur[964]. Dans l'hypothèse où il s'avérerait que les critères de l'algorithme sont non conformes au droit, cela permettrait ensuite de contester par l'intermédiaire d'un recours pour excès de pouvoir l'outil d'aide à la décision parce qu'il serait assimilable au régime juridique des circulaires impératives ou encore des lignes directrices, c'est-à-dire des actes faisant griefs[965].

480. Le recours pour excès de pouvoir doit alors être privilégié puisque les débats autour des critères pour apprécier la légalité de l'acte algorithmique qui, bien que pris formellement par un auteur humain si la décision n'est pas exclusivement automatisée, revient à contester le

[963] En effet, nous pouvons tout à fait imaginer que dans certains cas, l'agent soit dans une situation de compétence liée. En ce sens, voir PAULIAT H., « La décision administrative et les algorithmes : une loyauté à consacrer », *RDP*, 2018, p. 641.
[964] *Supra*., n° 459 et s.
[965] Voir notamment en ce sens, CE, 12 juin 2020, n° 418142 : *« 1. Les documents de portée générale émanant d'autorités publiques, matérialisés ou non, tels que les circulaires, instructions, recommandations, notes, présentations ou interprétations du droit positif peuvent être déférés au juge de l'excès de pouvoir lorsqu'ils sont susceptibles d'avoir des effets notables sur les droits ou la situation d'autres personnes que les agents chargés, le cas échéant, de les mettre en œuvre. Ont notamment de tels effets ceux de ces documents qui ont un caractère impératif ou présentent le caractère de lignes directrices* ».

programme informatique qui a engendré cette décision puisque sans ce programme, le sens de cette dernière aurait peut-être été tout autre.

481. Mais ce débat ne doit pas effacer une réalité : celle que tout être humain, et donc les auteurs des actes administratifs, sont inconsciemment enclins à des biais cognitifs, et parfois plus encore lorsque certains sont gouvernés par des intérêts propres. C'est d'ailleurs à ce titre que la motivation des actes administratif s'inscrit notamment dans la diminution d'un risque d'arbitraire à l'encontre des administrés ; c'est aussi pour cela que les actes doivent répondre à un certain formalisme, dont la motivation est partie prenante. En ce sens, des auteurs considèrent par ailleurs que l'affectation des lycéens dans l'enseignement supérieur par la voie d'un algorithme est plus équitable que lorsqu'il est effectué par un humain dès lors que les critères sont communiqués[966]. Une action administrative de masse recourant aux traitements algorithmiques n'est pas sans risques. Certains y voient une opportunité pour une application plus rationnelle et uniformisée du droit[967], tandis que d'autres, et nous en faisons partie, craignent des motivations algorithmiques générales et stéréotypées[968]. Dans l'hypothèse du recours à un traitement algorithmique comme aide à la prise de décision, même s'il est indéniable que l'auteur de l'acte est juridiquement l'administration, nous ne pouvons que nous inquiéter que l'agent ne soit en situation de compétence liée. Selon Hélène Pauliat, l'administration est bien, dans certains cas, dans une situation de compétence liée par rapport à l'outil algorithmique [969]. Comment pourrait-il en être autrement dans les faits, dans la mesure où ces outils sont développés dans un but de rationalisation de l'action administrative ? Il serait donc étonnant pour un agent de recourir à un tel outil, qui a accès par ailleurs, dans certains cas, à des millions d'informations, pour finalement s'en défaire. En ne suivant pas les recommandations de l'algorithme, l'agent pourrait parfaitement être accusé de fonder sa décision sur des arguments non objectifs, dans la mesure où l'algorithme est censé incarner une certaine « scientificité » dans la prise de décision. Et s'il s'agit d'un algorithme déterministe, quel agent s'amuserait à recalculer le montant de la taxe d'habitation pour chaque contribuable de son portefeuille par exemple ? Le simple fait de vérifier chaque opération reviendrait par ailleurs à annihiler les bénéfices de l'automatisation.

---

[966] ABITEBOUL S., G'SELL F., « Les algorithmes pourraient-ils remplacer les juges », *in* G'SELL F. (dir.), *Le Big Data et le droit*, Thèmes et commentaires, *Dalloz*, 2020, p. 35.

[967] BARRAUD B., « Un algorithme capable de prédire les décisions des juges : vers une robotisation de la justice ? », *Cahiers de la justice*, 2017/1, p. 121 à 139. L'auteur estime que si la technologie permet un jour des algorithmes fiables, les algorithmes sont à mêmes d'appliquer des décisions les plus proches du droit positif, gageant d'une meilleure sécurité juridique tout en assurant une politique judiciaire uniforme sur l'ensemble du territoire.

[968] En ce sens, voir MOURIESSE E., « L'opacité des algorithmes et la transparence administrative », *RFDA*, 2019, p. 45 et PAULIAT H., « La décision administrative et les algorithmes : une loyauté à consacrer », *op. cit.*, p. 641.

[969] *Ibid.*

482. Au-delà de l'argumentaire classique de la déshumanisation du service public, il convient également de considérer que la sécurité juridique est moins remise en cause par une décision administrative purement humaine. En effet, dans l'hypothèse de l'arbitraire d'un agent administratif, il est possible d'obtenir l'annulation d'un tel acte sans avoir à connaître les inconvénients d'une annulation en cascade[970] d'un outil illégal qui déciderait de manière centralisée de la situation de millions d'administrés. En quelque sorte, nous pouvons affirmer que la multiplicité des agents prenant des décisions est une garantie pour la sécurité juridique, ce qui constitue une sorte de décentralisation de la prise de décision de l'administration. Cette décentralisation humaine profite à la sécurité juridique globale.

483. Enfin, le Premier ministre avait confié à Eric Bothorel une mission relative à la politique de la donnée, des algorithmes et des codes sources. Ce rapport a été remis le 23 décembre 2020 au Premier ministre Jean Castex[971]. S'appuyant sur les conclusions de cette mission, une circulaire[972] est venue réitérer certains objectifs. A cette fin, la Direction Interministérielle du Numérique (DINUM)[973] est davantage amenée à assurer un conseil personnalisé à l'administration[974] sur ces questions. De nouvelles feuilles de route devront également être établies par les ministères d'ici la fin 2021 afin de former les personnels de l'administration à cette tâche[975]. Afin de mettre en œuvre cette stratégie, un arrêté en date du 17 août 2021 instaure un « *administrateur ministériel des données, des algorithmes et des codes sources, en lien avec*

---

[970] En effet, nous pourrions tout à fait imaginer que l'exception d'illégalité permettent l'annulation de décisions en cascade dès lors que le programme serait considéré comme un acte n'ayant pas été attaqué dans le délai de recours.

[971] BOTHOREL E., COMBES S., VEDEL R., Pour une politique publique de la donnée, mission confiée par le Premier ministre, 23 décembre 2020., *Gouvernement.fr* [en ligne]. Décembre 2020. [Consulté le 23 mars 2021]. Disponible à l'adresse : https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publique_de_la_donnee_-_23.12.2020__0.pdf

[972] Circulaire n° 6264/SG du 27 avril 2021 relative à la politique publique de la donnée, des algorithmes et des codes sources, I.

[973] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique.

[974] Etalab est une mission instaurée par le décret n° 2011-194 du 21 février 2011 portant création d'une mission « Etalab » chargée de la création d'un portail unique interministériel des données publiques. Cette mission réunit déjà les codes sources et les jeux de données de plusieurs programmes utilisés par les personnes publiques en vertu de leur mission de service public, *Legifrance.gouv.fr* [en ligne]. Mis à jour le 31 octobre 2012. [Consulté le 26 février 2021]. Disponible à l'adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023619063. Elle est désormais un département rattaché à la DINUM. Elle a par ailleurs déjà publié plusieurs rapports sur l'explication des algorithmes publics, l'état des lieux de l'ouverture des codes sources dans l'enseignement supérieur et de la recherche, ou encore plus récemment sur l'évaluation d'impact algorithmique. CHIGNARD S., Algorithmes publics : Etalab publie un guide à l'usage des administration, *Etalab.gouv.fr* [en ligne]. 15 mars 2019. [Consulté le 16 novembre 2020]. Disponible à l'adresse : https://www.etalab.gouv.fr/algorithmes-publics-etalab-publie-un-guide-a-lusage-des-administrations. Ou CHIGNARD S., Evaluer les impacts des algorithmes : publication d'une étude internationale réalisée à la demande d'Etalab, *Etalab.gouv.fr* [en ligne]. 13 juillet 2021. [Consulté le 21 juillet 2021]. Disponible à l'adresse : https://www.etalab.gouv.fr/evaluer-les-impacts-des-algorithmes-publication-dune-etude-internationale-realisee-a-la-demande-detalab. Et GUERRY B., Etat des lieux des pratiques de publication des codes sources dans l'Enseignement Supérieur et la Recherche, *Etalab.gouv.fr* [en ligne]. 04 février 2021. [Consulté le 25 avril 2021]. Disponible à l'adresse : https://www.etalab.gouv.fr/les-pratiques-de-publication-des-codes-sources-dans-lenseignement-superieur-et-la-recherche

[975] Circulaire n° 6264/SG du 27 avril 2021 relative à la politique publique de la donnée, des algorithmes et des codes sources, II.

l'ensemble des directions d'administration centrale du ministère, Pôle emploi et du délégué ministériel à la protection des donnée »[976]. A titre d'exemple, il est intéressant de noter que comme le souligne le site internet de pôle emploi dans une rubrique dédiée à l'explicabilité des algorithmes, ce que nous pourrions par ailleurs dupliquer à d'autres domaines, « *ces algorithmes sont la traduction de la réglementation en vigueur* »[977]. C'est la raison pour laquelle leur transparence est essentielle, notamment afin qu'ils soient susceptibles de recours.

SECTION II - LA TRANSPARENCE DES ALGORITHMES UTILISES DANS LE CADRE DE LA VIE DEMOCRATIQUE

484. Les algorithmes ne sont pas seulement utilisés dans le cadre des décisions administratives individuelles. En effet, ils s'immiscent également dans les prises de décisions politiques aussi bien en dehors du scrutin (Paragraphe 1) qu'en période électorale (Paragraphe 2). Cette transparence concourt à ce que les citoyens exercent un contrôle sur la démocratie représentative et participative.

PARAGRAPHE 1 – La prise de décision politique par voie algorithmique hors scrutin

485. Il convient de constater que les algorithmes sont désormais utilisés pour sonder politiquement les individus à travers des collectes de données et d'analyse de ces dernières, et sont susceptibles de produire des effets juridiques. Ce nouveau mode de participation (A) nécessite une transparence particulière qui est loin d'être réalisée.

486. Le recours aux traitements algorithmiques est aussi le fait des gouvernants qui n'hésitent plus à se reposer sur certains de ces outils pour évaluer en amont et en aval les politiques publiques (B). Même si ces algorithmes et les données qu'ils manipulent sont une chance dans la compréhension de certaines réformes, ils ne peuvent l'être qu'à certaines conditions.

[976] Arrêté du 17 août 2021 instituant un administrateur ministériel des données, des algorithmes et des codes sources au ministère du travail, de l'emploi et de l'insertion.
[977] POLE EMPLOI, Algorithmes, Tout savoir sur les algorithmes publiés par Pôle Emploi, *Pole-emploi.fr* [en ligne]. [Consulté le 28 août 2020]. Disponible à l'adresse : https://www.pole-emploi.fr/candidat/algorithmes.html

A – Participation : traitements algorithmiques et démocratie continue

1 - Généralités

487. Le principe de participation n'est plus seulement l'apanage de la matière environnementale. En témoigne la multiplication des expérimentations de démocratie participative[978]. Nombreuses sont désormais les initiatives visant à associer les citoyens à la prise de décision. A ce titre, le numérique est un outil facilitant l'émergence d'une expression citoyenne en dehors de tout scrutin. Tel a été le cas en 2016 lorsqu'un projet de loi a fait pour la première fois l'objet d'une consultation publique sur internet[979]. Même si l'autorité publique n'est pas liée par ces contributions, il n'en demeure pas moins que ces plateformes numériques devraient respecter certains principes, y compris de transparence[980]. En ce sens, nous ne pouvons que partager l'analyse de Buge et Morio à ce sujet :

> *« (…) La sincérité implique notamment, en matière de décision publique, la reconnaissance d'un principe de transparence. Cette dernière concerne les modalités de la consultation, qui doivent être publiquement explicitées. Elle doit aussi porter sur ses résultats, qui appartiennent tant au commanditaire de la consultation qu'au public qui y a participé. Un principe d'open data est donc à affirmer. Enfin, s'agissant spécifiquement des plateformes numériques utilisées par les pouvoirs publics, la garantie minimale voudrait que, dans un domaine qui touche à l'exercice de la démocratie, les algorithmes sous-jacents (codes source) soient accessibles et étudiables, c'est-à-dire publiés en open source »*[981].

488. En effet, s'il ne fait aucun doute que les résultats sont à mettre à la disposition aussi bien des commanditaires que des participants, nous ajouterons à cela la nécessité de prévenir les erreurs de traitement[982] qui ne peuvent être décelées par la seule publication des codes sources des programmes utilisés.

---

[978] Qu'elles soient contraignantes ou non contraignantes, les consultations, notamment locales, prennent une place de plus en plus importante. Pour plus de précisions, lire RAMBAUD R., *Droit des élections et des référendums politiques*, *LGDJ*, 1e édition, 2019 ; COMBEAU P., « L'élaboration de la décision administrative à l'ère du numérique : vers l'action administrative collaborative ? », *in Le droit administratif au défi du numérique*, *AFDA*, 2019, p. 173.

[979] Le projet de loi pour une République numérique a fait l'objet d'une concertation citoyenne. Les citoyens ont été amenés à contribuer par l'intermédiaire d'une plateforme en ligne mise en place pour le gouvernement : ETAT FRANÇAIS, La loi pour une République numérique se construit avec les Français, *Le portail de la transformation de l'action publique* [en ligne]. 28 septembre 2015 [Consulté le 14 décembre 2020]. Disponible à l'adresse : https://www.modernisation.gouv.fr/outils-et-methodes-pour-transformer/la-loi-pour-une-republique-numerique-se-construit-avec-les-francais

[980] *Ibid*., principe 12.

[981] BUGE E., MORIO C., « Le Grand débat national, apports et limites pour la participation citoyenne », *RDP*, 2019, p. 1205.

[982] *Supra*., n° 13.

489. Les jeux de données doivent alors également être soumis au principe de *l'open data*, afin que ces traitements puissent être reproduits par les personnes qui le souhaiteraient. La société civile pourrait d'ailleurs jouer un rôle non négligeable dans ce processus, ce qui permettrait de discuter aussi bien les critères de l'algorithme que la qualité des données utilisées. Ce débat contradictoire sur l'interprétation des données entre les organisateurs et le public qui y a pris part, ne peut qu'être vertueuse pour la démocratie. En d'autres termes, cette mesure serait une garantie collective visant à s'assurer que les résultats soient le plus proche possible de l'opinion exprimée par les participants. La finalité est bien entendu de se prémunir des éventuelles irrégularités, ou des mauvaises interprétations qui sont amenées à fonder, voire à légitimer la mise en place d'une politique plutôt qu'une autre. La transparence des algorithmes, lorsqu'elle vient prendre sa source dans la notion de sincérité[983], se doit d'apporter les garanties à ce que le résultat soit conforme à la volonté des participants. Parce que les traitements algorithmiques revêtent une « scientificité » susceptible de légitimer bien des choix politiques, il convient de pouvoir les contester.

490. Il est également primordial de considérer que l'émergence des algorithmes auto-apprenants ouvre la voie à une vulnérabilité des citoyens, qui par leur participation à ces consultations, livrent des données politiques comportementales, c'est-à-dire leur for intérieur, aux gouvernants ainsi qu'aux sociétés privées, puisque ne l'oublions pas, le principe d'*open data* contient dans sa genèse la réutilisation de ces données, y compris à des fins commerciales[984]. Or, même si ces données sont anonymisées, ce qui ne permet pas en théorie de ré-identifier les personnes, elles permettent parfois de cerner les habitudes comportementales de groupes sociaux qui ont participé à ces contributions. En effet, il est par exemple possible de le déduire sur le fondement du profil des participants, qui lui est connu[985].

491. Il existe à notre sens, comme l'indique Antoinette Rouvroy, un risque de gouvernance par les techniques de *data mining*[986], ce qui risque de décorréler de plus en en plus le citoyen

[983] Sur le fondement de la notion de sincérité du scrutin, la notion de sincérité des débats consiste à s'assurer que les conclusions de ces débats correspondent bien à la volonté réelle des participants. *Infra.*, n° 519 et s.

[984] DECAUX M., DUVAL L., LABBAY A., PAQUIER Y., PENITOT M., « Chronique de jurisprudence des droits numériques 2017-2018 », *Cahiers de la Recherche sur les Droits fondamentaux*, n° 17, 2019, p. 217.

[985] En ce sens, le profil des participants du « Grand débat national » est connu. Voir FOURNIAU J-M., Le « grand débat national » : un exercice inédit, une audience modérée au profil socioéconomique opposé à celui des Gilets jaunes, *Observatoire des débats* [en ligne]. 11 avril 2019 [Consulté le 26 novembre 2020]. Disponible à l'adresse : https://observdebats.hypotheses.org/413

[986] « *Le data mining ou la fouille de données regroupe l'ensemble des techniques capables d'extraire de la connaissance à partir des données pour aider à la décision, en particulier celles permettant d'extraire des corrélations entre les données et celles permettant de découvrir des modèles implicites* », METAIS E., SYSTÈMES INFORMATIQUES - Systèmes d'aide à la décision, *Encyclopædia Universalis* [en ligne]. [Consulté le 10 août 2021]. Disponible à l'adresse : https://www.universalis.fr/encyclopedie/systemes-informatiques-systemes-d-aide-a-la-decision/

du débat politique. A ne pas en douter, la démocratie d'opinion déjà tant décriée, sera remplacée par cette gouvernementalité algorithmique[987] reposant sur les données comportementales de la société. Cette idée, déjà effrayante par nature, ne peut, de plus, que l'être lorsque l'exploration repose sur des données parcellaires, voire de mauvaise qualité.

492. La question des algorithmes est également centrale même si dans l'actuel champ d'étude, le résultat des algorithmes ne modifie pas l'ordonnancement juridique au premier abord. Mais c'est parce que la décision est susceptible d'avoir des incidences politiques, et donc à même de modifier l'ordonnancement juridique, que les participants doivent pouvoir garder la main sur la vérifiabilité des résultats.

2 - L'étude du principe de transparence des traitements algorithmiques : l'exemple du Grand débat national

493. Les consultations intervenues dans le cadre du Grand débat national, à la suite de la crise des gilets jaunes, remplissaient initialement certaines garanties de transparence. Cette consultation, parce qu'elle a été à l'initiative du Président de la République, dans l'urgence, ne se rattache pas à des dispositions législatives et réglementaires existantes.

494. Bien que certaines garanties aient été apportées, toutes ne sont pas particulièrement précises[988]. C'est notamment à un collège des garants du Grand débat national qu'incombait la mission d'organiser et de coordonner les consultations[989]. Et comme nous ne sommes pas en présence d'un scrutin, les garanties pouvaient très bien ne pas être identiques[990]. D'ailleurs, les

---

[987] SALMON C., « Bojo le clown » et son ingénieur magicien, *Médiapart* [en ligne]. 26 janvier 2020. [Consulté le 12 mars 2020]. Disponible à l'adresse : https://www.mediapart.fr/journal/international/260120/bojo-le-clown-et-son-ingenieur-magicien?onglet=full : « *Il vise à mettre en place ce que la philosophe du droit Antoinette Rouvroy appelle la « gouvernementalité algorithmique ». Soit « l'hypothèse d'un gouvernement du monde social fondé sur le traitement algorithmique (automatique) des données massives proliférant de nos comportements plutôt que sur la politique, le droit, les normes sociales, dans une multitude de secteurs d'activité et de gouvernement ».*
Le projet de Cummings vise à systématiser dans la décision politique l'usage du data mining (exploration de données) et de tout ce que l'on place sous le signe de l'intelligence artificielle. L'enjeu politique selon Rouvroy réside dans le fait de « sous-traiter à des machines algorithmiques la tâche de fixer à la place des normes juridiques et des choix politiques les critères de mérite, de besoin présidant à la répartition des ressources ».
Derrière ce projet d'auto-gouvernance des algorithmes, il y a l'utopie d'une disparition de l'État et d'une dépolitisation radicale de la société. Les modèles de prédiction algorithmique capables de s'autoréguler et de se corriger par des mécanismes de rétroaction se substitueraient à la délibération démocratique. ».

[988] Décret n° 2019-23 du 14 janvier 2019 instituant une mission d'organisation et de coordination du grand débat national, *Legifrance.fr* [en ligne]. Mis à jour le 16 janvier 2019. [Consulté le 20 janvier 2020]. Disponible à l'adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038002225

[989] Décret n° 2019-61 du 31 janvier 2019 instituant un collège des garants du grand débat national, *Legifrance.fr* [en ligne]. Mis à jour le 1er février 2019. [Consulté le 20 avril 2021]. Disponible à l'adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038081366

[990] *Infra.*, n° 519 et s.

garants ont considéré sur la base de la lettre du Président de la République[991] et des textes mettant en œuvre le Grand débat, que quatre principes devaient guider ce dernier[992]. Parmi ces quatre principes, nous y trouvons la transparence : l'objectif de cette transparence étant d'établir la confiance en communiquant toutes les informations et les données permettant aux citoyens « *de vérifier par eux-mêmes l'ensemble du dispositif, depuis la collecte de la parole citoyenne jusqu'à sa restitution* »[993]. Fallait-il pour autant en déduire qu'une transparence accrue serait assurée ?

495. Ainsi, ce collège,

> « *est chargé de veiller au respect des exigences d'impartialité et de transparence dans l'organisation et le déroulement du grand débat national. Il examine notamment les modalités d'organisation et les travaux d'analyse et de synthèse des contributions recueillies. Il formule les recommandations qu'il juge nécessaires au titre de sa mission* »[994].

496. Ce garant est alors institué en tant que tiers de confiance au bon déroulement et à l'organisation du Débat national. Il ne s'agit donc pas d'une transparence directe vis-à-vis des participants, mais indirecte. Mais il est surtout, et c'est ce qui retient particulièrement notre attention, garant des travaux et de la synthèse des contributions recueillies dans le cadre du Grand débat. Ce climat de défiance, sans doute alimenté par l'absence d'une transparence directe, s'est notamment illustré lorsqu'une plateforme concurrente, appelée « *Le Vrai Débat* », a été mise en ligne par certains « Gilets jaunes »[995].

497. Ces garanties sont d'autant plus essentielles dans un contexte de défiance où les autorités publiques sont aujourd'hui concurrencées par les plateformes privées ; plateformes sur lesquelles s'exercent également le militantisme politique. Il est sans doute utile de rappeler que le mouvement des « Gilets jaunes » a notamment pu émerger sur *Facebook*, et que bien des données sensibles relatives à des opinions politiques des participants sont désormais entre les

---

[991] ETAT FRANÇAIS, Grand débat national : la lettre aux Français du président de la République, *Site du Gouvernement français* [en ligne]. 13 janvier 2019 [Consulté le 22 novembre 2020]. Disponible à l'adresse : https://www.gouvernement.fr/grand-debat-national-la-lettre-aux-francais-du-president-de-la-republique

[992] Nous y retrouvons la transparence, l'impartialité, l'inclusion et la neutralité des débats, voir en ce sens BAILLY J-P., BELLAOUI N. et al., Rapport du Collège des garants du grand débat national, p. 7, *Grand Débat.fr* [en ligne]. 9 avril 2019. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://granddebat.fr/media/default/0001/01/ee2712c96c5035c3c2913174a7b5535fc52642a4.pdf

[993] *Ibid,*.

[994] Décret n° 2019-61 du 31 janvier 2019 instituant un collège des garants du grand débat national, *op. cit.*, art. 2.

[995] LE VRAI DEBAT, Site participatif réalisé par un collectif de gilets jaunes de différentes régions de France [en ligne]. [Consulté le 2 juillet 2021]. Disponible à l'adresse : https://www.le-vrai-debat.fr/

mains de cette plateforme[996]. L'enjeu est donc de taille, y compris en matière de transparence, pour rétablir la confiance et permettre une contribution politique respectant les principes fondamentaux de la participation citoyenne, voire les renforcer, en y appliquant les principes du scrutin électronique[997] (sincérité, transparence, vérifiabilité, secret). Or, le collège, en l'absence de base légale et réglementaire, a été libre de poser les garanties qu'il a jugées opportunes[998]. La difficulté est que d'une concertation à l'autre, les garanties de transparence des plateformes numériques divergent en la matière.

498. Cette transparence devait être réalisée par la mise en ligne en *open data* des jeux de données des contributions du Grand débat national[999], ce qui a partiellement été réalisé sur la plateforme Etalab. Mais tous les jeux de données n'ont à ce jour pas été mis en ligne, officiellement pour des raisons techniques[1000]. La numérisation des cahiers de doléance a par exemple nécessité une logistique importante.

499. Ces mécanismes, parce qu'ils visent à compléter la représentation, et donc l'exercice de la souveraineté politique, doivent faire l'objet d'une transparence accrue, et ce bien entendu dans le respect des données à caractère personnel. Cette transparence ne doit pas servir à générer un fichage politique des participants. En effet, l'excès de transparence est parfois pointé du doigt comme étant l'apanage des régimes totalitaires. Or, la transparence dont nous nous réclamons, n'est pas la transparence des personnes, mais des outils utilisés.

500. Les algorithmes opérant les synthèses de ces débats sont tout aussi importants que les données collectées.

501. Nous retrouvions déjà certains éléments dans le document « Pour une action publique transparente et collaborative : plan d'action national pour la France 2015-2017 »[1001]. L'engagement 12 précise que « *la consultation des citoyens sur les projets de loi ou en amont*

[996] ERTZSCHEID O., Avec les gilets jaunes, Facebook dispose d'une formidable base de données d'opinion, *Alternatives économiques* [en ligne]. 13 décembre 2018 [Consulté le 29 novembre 2020]. Disponible à l'adresse : https://www.alternatives-economiques.fr/gilets-jaunes-facebook-dispose-dune-formidable-base-de-donnees/00087367
[997] *Infra*., n° 538 et s.
[998] BAILLY J-P., BELLAOUI N. et al., Rapport du Collège des garants du grand débat national, *op. cit.*, p. 17.
[999] *Ibid*.
[1000] CORI N., Grand débat : l'illusion perdue de l'open data, *Les jours* [en ligne]. 3 janvier 2020 [Consulté le 23 octobre 2020]. Disponible à l'adresse : https://lesjours.fr/obsessions/gilets-jaunes/ep43-grand-debat-resultats/ ; CORI N., A la recherche des doléances perdues, *Les jours* [en ligne]. 18 juillet 2021 [Consulté le 23 octobre 2020]. Disponible à l'adresse : https://lesjours.fr/obsessions/cahiers-doleances-grand-debat/ep1-gilets-jaunes/
[1001] ETAT FRANÇAIS, Pour une action publique transparente et collaborative : plan d'action national pour la France, engagement n° 12, p. 31, *Modernisation.gouv.fr* [en ligne]. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.modernisation.gouv.fr/sites/default/files/fichiers-attaches/pgo_plan_action_france_2015-2017_fr.pdf

de leur préparation peut permettre de bâtir une décision publique et une législation efficace et de revitaliser la démocratie ».

502. Le rapport du Collège des garants du Grand débat national en date du 9 avril 2019 reprend d'ailleurs certaines recommandations visant à assurer la loyauté du traitement[1002]. Il nous semble important de rappeler que la loyauté telle qu'entendue, concourt à la transparence que nous étudions, car, à défaut de transparence absolue, elle est censée « responsabiliser » les acteurs au sujet des traitements qu'ils opèrent. Mais la loyauté n'est pas la transparence, et cette notion, traditionnellement civiliste que nous avons étudié dans le cadre du premier chapitre de ce titre[1003], offre une latitude considérable au responsable du traitement du Grand débat, et ne sert absolument pas la conformité de ces traitements avec la promesse des organisateurs de cette consultation, à savoir que les participants devaient avoir la capacité de vérifier par eux-mêmes la collecte et les traitements algorithmiques effectués.

503. A défaut de pouvoir fournir une transparence absolue aux participants, les garants avaient vu dans la mise à disposition des données une garantie de loyauté du traitement, notamment car elle permettrait à tout acteur de proposer une analyse alternative des contributions[1004].

504. Cela étant, la publication des données ne peut-être une fin en soi, ne serait-ce parce que la publication des données, bien que demeurant encore incomplète, ne comprend pas la communication des algorithmes utilisés dans le cadre de ces traitements. Comme nous le verrons plus tard, et nous le comprenons tout à fait, le code source et les caractéristiques des algorithmes utilisés dans le cadre du Grand débat national sont soumis à la propriété intellectuelle, et ne peuvent être de ce fait être communiqués, en raison notamment du secret des affaires.

505. Le traitement des questions fermées ne semble pas avoir posé tant de difficultés dans la mesure où les occurrences ont été comptabilisées afin de réaliser les résultats sous forme de pourcentage. En revanche, pour les questions ouvertes, la difficulté est tout autre. En effet, les

---

[1002] Le point III du Rapport est intitulé « traitement et une restitution crédible ». BAILLY J-P., BELLAOUI N. et al., Rapport du Collège des garants du grand débat national, *op. cit.*

[1003] *Supra.*, n° 266 et s.

[1004] « *l'ouverture des données a constitué une garantie a priori de loyauté du traitement et de restitution finale dès lors qu'elle revenait, pour le gouvernement, à se dessaisir volontairement du monopole sur l'analyse du grand débat : tout acteur a en effet la possibilité de produire une analyse alternative des données du grand débat et de contester, le cas échéant, tel ou tel aspect de l'analyse proposée par les organisateurs. Cette exposition délibérée à la critique constitue un gage particulièrement fort de crédibilité.* », BAILLY J-P., BELLAOUI N. et al., Rapport du Collège des garants du grand débat national, *op. cit.*, p. 16.

analyses textuelles performantes nécessitent le recours à des technologies plus poussées, ne serait-ce car le langage naturel doit être interprété par la machine pour formuler un résultat. C'est une société privée, la société QWAM[1005], qui a été chargée d'interpréter les questions ouvertes. Concernant le volet technique de ces algorithmes, il s'agit en l'espèce d'outils d'analyse automatique des données textuelles recueillies dans le cadre du Grand débat. Selon le document[1006], les techniques utilisées recourraient aussi bien à des traitements d'analyse du langage naturel par des algorithmes classiques, qu'à des algorithmes auto-apprenants. L'une des garanties apportées est qu'une intervention humaine a lieu afin de s'assurer que les résultats sont cohérents et que les analyses sont conformes à ce qui a été exprimé par les participants[1007]. Mais nous pouvons considérer que les éléments communiqués aussi bien par *OpinionWay* que par le Collège du Grand débat national sont insuffisants à garantir une transparence des outils utilisés alors même que la transparence des traitements était l'un des critères fixés par ledit Collège[1008]. Cette opacité s'explique du fait du caractère secret de ces technologies. A défaut de transparence directe, assurant la préservation de la crédibilité du traitement de ces données, les garants ont missionné un Collège de scientifique composé d'experts de l'INRIA et du CNRS. Sans plus de précisions, il est ressorti « *des échanges croisés avec ces scientifiques et les prestataires de la Mission du grand débat que ces méthodes présentaient un niveau satisfaisant de crédibilité* »[1009]. Les prestataires devaient également publier, en vertu du principe de transparence, *« une documentation consolidée qui retrace et explicite leurs arbitrages au cours du traitement. Ces documents permettront à tous de juger la qualité du travail accompli en rendant « vérifiable » l'analyse ainsi menée »*[1010]. Or, à ce jour, ce document n'a toujours pas été communiqué. Or, quand bien même les critères ont été déclarés à ce Collège, rien ne démontre qu'il s'agit des critères vraiment utilisés. On peut tout à fait imaginer qu'en fonction des méthodes d'analyse, les résultats puissent varier. C'est d'ailleurs le but de l'IA que de s'améliorer en fonction des données scrutées, et ce en permanence.

506. La promesse n'ayant pas été tenue, nous ne pouvons donc que nous prononcer en faveur de l'utilisation d'algorithmes libres afin qu'ils soient communiqués et étudiés. La consultation

[1005] Selon le document d'Opinion Way : « *La technologie de QWAM permet de traiter l'exhaustivité des verbatim. Grâce à des algorithmes puissants, les notions citées par les répondants sont relevées, analysées, triées et classées en différentes catégories et sous-catégories.* ». p. 2. OPINION WAY, Analyse des contributions au Grand Débat National : Q&A, *Site d'Opinion Way* [en ligne]. 15 février 2019 [Consulté le 2 mars 2021]. Disponible à l'adresse : https://www.opinion-way.com/fr/mediatheque/presse/opinionway-q-a-sur-l-analyse-des-contributions-grand-debat-national-15-fevrier-2019/viewdocument.html
[1006] *Ibid.*
[1007] *Ibid.*
[1008] *Supra.*, n° 494.
[1009] BAILLY J-P., BELLAOUI N. et al., Rapport du Collège des garants du grand débat national, *op. cit., p. 17.*
[1010] *Ibid.*

publique relative à la réforme des retraites a également fait l'objet d'un traitement par la société *OpinionWay* alors que la méthodologie n'a pas davantage été explicitée[1011], ce qui n'est pas sans poser des questions démocratiques.

507. A défaut d'obtenir la communication des codes sources des programmes utilisés, la mise en ligne des jeux de données avait pour vocation à ce que tout acteur puisse lui-même vérifier les résultats[1012]. Or, force est de constater que, d'une part, peu sont les acteurs à bénéficier des moyens techniques permettant de vérifier les résultats, surtout pour les questions ouvertes traitées par des algorithmes auto-apprenants, qui comme nous l'avons déjà rappelé, sont de plus des technologies opaques dans la manière dont ils obtiennent des résultats, même quand ces outils sont communiqués. En effet, les techniques d'IA sont opaques par nature, ce qui leur vaut l'appellation de boîte noire*[1013]*.

508. Il serait opportun que les données soient publiées avant que ne soient restituées les synthèses afin que des associations ou des laboratoires universitaires intéressés puissent également mener des travaux, dans le même temps, afin de constater si leurs résultats corroborent ceux des études des concertations publiques. En effet, si les travaux de vérification ont lieu plusieurs mois après, voire années, il sera difficile de contester l'étude, qui elle-même aura déjà sans doute produit des effets politiques, et donc modifié, le cas échéant l'ordonnancement juridique. Il conviendrait également que les données brutes[1014] soient publiées afin de s'assurer que les données finalisées par le prestataire mandaté soient conformes à la réalité.

509. Pour conclure, il convient de considérer qu'il existe plusieurs chemins. D'une part, il s'agirait de rapprocher l'encadrement juridique du recours à ces consultations publiques de celui des sondages électoraux. En effet, les sondages électoraux sont soumis en France à un régime juridique particulier, y compris de transparence, parce que ces derniers sont susceptibles d'altérer la sincérité du scrutin[1015]. D'autre part, au-delà des considérations pures de

---

[1011] ETAT FRANÇAIS, Conclusions de la concertation sur la mise en place d'un système universel de retraite, p. 23, *Participez.reforme-retraite.gouv.fr* [en ligne]. [Consulté le 12 mars 2021]. Disponible à l'adresse : https://participez.reforme-retraite.gouv.fr/media/default/0001/01/052fe41833cdf2384392e4e0f243bebe417f7d81.pdf

[1012] BAILLY J-P., BELLAOUI N. et al., Rapport du Collège des garants du grand débat national, *op. cit.,* p. 17.

[1013] *Supra*., n° 16.

[1014] Il convient d'entendre par données brutes, les documents originaux qui ont soient fait l'objet d'une dématérialisation ou les données n'ayant pas encore été traitées par le prestataire.

[1015] Bien que l'encadrement juridique des sondages électoraux soit imparfait, il dénote l'importance de rendre transparent la méthodologie et les données des sondages en vertu du principe de sincérité du scrutin. En ce sens, voir la loi n° 77-808 du 19 juillet 1977 *relative à la publication et à la diffusion de certains sondages d'opinion* telle que modifiée par la loi n° 2016-508 du 25 avril 2016 *de modernisation de diverses règles applicables aux élections* ; Pour plus de précisions, voir RAMBAUD R., *Droit des élections et des référendums politiques*, *op. cit*., p. 581 à 584.

transparence, sonder le for intérieur des citoyens n'est pas sans risque sur la démocratie comme l'indique Antoinette Rouvroy. Nous ne pouvons donc que nous demander s'il ne conviendrait pas mieux d'interdire ces usages, ou du moins le recours aux technologies d'IA, dans le cadre de ces consultations.

B - Représentation et traitements algorithmiques

510. Indépendamment des aspects relatifs à la démocratie participative, les gouvernants se fondent également de plus en plus sur des traitements algorithmiques dans l'élaboration des normes. L'immixtion des algorithmes dans le travail normatif est certaine et doit à cet égard répondre à des exigences de transparence.

1 - Le travail parlementaire et gouvernemental

511. Les programmes informatiques sont d'ores et déjà utilisés afin d'évaluer les incidences des éventuelles réformes législatives. Il s'agit ici d'un outil de « gouvernance par les nombres »[1016] bien que nous n'ignorions pas que des réformes économiques reposent nécessairement sur des sciences économiques et sociales. Mais comme dans toute science, les modèles doivent pouvoir être discutés, surtout lorsqu'ils inspirent des réformes qui ont une incidence sur la vie des personnes. A certains égards, il s'agit d'un outil prédictif, car l'issue de la simulation n'est pas pour autant certaine, mais elle va influencer les travaux préparatoires sur le projet de texte. Ces outils sont relativement secrets, justement parce qu'ils ne sont pas communiqués. Et lorsqu'ils le sont, ils ne le sont pas toujours de manière intelligible.

512. Comme nous l'avons vu dans le cadre de la première section[1017], certains programmes sont déjà utilisés en France à cette fin[1018]. Ces outils demeurent toutefois opaques. En effet, dans certains cas, ils ne sont pas communicables parce qu'ils sont soumis au secret des délibérations, dans les hypothèses où ils s'inscrivent dans un processus décisionnel indissociable d'une initiative politique du Gouvernement[1019]. Les codes sources avaient

[1016] Pour reprendre l'ouvrage de SUPIOT A., *La gouvernance par les nombres*, *op. cit*.
[1017] *Supra*., n° 428.
[1018] Parmi les logiciels dont la communication du code source a été demandée, nous retrouvons le logiciel SAPHIR qui est utilisé « *notamment afin de réaliser des évaluations de la législation fiscale dans le domaine social* ». Le programme Mésange est de « *réaliser des évaluations ex ante de l'impact de différentes mesures de politique économique sur l'emploi, le produit intérieur brut ou les prix* ». Pour finir, le logiciel Opale « *est un modèle utilisé pour prévoir les principales variables macroéconomiques (croissance du produit intérieur brut, consommation, investissement) sur une ou deux années* », CADA, avis n° 20180276 du 19 avril 2018.
[1019] *Ibid*.

toutefois finalement été diffusés publiquement sur le site internet de la Direction générale du Trésor le 5 septembre 2018[1020], mais la documentation s'y afférant, comme l'avait pourtant prévu le Gouvernement, n'a pas été communiquée, ce qui rend la compréhension des codes sources difficiles[1021] comme nous l'avons déjà évoqué.

513. Bien que la transparence des algorithmes n'ait pas pour prétention de rendre transparent tout ce qui ne l'était pas auparavant, lorsque l'outil existe et qu'il fait revêtir une « scientificité » à toute démarche, il doit être expliqué. En ce sens, la députée Paula Forteza s'était prononcée en faveur de l'ouverture de ces simulateurs[1022]. Un sénateur, Vincent Eblé, a même déposé un amendement allant dans le sens de la publication des codes sources, s'appliquant à chaque projet de loi de finance ou loi de finance rectificative[1023]. Cet amendement adopté en première lecture n'a finalement pas été retenu dans le texte final, alors qu'il allait plus loin que la LRN sur ce sujet puisqu'il demandait la communication des documents suivants :

> « *(…) 1° le code source correspondant à l'ensemble des dispositions législatives et réglementaires en vigueur pour cette imposition et des instructions et circulaires publiées par l'administration qui portent sur cette imposition ;*
>
> *2° le code source correspondant aux dispositions législatives proposées et, à titre facultatif, aux dispositions réglementaires, instructions et circulaires envisagées ;*
>
> *3° les données synthétiques et les hypothèses retenues pour évaluer les conséquences économiques, financières, sociales et environnementales, ainsi que des coûts et bénéfices financiers attendus des dispositions envisagées pour chaque catégorie d'administrations publiques et de personnes physiques et morales intéressées, en indiquant la méthode de calcul retenue* ».

514. L'objectif à terme est de permettre également aux citoyens d'utiliser eux-mêmes ces outils, notamment afin qu'ils prennent part à une consultation citoyenne portant sur la dépense

[1020] CADA, avis n° 20180276 du 19 avril 2018. TRESOR DIRECTION GENERALE, La DG Trésor met à la disposition du public les codes sources des modèles Mésange, Opale et Saphir, *op. cit.*
[1021] BERNE X., Sous pression, Bercy ouvre les codes sources des modèles Mésange, Opale et Saphir, *op. cit.*
[1022] ASSEMBLEE NATIONALE, 2e Conférence des réformes, Propositions des groupes de travail, *Assemblee-nationale.fr* [en ligne]. Juin 2018 [Consulté le 12 mai 2021]. Disponible à l'adresse : http://www2.assemblee-nationale.fr/static/reforme-an/democratie/Rapport-2-GT6-democratie.pdf
[1023] EBLE M., Amendement Article additionnel n° II-682 au projet de loi de finances pour 2018, session ordinaire 2017-2018, Sénat, enregistré à la Présidence du Sénat le 6 décembre 2017, *Senat.fr* [en ligne]. 6 décembre 2017 [Consulté le 12 décembre 2020]. Disponible à l'adresse : http://www.senat.fr/amendements/2017-2018/107/Amdt_II-682.html

publique sur cette base[1024]. Une fois de plus nous recommandons que ces outils soient libres[1025] pour plus de transparence. Ces programmes pourraient également être utilisés par les parlementaires lors des débats ou du travail en commission. Cette idée est désormais proposée par l'Assemblée nationale qui autorise le développement d'un outil libre offrant aux députés d'estimer l'impact des réformes qu'ils discutent[1026]. Il est également important, comme nous le rappelons, que cet outil puisse être débattu, aussi bien dans sa conception, que dans les données qu'il utilise. Dans la mesure où il est question que ce programme aide la représentation nationale dans les choix à opérer, il est impératif que l'outil soit le moins faussé possible et puisse être représentatif des théories scientifiques élaborées dans ces domaines.

515. La multiplication des logiciels comme aide à la prise de décision doit servir le débat, ce qui nécessite que ces outils soient intelligibles pour les Parlementaires. Il en va du respect du principe de clarté et de sincérité du débat parlementaire pour que les discussions continuent de contribuer à forger la volonté générale qui ne peut se former que par la confrontation des idées contradictoires et du pluralisme[1027]. Il est impératif d'éviter que ces discussions démocratiques se limitent à une logique de « gouvernance par les nombres », faisant prévaloir l'idée selon laquelle les outils informatiques seraient neutres, et dont les conclusions seraient incontestables[1028]. La clarté et la sincérité des débats parlementaires doivent également servir la transparence des travaux de ces derniers, pour que les citoyens s'approprient le fondement des décisions de la représentation nationale.

2 - L'évaluation des politiques publiques

516. Les algorithmes sont également amenés à jouer un rôle important dans l'évaluation des politiques publiques[1029], c'est-à-dire en aval de la prise de décision publique. C'est effectivement ce que révèle une étude annuelle du Conseil d'Etat dédiée à cette question[1030],

---

[1024] *Ibid*.
[1025] Par opposition aux logiciels propriétaires dont les codes sources ne peuvent être communiqués parce que des droits d'auteur sont en cause.
[1026] ETAT FRANÇAIS, LexImpact, Aider nos parlementaires à estimer les impacts de leurs amendements avant vote !, *Beta.gouv.fr* [en ligne]. [Consulté le 2 janvier 2021]. Disponible à l'adresse : https://beta.gouv.fr/startups/leximpact.html
[1027] Le principe de sincérité de clarté et du scrutin. En ce sens, lire BRUNESSEN B., « L'exigence de clarté et de sincérité du débat parlementaire. Etude sur un concept régulateur de la procédure législative sous la Ve République », *RDP*, 2011, p. 431.
[1028] En effet, il est nécessaire de rappeler que les algorithmes ne sont pas neutres et qu'ils ne peuvent l'être. En ce sens, CARDON D., « Le pouvoir des algorithmes », *op. cit*.
[1029] Traditionnellement c'est au titre de l'article 24 de la Constitution du 4 octobre 1958 que le Parlement évalue les politiques publiques. Mais la société civile participe également de plus en plus à cette tâche.
[1030] CONSEIL D'ETAT, *Etude annuelle, Conduire et partager l'évaluation des politiques publiques, La documentation française*, 2020, p. 28

mais aussi un Rapport de l'Assemblée nationale en date du 15 mars 2018[1031]. Ce dernier met en avant que le numérique est une opportunité ouvrant la voie, grâce au *big data*, à une évaluation plus pertinente des politiques publiques. L'objectif est notamment que le citoyen puisse se positionner en tant qu'évaluateur. Tout cela ne peut s'inscrire que dans le cadre de la politique d'*open data* qui vise à libérer les données afin qu'elles soient réutilisées. En ce sens, l'une des propositions du rapport est de confier à Etalab la « *conception d'une application permettant aux citoyens d'évaluer les politiques publiques du quotidien* »[1032]. La transparence doit alors être accrue au sujet de ces outils qui sont à même d'altérer la sincérité des débats[1033], si les critères et les données ne peuvent pas être contestés par des études contradictoires. En effet, ces outils étant complexes à appréhender pour la plupart des citoyens, parce qu'ils sont clés en main et que nous n'avons pas tous des connaissances techniques en la matière, nous n'avons pas le moyen de nous assurer que les résultats sont corrects. La sincérité du scrutin pourrait alors être altérée par des données partielles et/ou de mauvaise qualité, renvoyant à une image erronée du réel. Dans ce cas de figure, la transparence contribuerait à réduire les risques d'altération du scrutin en période électorale, dans le prolongement de la loi *relative à la lutte contre la manipulation de l'information*[1034]. Il nous semble également opportun que ces opérations soient mises en place et contrôlées par une AAI, ce qui sera explicité dans la seconde partie de cette thèse[1035].

3 - Le cas particulier de la transparence des modèles prédictifs utilisés dans le cadre de l'urgence sanitaire pour fonder des décisions politiques

517. La pandémie de SARS-COV-2 a notamment d'inédit qu'elle a été observée par des moyens techniques permettant d'identifier l'arrivée du virus sur notre territoire et d'en évaluer sa dynamique. Naturellement, dans un premier temps, la qualité des données était très discutable. Dès janvier 2020 des chercheurs de l'Institut National de la Santé Et de la Recherche Médicale (INSERM) ont proposé un « outil théorique d'aide à la décision publique ». Les

[1031] MOREL-A-L'HUISSIER P., PETIT V., Rapport d'information sur l'évaluation des dispositifs d'évaluation des politiques publiques de l'Assemblée nationale, 15e législature, fait au nom du comité d'évaluation et de contrôle des politiques publiques, enregistré à la Présidence de l'Assemblée nationale le 15 mars 2018., proposition 13, [en ligne]. 15 mars 2018. [Consulté le 12 juin 2020]. Disponible à l'adresse : http://www.assemblee-nationale.fr/15/rap-info/i0771.asp#P967_212715
[1032] *Ibid.*
[1033] Sur la question de l'altération de la sincérité du scrutin, notamment dans la lutte contre les fausses informations : Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information ; CC, décision n° 2018-773 DC, 20 décembre 2018, *Loi relative à la lutte contre la manipulation de l'information* ; CC, décision n° 2018-774 DC, 20 décembre 2018, *Loi organique relative à la lutte contre la manipulation de l'information* ; MONTECLER M-C., « Le Conseil constitutionnel définit la manipulation de l'information », *AJDA*, 2019, p. 5.
[1034] *Infra.*, n° 521 et s.
[1035] *Infra.*, n° 717 et s.

scénarios envisagés par l'outil considéraient que le risque d'importation sur le territoire européen du virus provenant de Chine était faible à court terme[1036].

518. Qu'il s'agisse du gouvernement ou du Conseil scientifique chargé de le conseiller, les modèles épidémiologiques ont joué un rôle significatif dans les décisions prises puisqu'il s'agissait des seuls indicateurs permettant d'anticiper la dynamique épidémique, alors que ces outils sont cantonnés à l'état de l'art sur la connaissance du virus ainsi qu'à la politique de dépistage mise en œuvre qui a été relativement variable d'une période à l'autre. Ainsi, ces modèles prédictifs étant susceptibles de fonder des décisions politiques avec un fort impact sur l'exercice des droits et libertés, l'acceptabilité de ces mesures ne peut reposer que sur une transparence de ces outils et de leurs données. En ce sens, la mission menée par Eric Bothorel recommande la publication de ces modèles dans une approche « pédagogique et collaborative »[1037]. Il convient par ailleurs d'ajouter qu'une telle transparence doit être assurée vis-à-vis de l'Etat qui est susceptible de se retrouver dans une situation de vulnérabilité au regard de ces outils, et particulièrement lorsqu'il n'a pas accès à ces informations, notamment parce que certains d'entre eux seraient propriétaires[1038].

PARAGRAPHE 2 - Algorithmes et période électorale

519. Force est de constater que les algorithmes sont désormais au cœur de la diffusion de l'information sur les plateformes en ligne, ce qui est à même d'altérer la sincérité du scrutin lorsque de fausses informations y sont véhiculées (A). En effet, ces plateformes sont désormais devenues un canal classique d'information des citoyens sur lequel s'exerce également le militantisme politique. Même s'il est désormais envisagé dans la proposition de la Commission européenne relative au marché intérieur des services numériques d'appréhender la manipulation intentionnelle à des fins électorales[1039], y compris par les algorithmes, le droit national est déjà intervenu en la matière.

[1036] INSERM, Coronavirus : des chercheurs de l'Inserm proposent un modèle pour estimer le risque d'importation de l'épidémie en Europe, *Site de l'Inserm* [en ligne]. 24 janvier 2020 [Consulté le 2 mars 2020]. Disponible à l'adresse : https://presse.inserm.fr/coronavirus-des-chercheurs-de-linserm-proposent-un-modele-pour-estimer-le-risque-dimportation-de-lepidemie-en-europe/38000/

[1037] BOTHOREL E., COMBES S., VEDEL R., Pour une politique publique de la donnée, *op. cit*., p. 47.

[1038] Voir en ce sens, DOUVILLE T., HERVOCHON C., NOEL E., PAQUIER Y., « Les vulnérabilités numériques », *op. cit*., p. 117.

[1039] L'article 26 (c) de la proposition de règlement européen du Parlement européen et du Conseil relatif à un marché intérieur des services numériques en date du 15 décembre 2020 évoque une évaluation des risques pour les très grandes plateformes en ligne parmi laquelle nous retrouvons « *la manipulation intentionnelle de leur service, y compris via l'utilisation non authentique ou l'exploitation automatisée de leur service, avec un effet négatif avéré ou prévisible sur la protection de la santé publique, des mineurs, du discours civique, ou des effets avérés ou prévisibles en lien avec les processus électoraux et la sécurité publique* ».

520. Ils sont également d'autant plus problématiques lorsque nous les autorisons à intervenir dans les opérations de vote lors des scrutins à travers les machines à voter ou encore dans le cadre du vote électronique à distance (B). Dans ces deux cas de figure, la transparence des algorithmes est au cœur de la confiance que les citoyens peuvent avoir dans la démocratie[1040].

A - Information et altération de la sincérité du scrutin

521. L'avènement des plateformes en ligne, par leurs caractéristiques techniques[1041], modifient la propagation classique des idées. Ces opérateurs[1042], qu'ils s'agissent des réseaux sociaux, mais également des moteurs de recherche par exemple, sont désormais utilisés aussi bien comme source d'information que comme espace de militantisme politique, et donc potentiellement comme relais massif à de fausses informations. Bien que nous ayons déjà abordé certaines de ces questions dans le cadre du chapitre précédent[1043], il convient de s'intéresser à la transparence de ces algorithmes en période électorale.

522. L'élection de Donald Trump en 2016 à la Présidence des Etats-Unis d'Amérique, a mis en exergue, notamment par l'intermédiaire du scandale *Cambridge analytica*[1044], que la manipulation du corps électoral par des contenus véhiculés sur les plateformes en ligne était possible. Le législateur, à la suite d'un débat politique houleux parce que nombreux de ces dispositifs étaient jugés liberticides, a finalement décidé que traiter la propagande électorale uniquement sous l'angle des candidats n'était guère suffisant et qu'il convenait désormais de se saisir de ce nouvel espace[1045], ce qui est chose faite depuis la loi n° 2018-1202 du 22 décembre 2018 *relative à la lutte contre la manipulation de l'information***.**

[1040] Nous n'aborderons pas les dispositions de l'article L. 2122-10-7 et R. 2122-53 à 55 du Code du travail relatif au vote électronique pour les élections syndicales dans la mesure où elles n'évoquent pas la transparence de ces systèmes à l'exception de l'exigence d'une expertise indépendante. Les réflexions qui seront toutefois amenées dans ce cadre sont susceptibles de s'y appliquer.

[1041] ERTZSCHEID O., Trump, Google, l'idiot utile, les architectures techniques toxiques et le meilleur des algorithmes possibles, *Affordance.info, Le blog d'un maître de conférences en sciences de l'information* [en ligne]. 17 décembre 2018 [Consulté le 3 mars 2020]. Disponible à l'adresse : https://www.affordance.info/mon_weblog/2018/12/meilleur-algorithmes-possibles-trump-idiot.html

[1042] Pour reprendre les propos du commentaire de la décision du Conseil constitutionnel relatif aux décisions n° 2018-773DC et n° 2018-774DC du 20 décembre 2018, p. 2. : *« La définition ainsi retenue vise, à la fois, des moteurs de recherche (comme Google ou Qwant), des sites de référencement (comme Lafourchette ou Tripadvisor), des « places de marchés » (comme Amazon, Leboncoin ou Airbnb) ou des réseaux sociaux (comme Facebook ou Twitter).* ».

[1043] *Supra.*, n° 260 et s.

[1044] L'EXPRESS.FR, Election de Trump : le hold-up de Cambridge Analytica sur les usagers de Facebook, *Page Actualités du site L'Express* [en ligne]. 18 mars 2018 [Consulté le 2 mai 2020]. Disponible à l'adresse : https://www.lexpress.fr/actualite/monde/amerique-nord/election-de-trump-le-hold-up-de-cambridge-analytica-sur-les-usagers-de-facebook_1993257.html. La société *Cambridge analytica* a traité les données Facebook de nombreux utilisateurs dans le but de modifier leur comportement de vote aux élections américaines de 2016.

[1045] RAMBAUD R., *Droit des élections et des référendums politiques, op. cit.*, p. 579.

523. Nous ne traiterons que des dispositions de cette loi[1046] relatives à la transparence du traitement de l'information par les plateformes en ligne[1047], visant à empêcher l'altération de la sincérité du débat ainsi que du scrutin[1048]. Deux dispositifs attirent notre attention : d'une part la disposition de l'article L. 163-1 du Code électoral[1049] qui instaure des obligations de transparence aux plateformes portant sur les contenus publicitaires qu'elles diffusent en lien avec la campagne électorale[1050], et d'autre part, l'article 11 de la loi étudiée mettant en place une obligation de transparence spécifique aux algorithmes utilisés par les plateformes dans la lutte contre les fausses informations, y compris en période électorale.

524. Ces deux régimes juridiques posent des obligations renforcées de transparence aux plateformes[1051].

1 - La propagande électorale véhiculée par les publicités soumises aux utilisateurs des plateformes (l'article L. 163-1 du Code électoral)

525. Ces obligations ne s'appliquent que *« pendant les trois mois précédant le premier jour du mois d'élections générales et jusqu'à la date du tour de scrutin où celles-ci sont acquises* »[1052].

526. Bien que ces dispositions ne fassent pas explicitement état d'une transparence des algorithmes, c'est bel et bien par leur intermédiaire que les contenus de propagande électorale sont véhiculés sur ces plateformes. L'objectif est de s'assurer que l'utilisateur, et donc le citoyen potentiel, ne sera pas influencé dans son expression le jour du scrutin. C'est donc au regard *« de l'intérêt général attaché à l'information éclairée des citoyens en période électorale et à la sincérité du scrutin* »[1053] que ces dispositions se justifient. Les plateformes en ligne telles que

[1046] Nous ne traiterons donc pas l'article L. 163-2 du Code électoral qui met en place un référé pour **«** *les allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir sont diffusées de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne* ». Bien que cette procédure puisse mettre fin à la diffusion de contenus véhiculés par des algorithmes, elle n'est pas mise en œuvre par un algorithme, mais elle est ordonnée par le juge des référés.
[1047] Il convient d'entendre par plateforme en ligne, les opérateurs qui sont définis à l'article L. 111-7 du Code de la consommation et dont le nombre de connexions sur le territoire nationale est supérieure à cinq millions par mois. *Supra.,* n° 266.
[1048] L. 163-1 du code électoral : *« au regard de l'intérêt général attaché à l'information éclairée des citoyens en période électorale et à la sincérité du scrutin ».*
[1049] Ce dispositif s'applique aux élections législatives, sénatoriales ainsi qu'à l'élection présidentielle par l'intermédiaire de loi organique n° 2018-1201 du 22 décembre 2018 *relative à la lutte contre la manipulation de l'information.*
[1050] CC, décision n° 2018-773 DC, 20 décembre 2018, *Loi relative à la lutte contre la manipulation de l'information*, § 8.
[1051] Ces obligations d'informations sont renforcées par rapport aux dispositions déjà mises en place par le Code de la consommation. *Supra.*, 260 et s.
[1052] Art. L. 163-1 du Code électoral.
[1053] *Ibid.*

définies à l'article L. 111- 7 du Code de la consommation[1054] dont le nombre de connexions *« est fixé à cinq millions de visiteurs uniques par mois, par plateforme, calculé sur la base de la dernière année civile »*[1055] doivent d'une part préciser à l'utilisateur, par l'intermédiaire d'une information loyale, claire et transparente, l'identité de la personne (morale ou physique) ou de celle pour laquelle elle agit, dès lors que la promotion d'un contenu « *d'information se rattachant à un débat d'intérêt général »* a donné lieu, en contrepartie, à une rémunération[1056] ; et d'autre part, expliciter la manière dont les données à caractère personnel de l'utilisateur ont été utilisées dans le cadre de la promotion des contenus précités[1057]. Enfin, ces opérateurs, lorsque la rémunération atteint un montant de 100 euros HT pour la promotion d'un contenu d'information se rattachant à un débat d'intérêt général, doivent rendre public le montant des sommes perçues[1058].

527. Toutes ces informations sont par ailleurs à consigner dans un registre et *« mis à la disposition du public par voie électronique, dans un format ouvert, et régulièrement mis à jour au cours de la période mentionnée au premier alinéa du présent article »*[1059].

2 - Devoir de coopération des opérateurs dans la lutte contre la diffusion de fausses informations

528. Indépendamment des obligations d'information de transparence de l'article L. 163-1 du Code électoral, les plateformes[1060] sont également en charge de la lutte contre la diffusion de fausses informations portant atteinte à l'ordre public ou en mesure d'altérer la sincérité du scrutin[1061]. A ce titre, elles doivent spécifiquement mettre « *en place un dispositif facilement accessible et visible permettant à leurs utilisateurs de signaler de telles informations, notamment lorsque celles-ci sont issues de contenus promus pour le compte d'un tiers* »[1062].

[1054] *Supra.*, n° 260 et s.
[1055] Art. D. 102-1.-I du Code électoral.
[1056] Art. L. 163-1 1° du Code électoral.
[1057] Art. L. 163-1 2° du Code électoral.
[1058] Art. L. 163-1 3° du Code électoral et art. D. 102-1.-II du même code.
[1059] Art. L. 163-1 du Code électoral.
[1060] Les plateformes en ligne concernées par ce devoir de coopération sont celles citées à l'article L. 163-1 du Code électoral. *Supra.*, n° 525 et s.
[1061] Art. 11 de la Loi n° 2018-1202 du 22 décembre 2018 *relative à la lutte contre la manipulation de l'information*.
[1062] *Ibid.*

529. Mais la loi laisse aux opérateurs le soin de mettre en place des mesures complémentaires[1063] pouvant notamment porter sur la transparence des algorithmes que les plateformes utilisent dans le cadre de cette mission.

530. Par une décision en date du 20 décembre 2018, le Conseil constitutionnel a été amené à se prononcer sur la constitutionnalité de ce dispositif. Le juge constitutionnel rappelle que, bien qu'il existe une inconnue sur ce qu'est une fausse information[1064], le législateur « *a entendu prévenir les atteintes à l'ordre public et assurer la clarté du débat électoral et le respect du principe de sincérité du scrutin* »[1065]. De plus, la liste non limitative des mesures complémentaires[1066] qui a été posée par le législateur ne peut par nature être contraire à la liberté d'expression et de communication[1067], comme si la transparence était finalement une nécessité permettant d'éviter les dérives algorithmiques dans ce domaine. Par ailleurs, concernant les autres mesures complémentaires que sont susceptibles de mettre en œuvre les plateformes, toujours dans ce cadre, c'est au juge qu'il conviendra de s'assurer « *si elles sont nécessaires, adaptées et proportionnées à l'objectif poursuivi* »[1068] . Pour les Sages, cette obligation de transparence des algorithmes utilisés par les plateformes, dans le cadre du signalement des *fake news,* n'est pas une atteinte disproportionnée à la liberté d'entreprendre au regard de l'objectif poursuivi[1069] qu'est la prévention des « *atteintes à l'ordre public et assurer la clarté du débat électoral et le respect du principe de sincérité du scrutin* ». Nous ne pouvons que regretter l'absence de développement du Conseil à ce sujet ; il s'agissait pourtant de la première conciliation opérée par les Sages, entre la liberté d'entreprendre et la transparence des algorithmes. Nous étudierons toutefois cette conciliation dans la deuxième partie de cette thèse[1070].

[1063] *Ibid*,. : « *(…) Ils mettent également en œuvre des mesures complémentaires pouvant notamment porter sur :*
1° La transparence de leurs algorithmes ;
2° La promotion des contenus issus d'entreprises et d'agences de presse et de services de communication audiovisuelle ;
3° La lutte contre les comptes propageant massivement de fausses informations ;
4° L'information des utilisateurs sur l'identité de la personne physique ou la raison sociale, le siège social et l'objet social des personnes morales leur versant des rémunérations en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général ;
5° L'information des utilisateurs sur la nature, l'origine et les modalités de diffusion des contenus ;
6° L'éducation aux médias et à l'information ».
[1064] Ce qui rejoint sa réserve d'interprétation de la loi à ce sujet. CC, décision n° 2018-773 DC, 20 décembre 2018, *Loi relative à la lutte contre la manipulation de l'information*, § 21.
[1065] *Ibid*., § 85.
[1066] Art. 11 de la loi n° 2018-1202 du 22 décembre 2018 *relative à la lutte contre la manipulation de l'information*.
[1067] CC, décision n° 2018-773 DC, 20 décembre 2018, *Loi relative à la lutte contre la manipulation de l'information*, § 87.
[1068] *Ibid*.
[1069] *Ibid*., § 89.
[1070] *Infra*., n° 647 et s.

3 - Les nouveaux pouvoirs du Conseil supérieur de l'audiovisuel

a - L'extension des pouvoirs du Conseil supérieur de l'audiovisuel

531. Par extension au moyen de communication plus classique qu'est désormais l'audiovisuel, le CSA est le garant du respect des obligations de transparence de l'article 11 que nous venons d'étudier[1071]. Il peut à ce titre adresser des recommandations aux plateformes en ligne, désignées à l'article L. 163-1 du Code électoral, afin d'améliorer la lutte contre la diffusion des fausses informations « *susceptibles de troubler l'ordre public ou de porter atteinte à la sincérité d'un des scrutins* »[1072]. Le CSA doit également publier un bilan périodique de l'application et de l'effectivité de ces obligations. Enfin, il dispose également, dans ce cadre, de la faculté de procéder à des enquêtes[1073].

b - La recommandation n° 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations

532. Comme nous l'avons vu précédemment, le 1° de l'article 11-1 de la loi du 22 décembre 2018, n'était pas suffisamment précis. En effet, que convenait-il d'entendre par le fait que les plateformes « *mettent également en œuvre des mesures complémentaires pouvant notamment porter sur : 1° La transparence de leurs algorithmes* » ?

533. Au titre de ses nouveaux pouvoirs, c'est par une recommandation en date 15 mai 2019 que le CSA a explicité le degré ainsi que la nature de la transparence des algorithmes utilisés dans la lutte contre les « *fausses informations susceptibles de troubler l'ordre public ou d'altérer la sincérité »* de certains scrutins.

534. Par une recommandation du 15 mai 2019[1074], le Conseil rappelle que

> « *(…) Les utilisateurs doivent pouvoir exercer de manière éclairée leur esprit critique sur les contenus qui leur sont proposés par les plateformes en ligne. Ils*

[1071] Art. 11-I 1° de Loi n° 2018-1202 du 22 décembre 2018 *relative à la lutte contre la manipulation de l'information* : « *Ces mesures, ainsi que les moyens qu'ils y consacrent, sont rendus publics. Chaque opérateur adresse chaque année au Conseil supérieur de l'audiovisuel une déclaration dans laquelle sont précisées les modalités de mise en œuvre desdites mesures.* »
[1072] Art. 17-2 de la Loi n° 86-1067 du 30 septembre 1986 *relative à la liberté de communication* modifiée. Les scrutins dont il est fait mentions sont « *l'élection Président de la République, des élections générales des députés, de l'élection des sénateurs, de l'élection des représentants au Parlement européen et des opérations référendaires* », *ibid*., art. 33-1-1.
[1073] Art. 19 la Loi n° 86-1067 du 30 septembre 1986 *relative à la liberté de communication.*
[1074] Recommandation n° 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel *aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations*.

doivent pouvoir accéder aux informations leur permettant de connaître et de comprendre les principes de fonctionnement des algorithmes qui régissent l'organisation, la sélection et l'ordonnancement de ces contenus »[1075].

535. Toutefois, ce n'est pas par l'intermédiaire du droit dur que cette transparence s'opère puisque

« A cette fin, le Conseil encourage les opérateurs à assurer à chaque utilisateur :
a) La traçabilité de ses données exploitées à des fins de recommandation et de hiérarchisation des contenus, qu'elles soient fournies sciemment ou collectées par l'opérateur de la plateforme en ligne ;
b) Une information claire, suffisamment précise et facilement accessible sur les critères ayant conduit à l'ordonnancement du contenu qui lui est proposé et le classement de ces critères selon leur poids dans l'algorithme ;
c) Une information claire et précise sur sa faculté, si elle existe, de procéder à des réglages lui permettant de personnaliser le référencement et la recommandation des contenus ;
d) Une information claire et suffisamment précise sur les principaux changements opérés dans les algorithmes de référencement et de recommandation, ainsi que sur leurs effets ;
e) Un outil de communication accessible permettant l'interaction en temps réel entre lui et l'opérateur, et offrant à l'utilisateur la possibilité d'obtenir des informations personnalisées et précises sur le fonctionnement des algorithmes »[1076].

536. Le recours au verbe « encourager » est une fois de plus symptomatique de la multiplication du droit souple dans la régulation du cyberespace, même lorsqu'il s'agit des algorithmes pouvant altérer la sincérité du corps électoral. Or, le droit souple n'est pas le droit dur. Ces non-exigences ne reposant de plus que sur du déclaratif, on imagine mal comment le CSA pourra s'assurer dans les faits de la véracité des informations communiquées par les géants du numérique.

[1075] *Ibid.*
[1076] *Ibid.*

537. Les algorithmes ne jouent pas qu'un rôle dans la manipulation du corps électoral. Ils peuvent également altérer la sincérité du scrutin lors de l'opération de vote.

B - Sincérité du scrutin et transparence des systèmes de vote électronique : l'opération de vote

538. Il n'existe non pas un, mais des systèmes de vote électronique : d'une part, les machines à voter mises à disposition dans les bureaux de vote, et d'autre part, le vote par correspondance s'effectuant par internet. Ces deux méthodes de vote électronique font référence à des questions juridiques et techniques différentes. Nous évoquerons toutefois la problématique de la transparence de ces deux dispositifs qui sont, pour le premier, encore utilisés malgré un moratoire mis en place en 2008[1077], et pour le second, bien que l'expérimentation n'ait pas été réitérée, les dispositions sont toujours présentes dans le Code électoral.

539. A titre liminaire, il convient de rappeler que le vote n'est pas une donnée à caractère personnel dans la mesure où le scrutin est secret. Les machines à voter ne collectent d'ailleurs pas de données à caractère personnel. Il n'est donc pas en théorie possible d'identifier un électeur à son vote dans le cadre de ce dispositif.

540. En revanche, bien qu'il s'agisse moins d'une évidence concernant le vote par internet, puisqu'il nécessite une identification ainsi qu'une authentification de l'électeur afin qu'il soit autorisé à voter sur une plateforme en ligne, ce vote est également secret. C'est donc par l'intermédiaire d'autres régimes juridiques non encore étudiés, reposant notamment sur des principes de droit dur et de droit souple, que la transparence de ces algorithmes est censée s'opérer.

1 - Les enjeux

541. Comme l'a affirmé le Conseil constitutionnel, lors du contrôle de la *Loi relative à la lutte contre la manipulation de l'information*, « *aux termes du troisième alinéa de l'article 3 de la Constitution, « Le suffrage peut être direct ou indirect dans les conditions prévues par la Constitution. Il est toujours universel, égal et secret ». Il en résulte le principe de sincérité du*

[1077] En effet, de nombreuses machines sont encore en fonctionnement. Le moratoire de 2008 ne porte que sur les nouvelles autorisations.

scrutin » »[1078]. Bien que cette disposition constitutionnelle ne fasse pas référence explicitement au principe de liberté de suffrage, il ne peut qu'être déduit dans un Etat de droit au sens matériel[1079].

542. L'enjeu de la transparence de ces systèmes est fondamental parce qu'il permet de s'assurer que les traitements algorithmiques ne remettent pas en cause les principes guidant les opérations de vote. Les machines à voter et le vote par internet ne recoupent pas les mêmes problématiques juridiques et techniques, ils sont tous deux, par leur nature, susceptibles d'affecter l'effectivité des principes du droit électoral.

543. Nous ne traiterons toutefois pas de la liberté du suffrage qui consiste spécifiquement à ce que « *les conditions de déroulement d'un scrutin doivent garantir la liberté de choix des électeurs entre différents candidats* »[1080]. Même si en toute hypothèse la liberté du suffrage est, contrairement aux machines à voter, particulièrement affectée par le vote par internet[1081], les traitements algorithmiques y sont totalement indifférents.

a - Secret

544. Du point de vue technique, contrairement au vote par internet, les machines à voter sont moins susceptibles de remettre en cause l'effectivité du secret du suffrage. En effet, dans le cadre des ordinateurs de vote, qui sont déployés dans certains bureaux de vote[1082], comme dans le cadre du vote traditionnel, c'est une autorité électorale qui va être chargée de vérifier que l'électeur est autorisé à voter. En revanche, dans l'hypothèse du vote par internet, l'identification et l'authentification s'effectuent en ligne afin d'être autorisé à voter sur la plateforme : il existe donc un risque supplémentaire d'associer un électeur à son vote. La transparence a également un rôle à jouer en matière de liberté du suffrage dans la mesure où le recours aux dispositifs numériques dans la sphère électorale pourrait dissuader l'électeur d'exprimer sa volonté réelle.

[1078] CC, décision n° 2018-773 DC, 20 décembre 2018, *Loi relative à la lutte contre la manipulation de l'information*, § 16.
[1079] En ce sens, GHEVONTIAN R., « La notion de sincérité du scrutin », *Cahiers du Conseil constitutionnel*, n° 13, janvier 2003.
[1080] RAMBAUD R., *Droit des élections et des référendums politiques*, *op. cit.*, p. 111.
[1081] ENGUEHARD C., « Vote par internet : failles techniques et recul démocratique », *Jus Politicum*, n° 2 [en ligne]. [Consulté le 12 mars 2021]. Disponible à l'adresse : http://juspoliticum.com/article/Vote-par-internet-failles-techniques-et-recul-democratique-74.htm
[1082] Art. L. 57-1 du Code électoral.

b - Egalité du suffrage

545. Le principe d'égalité du suffrage implique qu'un électeur dispose d'une seule voix lors du scrutin. Or, comparativement au vote traditionnel, il apparaît que dans le cadre des machines à voter ; « *globalement, les différences entre nombres de votes et nombres d'émargements sont plus fréquentes et d'ampleur plus importante en présence d'une machine à voter par rapport au vote avec bulletins en papier et urne* »[1083], bien qu'il ne soit pas possible de l'expliquer[1084], notamment parce que le vote est secret. Il n'est cependant pas exclu que l'ordinateur de vote[1085] soit en cause et que des voix aient pu compter double ou n'ont tout simplement pas été comptabilisées par la machine[1086].

c - La sincérité du scrutin

546. L'immixtion des algorithmes dans les opérations de vote est effective depuis que les ordinateurs de vote et le recours au vote par internet ont été autorisés par le législateur[1087]. Se pose donc naturellement la question de la conformité de ces systèmes de vote aux principes du droit électoral s'appliquant lors de l'opération de vote. En effet, de nombreux bureaux de vote recourent à des machines à voter, et le vote par correspondance par internet a même été utilisé dans certaines élections[1088]. Bien que le principe de transparence ne soit pas directement utilisé par les juridictions dans le cadre du contentieux électoral national, il suppose que les résultats correspondent à la volonté réelle des électeurs.

2 - Les sources de la transparence

547. L'utilisation des machines à voter est encadrée par le Code électoral, mais force est de constater que l'article L. 57-1 du Code électoral, qui liste les conditions à satisfaire, ne cite pas la transparence. Cette disposition renvoie toutefois à un règlement technique à respecter afin que ces machines soient agréées par le ministère de l'Intérieur[1089]. Pour être approuvées, les machines à voter devaient respecter certains critères qui ont été déterminés par un arrêté du 17

[1083] ENGUEHARD C., GRATON J-D., « Machines à voter et élections politiques en France : étude quantitative de la précision des bureaux de vote », *Cahiers Droit, Sciences & Technologies*, n° 4, 2014, p. 159 à 198, spéc. § 119.
[1084] *Ibid*., § 21. En effet, « *Mesurer scientifiquement la précision des résultats délivrés par une machine à voter fonctionnant lors d'une élection réelle, sans risquer de porter atteinte au secret du vote, constitue un défi non résolu.* ».
[1085] *Ibid*., § 152.
[1086] *Ibid*., § 140.
[1087] *Infra*., n° 547 et s.
[1088] *Supra*., n° 574 et s.
[1089] Toutefois, le ministère de l'Intérieur n'octroie plus d'agréement depuis 2008, date du moratoire des machines à voter.

novembre 2003 portant approbation du règlement technique fixant les conditions d'agrément des machines à voter. Le respect de ces critères conditionne l'octroi de l'agrément par le Ministère aux fournisseurs de ces ordinateurs de vote. Les machines à voter qui ont été mises en circulation avant le moratoire de 2008[1090] et qui sont pour certaines encore utilisées dans les bureaux de vote, sont toujours soumises à ce règlement technique de 2003[1091]. L'agrément est conditionné au respect de plusieurs principes directeurs parmi lesquels nous trouvons la transparence.

548. Selon les termes de l'arrêté, la transparence signifie que « *le processus doit pouvoir être examiné et vérifié* ». Nous retrouvons également d'autres principes qui vont concourir à la transparence : l'exactitude[1092] et le caractère vérifiable[1093] du vote. D'une part, l'exactitude permet de s'assurer que le décompte final est conforme à la volonté réelle des électeurs. Et d'autre part, le caractère vérifiable signifie que les résultats du vote peuvent être vérifiés après le dépouillement du scrutin.

549. Le processus précité correspond donc à la transparence de l'opération de vote. Mais cette transparence n'a pas pour nécessité d'être directe, c'est-à-dire opérée par les électeurs eux-mêmes. Elle est en effet assurée par un tiers de confiance, à savoir l'organisme accrédité par le Comité français d'accréditation et agrée par le ministère de l'Intérieur[1094].

550. Les électeurs sont donc dans l'impossibilité d'attester eux-mêmes que les résultats correspondent à leurs volontés réelles à cause de l'opacité de ces systèmes, qui sont en France, des technologies propriétaires développées et mise à disposition par des entreprises privées spécialisées[1095].

551. Il est important de ne pas perdre de vue que la technique elle-même a des incidences sur l'effectivité des principes vus précédemment. En effet, elle pourrait être garantie, mais dans cette hypothèse, la conciliation des droits devrait être revue[1096]. En ce sens, en l'état de la technique, nous sommes dans l'impossibilité de concilier par exemple le fait que le scrutin doive être secret avec la transparence des systèmes informatiques. Nous reviendrons plus en

[1090] A la suite de multiples désagréments, un moratoire a été mis en place en 2008.
[1091] Arrêté du 17 novembre 2003 *portant approbation du règlement technique fixant les conditions d'agrément des machines à voter.*
[1092] *Ibid*., p. 3 : « *exactitude : le décompte final du scrutin doit refléter la volonté exacte des électeurs ;* »
[1093] *Ibid*., p. 3 : « *caractère vérifiable : les résultats du vote peuvent être vérifiés après le dépouillement du scrutin ;* »
[1094] *Ibid*., art. 2. 1 relatif à la procédure d'agrément.
[1095] ENGUEHARD C., GRATON J-D., « Machines à voter et élections politiques en France : étude quantitative de la précision des bureaux de vote », *op. cit.*, p. 159 à 198, spéc. § 29.
[1096] *Infra*., n° 997.

détail sur la question de la conciliation des droits avec la transparence dans la deuxième partie de cette thèse[1097]. Dans notre étude, nous verrons que la transparence n'a donc pas pour but de connaître l'identité des électeurs, ni vers quel candidat s'est porté son choix ou non choix en cas de bulletin blanc, mais si le système a correctement comptabilisé les suffrages, et qu'aucune erreur ou fraude n'est intervenue dans le processus, permettant de ce fait de connaître la volonté réelle des électeurs. En effet, le juge électoral ne peut être saisi que si des irrégularités sont observées. Nous revenons donc à un problème de nature probatoire. S'il est envisageable dans le cadre d'une élection recourant à des bulletins papiers d'observer qu'une personne a fraudé, seule une expertise permettrait de constater de telles irrégularités, tout en sachant qu'il existe des probabilités pour qu'une expertise n'aboutisse pas à des conclusions certaines[1098]. C'est bien toute la difficulté des traitements algorithmiques qui sont difficilement observables dans leur fonctionnement.

552. De manière générale, c'est-à-dire indépendamment de la question du vote électronique, « *(…) le lien intime entre la transparence et la démocratie semble ne plus devoir être remis en cause. Il s'est imposé comme une nouvelle condition de la démocratie tant dans les ordres constitutionnels et électoraux internes qu'au niveau du Conseil de l'Europe* »[1099].

553. Yannick Lécuyer précise à juste titre que l'urne dématérialisée, c'est-à-dire algorithmique, est opaque, et qu'en l'état de l'art en informatique, le principe de transparence de l'opération de vote ne peut être satisfait[1100]. Toutefois, nous ne pouvons que regretter que ces systèmes soient toutefois utilisés dans bien des démocraties.

554. Depuis que les ordinateurs de vote sont utilisés dans le cadre de l'organisation de certains scrutins[1101], la problématique de la transparence de ces systèmes a été mise en avant,

[1097] *Infra.*, n° 673 et s.
[1098] PELLEGRINI F., Chaînes de confiance et périmètres de certification : le cas des systèmes de "vote électronique", *op. cit.*
[1099] LECUYER Y., *Le droit à des élections libres, Conseil de l'Europe*, 2014, spéc, p. 103.
[1100] *Ibid.*
[1101] Les machines à voter sont prévues dans le Code électoral depuis 1969. Il s'agissait cependant à l'époque d'un vote mécanique. Avec l'émergence de l'informatique, les machines mécaniques ont laissé la place aux ordinateurs de vote.

surtout afin d'éviter la défiance à l'encontre des résultats[1102]. Dès 2004, une recommandation du Comité des ministre du Conseil de l'Europe[1103], précise concernant la transparence que

> « *20. Les Etats membres prendront des mesures afin que les électeurs comprennent le système de vote électronique utilisé et aient ainsi confiance en lui.*
>
> *21. Des informations sur le fonctionnement du système de vote électronique seront diffusées auprès du public.*
>
> *22. Les électeurs se verront offrir la possibilité de s'exercer sur tout nouveau système de vote électronique avant l'enregistrement du suffrage et indépendamment de celui-ci.*
>
> *23. La possibilité sera offerte à tous les observateurs, dans les limites fixées par la loi, d'assister à l'élection électronique, de l'observer et de la commenter, y compris au stade de l'établissement des résultats* ».

555. Les exigences de transparence vont également bien plus loin, dans la mesure où l'exactitude du résultat doit être vérifiable[1104], ce qui n'est pas sans poser des difficultés compte tenu de l'état de l'art en la matière[1105].

556. Ces éléments ont été confortés et précisés par une autre recommandation portant sur la démocratie électronique[1106]. L'annexe à la recommandation précise que les technologies ne sont pas neutres[1107] et qu'il est nécessaire de connaître les caractéristiques générales de ces programmes[1108]. A ce titre, « *la mise à disposition du code source au public améliore la transparence* »[1109]. Le recours à des programmes informatiques dont le code source est ouvert

---

[1102] Ce risque de défiance à l'encontre des résultats n'est pas théorique puisqu'ils ont fait l'objet de vifs débats aux Etats-Unis d'Amérique. Donald Trump, Président sortant, ainsi que ses partisans, ont insinué que le logiciel de nombreuses machines à voter était truqué. Ce logiciel privé développé par la société Dominion est installé dans des milliers de bureaux de vote, et concerne environ 71 millions électeurs. Bien qu'aucune preuve n'ait été apportée quant à ces allégations, il s'agit d'un argument supplémentaire au service de la déstabilisation d'un scrutin, voire d'un régime politique. Cette accusation a joué un rôle central dans l'envahissement du Capitole fédéral le 6 janvier 2021. REYNAUD F., Qu'est-ce que Dominion, le logiciel électoral attaqué par Donald Trump ?, *Le Monde* [en ligne]. 20 novembre 2020, mis à jour le 21 novembre 2020. [Consulté le 2 décembre 2020]. Disponible à l'adresse : https://www.lemonde.fr/pixels/article/2020/11/20/qu-est-ce-que-dominion-le-logiciel-electoral-attaque-par-donald-trump_6060562_4408996.html

[1103] Recommandation Rec(2004)11 du Comité des ministres aux Etats membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique.

[1104] *Ibid*., point 26.

[1105] ENGUEHARD C., « Vote par internet : failles techniques et recul démocratique », *op. cit.*

[1106] Conseil de l'Europe, Recommandation CM/Rec(2009)1 du Comité des Ministres aux Etats membres sur la démocratie électronique.

[1107] *Ibid*., § 52.

[1108] *Ibid*.

[1109] *Ibid*., § 54.

est recommandé, car il permet de renforcer la confiance dans la mesure où chaque utilisateur pourrait étudier le système utilisé[1110]. Même si le code source ne peut être compris pour un profane en informatique, comme nous l'avons déjà expliqué[1111], nous considérons qu'au même titre qu'il existe une garantie collective dans le cadre du vote traditionnel lors de l'opération de vote, car plusieurs membres des partis politiques et des citoyens peuvent assister à la surveillance et au dépouillement du scrutin, les associations, partis politiques ou les citoyens compétents, pourraient prendre part à l'étude du code source, et ainsi partager leurs travaux auprès de la société civile.

557. Cependant, l'étude du code source ne vaut pas contrôle de conformité, c'est-à-dire que le code source communiqué est celui s'exécutant sur l'ordinateur de vote. Il ne permet pas plus de se prémunir contre les erreurs de traitement[1112]. Il est également question que « *les logiciels de la démocratie électronique devraient être à code source ouvert et pouvoir être inspectés, ou, alternativement, être homologués par un organisme indépendant* »[1113]. Certains seraient tentés toutefois d'arguer que la communication au public du code source ouvrirait la voie à la détection de failles de sécurité qui permettraient ensuite à des personnes mal intentionnées de s'introduire dans le système afin de procéder à des fraudes.

558. Malgré une volonté d'assurer une transparence de ces systèmes, la transparence ne peut être assurée. Comme nous le verrons dans la seconde partie, lorsque la nature et le degré de transparence n'est pas satisfaisant en fonction des objectifs poursuivis, il convient mieux d'en exclure les usages[1114].

> *« Il conviendrait de privilégier les formules reposant sur des normes ou spécifications ouvertes et des logiciels à code source ouvert, car ils empêchent les fournisseurs de verrouiller les codes sources et favorisent la transparence (…) »*[1115].

559. Cette *soft law* du Comité des ministres du Conseil de l'Europe est toutefois restée lettre morte. En effet, en France, le marché des machines à voter est détenu par des entreprises

[1110] *Ibid*., § 55.
[1111] *Supra*., n° 452.
[1112] PELLEGRINI F., Chaînes de confiance et périmètres de certification : le cas des systèmes de "vote électronique", *op. cit.*, p. 30.
[1113] Conseil de l'Europe, Recommandation CM/Rec(2009)1 du Comité des Ministres aux Etats membres sur la démocratie électronique, § 57.
[1114] *Infra*., n° 961 et s.
[1115] Conseil de l'Europe, Recommandation CM/Rec(2009)1 du Comité des Ministres aux Etats membres sur la démocratie électronique, § 60.

privées, utilisant des logiciels propriétaires, et l'once de transparence afférente n'est qu'indirecte, parce que les électeurs sont dépendants de ces tiers de confiance que sont les sociétés ayant mis en œuvre le système.

560. Le législateur français ne semble d'ailleurs pas saisir l'enjeu relatif à la transparence de ces dispositifs de vote, puisqu'il appréhende uniquement le risque algorithmique sous le prisme de la sécurité, et ce, malgré les mises en garde du Comité[1116] et de certains chercheurs[1117].

561. Par exemple, la commission des lois du Sénat plaide en faveur de la levée du moratoire du 2008 pour les machines à voter ainsi que du maintien du vote par internet pour les élections des Français de l'étranger. Bien que ce Rapport sénatorial considère que les systèmes de vote électronique doivent respecter le principe de transparence, il convient de noter que parmi les huit propositions effectuées par les Sénateurs, aucune ne porte sur la manière dont il conviendrait de mettre en œuvre la transparence de ces systèmes, alors que deux d'entre elles portent sur la sécurité de ces dispositifs[1118].

3 - La transparence comme enjeu probatoire

562. Dans la sphère numérique, l'enjeu de transparence est également probatoire. Comment est-il possible de constater des irrégularités si le processus n'est pas directement observable par les citoyens ?

563. Comme l'indique le Comité des ministres du Conseil de l'Europe[1119] dans sa recommandation, les problématiques relatives à la transparence sont aussi relatives à « *la confiance des citoyens dans la démocratie électronique* »[1120].

[1116] *Ibid.*

[1117] ENGUEHARD C., Audition lors de la mission d'information de la commission des lois du Sénat relative au vote électronique, 22 octobre 2013 : *« la promesse de sécurité n'est pas en mesure de compenser la disparition de la transparence directe* ». La transparence directe est entendue par l'auteur comme « *est l'exercice direct du contrôle des élections par les électeurs, sans média logiciel, matériel ou humain (expert autorisé ou membre du bureau de vote). Pour ce faire, les électeurs utilisent leurs cinq sens (vue, odorat, ouïe, toucher, goût). La transparence permet de constater les éventuels dysfonctionnements ou fraudes et d'en présenter des preuves à un juge électoral. »*, p. 1 et 2 [en ligne]. 22 octobre 2013 [Consulté le 18 septembre 2019]. Disponible à l'adresse : http://pagesperso.ls2n.fr/~enguehard-c/audition_Enguehard2013.pdf

[1118] DEROMEDI J., DETRAIGNE Y., Rapport d'information n° 73 réconcilier le vote et les nouvelles technologies du Sénat, session ordinaire 2018-2019, fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le vote électronique, enregistré à la Présidence du Sénat le 24 octobre 2018, p. 5 et 6.

[1119] Conseil de l'Europe, Recommandation CM/Rec(2009)1 du Comité des Ministres aux Etats membres sur la démocratie électronique.

[1120] *Ibid.*, § 25.

564. Il convient de reconnaître que l'incertitude probatoire conditionne la saisine du juge électoral qui ne pourra pas statuer sur les irrégularités dans la mesure où des preuves ne peuvent être apportées. Nous retrouvons donc l'idée que la transparence est, dans le domaine de l'informatique, une clé de voute indispensable à l'effectivité des droits qui ont été conceptualisés sur le terrain classique.

565. Bien que la jurisprudence ait déjà fait état d'irrégularités dans le cadre du recours aux machines à voter, aucune opération électorale n'a cependant été annulée par le juge électoral, notamment faute de preuves suffisantes permettant d'aboutir à une altération à la sincérité du scrutin. En effet, l'opacité de ces systèmes rend la preuve difficile, voire impossible à apporter pour les requérants[1121]. Certaines décisions relatent par exemple l'existence de différences entre le décompte des suffrages enregistrés par la machine et l'émargement des listes, sans pour autant l'expliquer, mais le juge électoral n'a pas considéré que l'écart de voix était de nature à vicier les conditions d'expression du suffrage[1122].

566. Le juge électoral a déjà également constaté des différences non négligeables entre les suffrages exprimés dans plusieurs bureaux de vote sur la machine à voter et le nombre de signatures relevées sur la liste d'émargement alors qu'aucune manœuvre ou erreur commise au moment de l'émargement ne serait à l'origine de cette différence selon l'instruction[1123].

567. Ainsi, dans une autre Commune recourant aux machines à voter, un requérant suspectait des fraudes, mais le juge note qu' *« il n'apporte au soutien de ses allégations aucune précision ni aucun commencement de preuve, de nature à mettre en cause la sincérité du scrutin »*[1124]. Bien que la charge de la preuve repose naturellement sur le requérant, il convient de constater que l'absence de transparence directe empêche également d'apporter certaines preuves et de lever des suspicions, parfois légitimes. En effet, les traitements algorithmiques ne sont pas visibles pour les électeurs, ni pour les autorités électorales organisant et s'assurant du bon déroulement du scrutin, alors que par exemple, une fraude, tel que le bourrage d'une urne physique, pourrait très bien être observée par quiconque se trouvant présent dans le bureau de vote au moment des faits.

[1121] Or, nous considérons que la transparence sert également l'apport de la preuve numérique. En effet, le processus opéré par la machine n'est pas directement observable par les électeurs, la preuve ne peut être apportée et le juge électoral ne peut constater l'irrégularité. En ce sens, les ordinateurs de vote peuvent être victimes d'erreurs de traitement, PELLEGRINI F., Chaînes de confiance et périmètres de certification : le cas des systèmes de "vote électronique", *op. cit*., p. 30.
[1122] En ce sens, CE, 1er décembre 2010, req. n° 337945.
[1123] CE, 6 juillet 2016, req. n° 394573.
[1124] CE, 9 juin 2015, req. n° 385717.

568. De plus, le fait que

> *« (…) le nombre de suffrages comptabilisés soit supérieur au nombre des émargements dans plusieurs bureaux de vote où fonctionnaient des machines à voter ne suffit pas à établir que les machines à voter, dont le modèle a été agréé par arrêté du ministre de l'intérieur, ne permettraient pas d'empêcher l'enregistrement de plus d'un seul suffrage par électeur, comme l'exige l'article L. 57-1 du code électoral, mais relève d'erreurs de manipulation ; qu'ainsi, eu égard aux écarts de voix précédemment mentionnés, l'utilisation des machines à voter ne peut être regardée comme ayant vicié les conditions d'expression des suffrages et, par conséquent, porté atteinte à la sincérité du scrutin »*[1125].

569. En sa qualité de juge électoral, le Conseil constitutionnel considère que le règlement technique en date du 17 novembre 2003 ne prévoit pas la publication *« des tests de conformité pratiqués sur chaque modèle de machines à voter par les organismes de certification agréés par le ministre ainsi que la publication des « codes sources » des logiciels utilisés, lesquels sont protégés par le secret industriel et commercial »* ce qui *« (…) ne méconnait ni le principe de liberté du vote, ni le principe de sincérité des opérations électorales »*[1126].

570. Cela étant, dans une affaire similaire[1127], des requérants avaient saisi le juge administratif après un refus de la CADA[1128] d'accéder à la demande d'agrément d'un modèle particulier de machine à voter. De plus, le demandeur prétendait devant la juridiction que le recours aux machines à voter ne garantissait pas *« le respect d'un principe de transparence des élections »*. Selon le Conseil d'Etat, conformément à la position de la CADA, le refus de communiquer les éléments du dossier étaient justifiés au *« motif que cette communication porterait atteinte au secret en matière commerciale et industrielle et serait de nature à mettre en cause le déroulement régulier d'élections à venir »*. Bien que le Ministère n'ait été disposé à communiquer ces pièces uniquement à la juridiction, le Conseil d'Etat a considéré qu'en vertu du principe du contradictoire, il convenait toutefois de verser au débat spécifiquement les éléments sur lesquels portent le débat, sous réserve des secrets protégés par la loi[1129]. Et que dans l'hypothèse où ces éléments ne seraient pas communicables pour les raisons énoncées, de

[1125] CE, 1er décembre 2010, req. n° 337945.
[1126] CC, décision n° 2007-3742/3947 AN, 20 décembre 2007, cons. 14.
[1127] CE, 13 février 2009, Association pour le contrôle citoyen des moyens de vote, req. n° 306563.
[1128] Concernant le régime juridique de la communication des documents administratifs, *Supra*., n° 410 et s.
[1129] *Supra.*, n° 421.

communiquer à la juridiction l'ensemble des pièces lui permettant de statuer. Dans cette affaire, le Conseil d'Etat a finalement rejeté le recours de l'association, et ce malgré l'absence de communication du dossier à la partie adverse puisqu'était en cause le secret industriel de fabrication commerciale[1130]. Joël Mekhantar souligne que *« dans ce contentieux, il est inquiétant de constater que le secret de fabrication commerciale tient en échec la revendication de transparence exigée par des citoyens »*[1131]. Certes, le juge a accédé au dossier d'agrément et relève que plusieurs visites et audits « *des sites de conception et de production des machines à voter* » ont été opérées et que *« le bureau Veritas a disposé de tous les éléments, dispositifs et documents nécessaires à son contrôle, en vue de vérifier la conformité de la machine à voter en cause à l'ensemble des exigences du règlement technique* ». Mais cette garantie ne nous paraît pas satisfaisante. Considérer sur le simple fondement d'une documentation, ou d'un audit des sites de fabrication de ces machines, qu'un système de vote électronique est conforme aux exigences réglementaires, ne nous semble pas judicieux d'un point de vue technique. La conformité de ces dispositifs ne peut être garantie qu'en situation réelle, par l'étude des traitements algorithmiques le jour du scrutin, ne serait-ce pour s'assurer que la machine est conforme à l'instant T. C'est également à notre sens tout l'enjeu du principe de vérifiabilité des résultats qui a été posé au niveau Européen.

571. Comme l'explique Joël Mekhantar, concernant les machines à voter

> « *Surtout, il faut observer que le suffrage électronique n'est plus égal mais seulement équitable. Cette transformation de l'égalité en simple équité trouve sa justification dans les pratiques où coexistent un système de vote traditionnel et un système de vote électronique. La stricte égalité n'existe plus, car des procédures différentes – électronique et traditionnelle – concourent à la formation du résultat pour une même élection* »[1132].

572. Il n'existe donc pas de symétrie entre le vote traditionnel et le vote électronique par machine à voter, comme si la technique avait *de facto* offert au législateur, à l'exécutif ainsi qu'au juge, la possibilité de faire bifurquer le régime juridique des opérations de vote, et donc les principes du droit électoral. Or, cette absence de symétrie, aurait dû aboutir à la

[1130] CE, 4 novembre 2009, req. n° 306563.
[1131] MEKANTAR J., « Le citoyen, la machine à voter et le juge », in FAVIER L., DOUEIHI M. (dir.), *La démocratie dématérialisée. Enjeux du vote électronique, Le Genre humain*, vol. 51, n° 2, 2011, *Le Seuil*, p. 125.
[1132] *Ibid*.

reconnaissance de principes juridiques plus protecteurs pour l'électeur pour alors que nous nous retrouvons finalement dans une situation inverse.

573. Le fait de considérer que les électeurs ne peuvent plus bénéficier des mêmes garanties, y compris de transparence, au prétexte qu'ils seraient dans des situations différentes ne devrait pas être un motif juridique valable. Quand bien même il n'existerait pas une symétrie entre ces différentes façons de voter, le juge devrait dégager comme l'a fait la Cour constitutionnelle fédérale d'Allemagne, un principe de transparence des opérations de vote pour protéger l'électeur contre ces dérives. En effet, lorsque la Cour de Karlsruhe a eu à se prononcer sur la conformité de certains modèles de machine à voter aux lois fondamentales allemandes, elle n'a pas hésité à reconnaître un principe de publicité des opérations de vote[1133]. Principe qui justifia l'interdiction du recours à une génération de machines à voter, au motif qu'elles ne permettent pas aux électeurs de comprendre et de s'assurer par eux-mêmes du bon déroulement de l'opération de vote. Bien que la Cour ne parle pas de principe de transparence, ne serait-ce parce qu'elle parle dans sa décision traduite en anglais par la Cour de « *The principle of the public nature of elections* »[1134], il est très intéressant de constater que ce principe, qui émane d'une lecture combinée de l'article 38[1135] avec les article 20.1[1136] et 20.2[1137] des Lois fondamentales allemandes, est à notre sens une adaptation des garanties du vote traditionnel vers le vote électronique, rétablissant ainsi l'égalité entre les électeurs. De ce fait, tant que ce principe, c'est-à-dire cette transparence directe, ne pourra être satisfait techniquement, le vote électronique demeurera interdit en Allemagne.

[1133] BVERFG, Judgment of the Second Senate of 03 March 2009 - 2 BvC 3/07 -, paras. (1-166), *Bundesverfassungsgericht.de* [en ligne]. [Consulté le 2 avril 2021]. Disponible à l'adresse : https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html
[1134] *Ibid*., § 35.
[1135] DEUTSCHER BUNDESTAG, Loi fondamentale pour la République fédérale d'Allemagne, art. 38, *Bundestag.de* [en ligne]. Mis à jour en novembre 2012. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.bundestag.de/resource/blob/189762/f0568757877611b2e434039d29a1a822/loi_fondamentale-data.pdf : « *Article 38 [Élections] (1) Les députés du Bundestag allemand sont élus au suffrage universel, direct, libre, égal et secret. Ils sont les représentants de l'ensemble du peuple, ne sont liés ni par des mandats ni par des instructions et ne sont soumis qu'à leur conscience. (2) Est électeur celui qui a dix-huit ans révolus ; est éligible celui qui a atteint l'âge de la majorité. (3) Les modalités sont définies par une loi fédérale.* »
[1136] *Ibid*., « *Article 20 [Fondements de l'ordre étatique, droit de résistance] (1) La République fédérale d'Allemagne est un État fédéral démocratique et social* ».
[1137] *Ibid*., « *(2) Tout pouvoir d'État émane du peuple. Le peuple l'exerce au moyen d'élections et de votations et par des organes spéciaux investis des pouvoirs législatif, exécutif et judiciaire* »

4 - Le cas spécifique du vote électronique par correspondance (par internet)

574. Le Code de bonne conduite de la Commission de Venise, considère au sujet du vote électronique qu'il

> « *doit être sûr, fiable, efficace, techniquement solide, ouvert à une vérification indépendante et aisément accessible aux électeurs ; la transparence du système doit être garantie ; à moins que les modes de vote électronique à distance ne soient universellement accessibles, ils ne doivent constituer qu'un moyen de vote supplémentaire et facultatif* »[1138].

575. Le vote électronique par correspondance est régi en France par les articles L. 330-13 et R. 176-3 et suivants du Code électoral. Il est mis en place pour le vote des députés des Français de l'étranger. La transparence va bien entendu permettre, comme dans le cadre des machines à voter, de vérifier que le résultat est conforme à la volonté réelle des électeurs.

576. Tout comme le vote par correspondance traditionnel, le recours à ce système de vote pose en plus des problématiques relatives à la liberté de l'électeur, que nous ne traiterons toutefois pas car il n'est pas en lien avec le recours aux traitements algorithmiques, au respect de la sincérité du scrutin et du secret du vote. En effet, dans le cadre des machines à voter, les ordinateurs de vote ne traitent pas des données à caractère personnel puisque l'identification de l'électeur n'est pas effectuée sur la machine. Lors du scrutin, même si chaque candidat peut désigner un délégué dont la mission est de contrôler l'opération de vote en ligne auprès du bureau du vote électronique, elle s'effectue sous réserve de la sécurité des systèmes, ce qui nuit à la compréhension des processus[1139]. En l'absence de garantie collective par l'observation lors du dépouillement d'un vote traditionnel papier, l'opacité de ces systèmes, impliquant le recours à un tiers de confiance technique, complexifie, comme dans le cadre des machines à voter, la détection des irrégularités. Ainsi, même lorsque le processus de dépouillement est interrompu pour des problèmes techniques à cause d'un « *d'un vote ne correspondant pas aux paramètres retenus par le système* », cela n'est pas de nature à établir une irrégularité permettant le recours à une expertise complémentaire dès lors que le système répond aux conditions de sécurité et de fiabilité des dispositions du Code électoral[1140].

[1138] *Ibid*., § 3.2 du a) procédure de vote, iv [en ligne]. [Consulté le 12 mars 2021]. Disponible à l'adresse : https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)008rev-f

[1139] Art. R. 176-3-2 du Code électoral.

[1140] CC, décision n° 2012-4597/4626 AN, 15 février 2013.

577. Dans le cadre du vote par internet, une expertise indépendante est prévue pour auditer aussi bien le logiciel que le matériel de la plateforme de vote afin de s'assurer que le secret du vote et du scrutin sont garantis[1141]. Il nous paraît intéressant qu'une expertise soit mise en œuvre pour étudier la partie logicielle et matérielle de la plateforme de vote, ce qui n'est pas le cas avec les machines à voter, sauf contentieux particulier comme nous l'avons étudié. Même si chaque candidat peut habiliter un délégué dont la mission est de contrôler l'opération de vote en ligne, elle s'effectue sous la réserve de la sécurité des systèmes, ce qui nuit à la compréhension des processus.

578. En l'état, les conditions n'ayant pas été satisfaites à la suite de l'expertise, le vote électronique par correspondance n'a pas été mis en œuvre pour les élections législatives des Français de l'étranger de 2017 par arrêté du ministre des Affaires étrangères et du développement international[1142].

579. En effet, la transparence permettant de vaincre l'opacité de ces systèmes, l'objectif est de s'assurer, en plus de la vérifiabilité du résultat, que la personne ayant voté est bien autorisée à le faire. Dans la mesure où ces dispositifs sont connectés à internet, contrairement aux machines à voter, il existe de plus un risque supérieur d'introduction malveillante dans ces systèmes. Le fait qu'il y ait des failles dans l'identification des électeurs, voire une possible identification d'un vote à l'électeur, n'est également pas à exclure. Mais une fois de plus, le garant du respect des principes du droit électoral n'est pas l'électeur lui-même, mais un tiers de confiance technique. L'électeur n'est pas plus en capacité de s'assurer du bon fonctionnement du système par lui-même. Or, nous ne pouvons que regretter, comme dans le cadre des machines à voter, qu'il ne soit pas prévu de vérifier le système en situation réelle, le jour du vote. Il apparaît que dans l'hypothèse d'une expertise sur ces dispositifs, elle ne peut qu'être incomplète car les traitements algorithmiques demeurent de plus complexes à étudier pour l'expert[1143].

[1141] Art. R. 176-3 II. du Code électoral : *« II. – Préalablement à sa mise en place, ou à toute modification substantielle de sa conception, le système de vote électronique fait l'objet d'une expertise indépendante destinée à vérifier le respect des garanties prévues par la présente sous-section.*
Si, au vu de cette expertise ou des circonstances de l'élection, il apparaît que les matériels et les logiciels ne permettent pas de garantir le secret du vote et la sincérité du scrutin au sens de l'article L. 330-13, le ministre des affaires étrangères peut, par arrêté pris après avis de l'Agence nationale de la sécurité des systèmes d'information, décider de ne pas mettre en œuvre le système de vote électronique. »

[1142] Arrêté du 17 mars 2017 relatif au vote par correspondance électronique pour l'élection de députés par les Français établis hors de France.

[1143] ENGUEHARD C., SHULGA-MORSKAYA T., De l'annulation d'élections par Internet par le moyen des insuffisances du système de vote, *Les convergences du droit et du numérique* [en ligne]. 13 mars 2018 [Consulté le 22 septembre 2020]. Disponible à l'adresse : https://hal.inria.fr/hal-01730380

580. Dans la mesure où le vote par internet nécessite un traitement de données à caractère personnel, ne serait-ce pour identifier l'électeur sur la plateforme, la CNIL est amenée à émettre des recommandations à ce sujet. Par une recommandation en date du 25 avril 2019[1144], la Commission pose des objectifs en fonction du niveau de risque du dispositif mis en œuvre. Plus le scrutin est sensible, plus les objectifs à atteindre sont renforcés. La grille de la recommandation fait état de trois niveaux[1145]. Les niveaux deux et trois nécessitent des objectifs particuliers de transparence. Pour le niveau deux, il convient d'assurer « *la transparence de l'urne pour tous les électeurs* », alors que pour le niveau trois, il faut « *permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers* ».

581. Enfin, la pandémie de SARS-COV-2 relance le débat relatif au vote par correspondance par internet afin de maintenir la vie démocratique de la Nation. En ce sens, un nouveau rapport d'information sénatorial[1146] estime que parmi les conditions à réunir pour que cette modalité de vote soit effective, il convient d'assurer la transparence de ce processus. Les personnes entendues dans le cadre de cette mission ont majoritairement considéré, dont Jean-Philippe Derosier, que ce mode de vote s'opposait à un contrôle éclairé des citoyens[1147].

CONCLUSION DU CHAPITRE II

582. Ce que nous appelons la transparence des traitements algorithmiques se réalise par l'intermédiaire de différents principes du droit administratif et du droit constitutionnel. Cependant, indépendamment de la question des traitements algorithmiques, la transparence de l'action administrative n'est pas absolue, ce qui constitue également des exceptions à la communication des algorithmes publics.

583. Les efforts de transparence opérés par la LRN, bien qu'imparfaits, sont dénaturés par des exceptions propres aux algorithmes : le cas de *Parcoursup* en est la parfaite illustration.

[1144] CNIL, Délibération n° 2019-053 du 25 avril 2019 *portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet* et Délibération n° 2019-053 du 25 avril 2019 *portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via internet (rectificatif).*

[1145] *Ibid*.

[1146] BUFFET F-N., Rapport d'information n° 240 relatif au vote à distance du Sénat, session ordinaire 2020-2021, fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et de l'administration générale, enregistré à la Présidence du Sénat le 16 décembre 2020, [Consulté le 24 janvier 2021]. Disponible à l'adresse : https://www.senat.fr/rap/r20-240/r20-2401.pdf

[1147] *Ibid*., p. 49.

584. A ces entraves juridiques, s'ajoutent des entraves techniques inhérentes aux algorithmes, ce qui empêche la transparence même lorsqu'elle doit avoir lieu juridiquement.

585. Le droit des algorithmes publics dénote une tentative d'adaptation d'un cadre juridique existant, laissant parfois perdre en efficacité et en visibilité le peu de transparence pouvant être obtenu.

CONCLUSION DU TITRE II

586. Qu'il s'agisse du droit privé ou du droit public, ces régimes juridiques particuliers relatifs à la transparence des algorithmes se sont construits dans le prolongement des dispositions existantes, et essentiellement en matière de droit à l'information. Même si les techniques juridiques employées sont intéressantes, elles sont souvent lacunaires, car rattachées à des règlementations non pas du terrain en ligne, mais classique, ce qui ne répond donc pas à tous les enjeux découverts pour l'heure sur la question du numérique. Et comme nous l'avons vu, ces régimes spéciaux s'imbriquent parfois mal avec le régime général relatif aux données à caractère personnel, notamment car le législateur a perdu une certaine cohérence dans ce domaine.

587. Nous constatons par conséquent un empilement de règles participant certes à une plus grande transparence des algorithmes, mais elles ne sauraient informer convenablement les personnes concernées, et encore moins la société civile. Les autorités de contrôle mises en œuvre au fur et à mesure des décennies, notamment afin de vérifier la conformité des algorithmes au droit, apparaissent éclatées en plus de souffrir d'un manque de moyens suffisants pour exercer convenablement leurs missions. Il ne s'agit ni plus ni moins que d'une dispersion de la puissance de l'Etat ne permettant pas de garantir l'effectivité des droits et libertés à l'environnement numérique. Enfin, les entraves juridiques à la transparence des algorithmes, y compris par l'intermédiaire d'un tiers de confiance, demeurent nombreuses, notamment à cause des libertés économiques ou des secrets protégés au titre du droit public.

CONCLUSION DE LA PREMIERE PARTIE

588. Même si l'établissement d'un régime général des données personnelles a été institué notamment afin de mettre en œuvre un droit à l'information ou à l'explicabilité des algorithmes manipulant de telles données, force est de constater qu'il s'est heurté assez vite aux limites du législateur qui a préféré se saisir que des effets du numérique relatifs au respect de la vie privée et de la transparence administrative.

589. Pourtant, dès les années soixante-dix, d'autres incidences des traitements algorithmiques sont clairement identifiées comme le démontre le rapport Tricot. Cette logique de recourir à un régime général propre aux données à caractère personnel, puis à des régimes particuliers afin de le compléter n'a pas été probant. Adopter une règlementation sectorielle n'est toutefois pas problématique dès lors que l'imbrication entre les différents régimes juridiques sont parfaitement bien pensée.

590. La tentation de recourir systématiquement au droit à l'information de régimes juridiques existants, et donc par rattachement, à la transparence de ces algorithmes, est naturelle. Mais l'objet saisi ne bénéficie pas des mêmes caractéristiques. Ainsi, la pertinence des techniques juridiques déployées afin de parvenir à la compréhension de ces outils est à tempérer et n'a pas su protéger convenablement les droits et libertés au sein de l'environnement numérique.

591. Le souhait d'obtenir la transparence des algorithmes par l'intermédiaire d'un régime juridique déjà existant engendre par effet mécanique que la conformité à cette règlementation dépend d'une pluralité d'autorités de contrôle qui n'ont pas été le plus souvent établies pour prendre en compte les particularités du numérique. L'Etat n'a pas su empêcher dans ce domaine de nombreuses vulnérabilités induites par le recours au numérique.

Partie II - VERS UN PRINCIPE DE TRANSPARENCE DES TRAITEMENTS ALGORITHMIQUES

592. Bien que de nombreux régimes juridiques concourent à la transparence des traitements algorithmiques, il existe encore de nombreuses porosités empêchant qu'elle se réalise totalement d'un point de vue juridique. Même si certains outils numériques sont opaques par nature, la transparence juridique est quant à elle une nécessité afin de lever les entraves juridiques à une meilleure compréhension de ces phénomènes.

593. Le fait d'appréhender cette thématique de la manière la plus large possible nous entraîne à étudier les limites constitutionnelles susceptibles de se heurter à la compréhension de ces outils, car comme nous le verrons le numérique répond à des règles propres qui exigent une conciliation particulière des droits et libertés, notamment avec les libertés issues libéralisme économique, afin de parvenir à l'objectif de transparence L'étude des régimes juridiques existants et de leurs avantages et inconvénients aboutit à ce que de nouvelles techniques constitutionnelles soient déployées pour parvenir à cette fin, et ce dans le respect de l'Etat de droit. Pour ce faire, une révision constitutionnelle apparaît comme indispensable. Cette réforme constitutionnelle arbore tout d'abord un volet relatif aux sources constitutionnelles qui ont naturellement toutes été pensées sur un terrain hors ligne, alors qu'aujourd'hui pour parvenir à la réalisation de la transparence, elles sont susceptibles de s'y opposer si elles ne sont pas précisées. Ensuite, c'est l'organisation des pouvoirs constitués de l'Etat, également élaborée pour régir le terrain classique qu'il conviendrait d'adapter à l'environnement numérique (Titre I).

594. Mais l'environnement constitutionnel ne peut être suffisant et doit être étayé et mis en œuvre à un niveau normatif inférieur. L'Etat doit encourager de nouveaux acteurs à participer à cette transparence, ce qui implique la construction d'un écosystème juridique dans lequel la société civile est susceptible de s'épanouir. Face à l'évolution frénétique des incidences du numérique sur les personnes et la société, l'éthique, en tant qu'« antichambre » du droit, est aussi amenée à jouer un rôle majeur. Cet écosystème est essentiel à une meilleure utilisation et transparence du numérique. Enfin, une règlementation devrait prendre en considération les spécificités du numérique afin de sélectionner les techniques juridiques les plus appropriées. Pour ce faire, nous nous appuierons naturellement sur la proposition de règlements européens en matière d'IA qui apporte de nouvelles obligations de transparence propres à l'environnement

numérique. Il apparaît que quand bien même la transparence des traitements algorithmiques se réaliserait, elle ne peut légitimer certains usages qu'il conviendrait d'interdire (Titre 2).

Titre I - L'INDISPENSABLE REVISION CONSTITUTIONNELLE A DES FINS D'EFFECTIVITE DE LA TRANSPARENCE DES ALGORITHMES

595. Que la transparence renvoie en droit public à l'action administrative ou démocratique, et en droit privé à la régulation des opérateurs économiques, les techniques juridiques participant à la compréhension des algorithmes sont diverses et manquent d'unicité conceptuelle. Les nouveaux enjeux, incarnés par le numérique en l'occurrence à travers la problématique de l'opacité, mais aussi des particularités du numérique, nécessitent des ajustements d'ordre constitutionnel puisque l'Etat est le seul outil agrégeant la puissance permettant d'exiger la transparence de ce nouvel environnement afin de garantir l'autonomie des citoyens en démocratie, c'est-à-dire « *que nous n'obéissions qu'à nous-même ou au moins à la volonté de la majorité des citoyens librement exprimée* »[1148].

596. C'est la raison pour laquelle il convient de s'intéresser à un certain formalisme de l'Etat de droit pour protéger les droits et libertés, ce qui implique de penser le principe de transparence des traitements algorithmiques de manière institutionnelle afin que sa réalisation par la puissance de l'Etat ne soit pas un prétexte à l'illibéralisme[1149].

597. Partant du postulat que la transparence des algorithmes est également un enjeu de souveraineté, il s'avère que notre ordre juridique constitutionnel comporte, y compris sous l'impulsion du juge constitutionnel, de nombreuses sources et interprétations susceptibles de s'opposer à une transparence des algorithmes utilisés par les gouvernants ou les opérateurs économiques. Ainsi, il apparaît plus que nécessaire de faire intervenir de nouvelles techniques juridiques pour que cette transparence puisse au moins s'opérer par l'intermédiaire d'un tiers de confiance, raison pour laquelle il convient de reconnaître un principe général de transparence des traitements algorithmiques, même s'il est naturellement à concilier avec d'autres libertés constitutionnellement protégées (Chapitre I).

598. Enfin, les sources constitutionnelles une fois clarifiée, de préférence par une Charte des droits et libertés à l'ère du numérique, ce principe constitutionnel devra être précisé et mis en œuvre par le législateur, y compris par l'intermédiaire de droits-créances. Afin de ne pas dénaturer cette exigence constitutionnelle il apparait que le numérique altère le fonctionnement

[1148] COHENDET M-A., *Droit constitutionnel*, *op. cit.*, p. 71.
[1149] JAUME L., « « Démocratie illibérale » : une nouvelle notion ? », Constitutions, *Dalloz*, 2019, p. 177.

de la démocratie tout en nous obligeant à instaurer un nouvel équilibre des pouvoirs. Les pouvoirs constitués sont amenés à se spécialiser pour prendre en compte ces particularités et lever l'opacité nécessaire à l'effectivité des droits et libertés (Chapitre II).

CHAPITRE I - UNE NECESSAIRE CONSTITUTIONNALISATION DE LA TRANSPARENCE JURIDIQUE DES TRAITEMENTS ALGORITHMIQUES

599. Les atteintes aux droits fondamentaux par le numérique ont été accentuées par un déploiement frénétique de nombreux outils dans tous les domaines de la société. Lorsqu'il s'agit de l'Etat, il repose essentiellement sur une appétence pour la gouvernance par les nombres[1150], tandis que pour les acteurs privés, cette nouvelle sphère est notamment une manière de s'affirmer sur un marché économique sur lequel l'Etat a encore peu d'emprise.

600. Mais la problématique majeure qui retient particulièrement notre attention est que les techniques, c'est-à-dire les choix opérés par les concepteurs de ces logiciels, conditionnent l'exercice des droits et libertés au sein de la sphère numérique. Elles peuvent les faciliter ou bien le cas échéant les affaiblir. Par ailleurs, il est à noter que les individus ne sont pas seulement les potentielles victimes de l'opacité algorithmique, car l'Etat est également susceptible d'être dans une situation de vulnérabilité en utilisant des outils qu'il ne comprendrait pas et qui affecterait la société[1151].

601. Il ne convient plus seulement d'appréhender le droit en fonction d'un ordre juridique valide, constitué de règles écrites intelligibles et dont leurs publicités seraient assurées. Partant du principe que les logiciels, privés ou publics, ont des incidences sur les droits et libertés, il est désormais nécessaire de rendre observable l'invisible par la transparence des langages informatiques, à savoir « le code », mais aussi les données sur lesquelles ils reposent, voire apprennent afin de réviser les règles par eux-mêmes. En effet, le « code » est devenu un nouveau régulateur sur lequel le pouvoir politique doit assurer son emprise, à défaut de quoi ce dernier se soumettra à des impératifs à des légitimités de toute autre nature (Section 1).

602. Ces travaux n'ont pas pour vocation de simplement constater la manière dont le droit s'est adapté à ce nouveau fait juridique[1152], mais bien d'offrir les outils les plus adaptés permettant d'assurer aux individus que leurs choix politiques seront respectés, ne serait-ce car le but est d'empêcher que le terrain en ligne, pour l'heure peu régulé en fonction de ses caractéristiques propres, n'accapare le monde physique classique. Pour ce faire, il convient d'une part de lever les entraves empêchant la transparence juridique, et d'autre part, il apparaît

[1150] Pour reprendre l'ouvrage de SUPIOT A., *La gouvernance par les nombres*, *op. cit*.
[1151] DOUVILLE T., HERVOCHON C., NOEL E., PAQUIER Y., « Les vulnérabilités numériques », *op. cit.*, p. 117.
[1152] *Supra.*, Partie I.

nécessaire de déployer certaines techniques juridiques constitutionnelles pour y parvenir (Section 2).

SECTION I - LA TRANSPARENCE : UN ENJEU DE SOUVERAINETE NUMERIQUE

603. Lawrence Lessig nous a offert une grille de lecture inédite du cyberespace[1153]. Le jeu de puissance auquel fait face cette sphère, qui se détache du terrain classique[1154] à bien des égards a une incidence sur notre ordre juridique, dans la mesure où il est concurrencé par des architectures techniques[1155], souvent opaques, et dont les choix sont opérés par les programmeurs informatiques, aboutissant à un choc des légitimités démocratiques (Paragraphe 1). Dans un tel contexte de rapports de force, il est impératif d'assurer l'autonomie des citoyens en démocratie, plus haut degré de la légitimité politique, en recourant à la technique juridique de la souveraineté politique, et ce dans le but de faire primer sur ces acteurs la transparence des architectures techniques pour le cas échéant permettre ensuite leur régulation (Paragraphe 2).

PARAGRAPHE 1 – L'opacité des architectures techniques

604. Le « code » ayant la capacité de concurrencer le droit étatique traditionnel (A), il a ouvert la voie à un choc des légitimités au sein du cyberespace (B). La mission principale de la transparence est alors de pouvoir observer le positionnement de ces puissances, et le cas échéant, si elles devaient aller à l'encontre de l'intérêt général, de les contraindre.

A - « *Code is Law* »

605. Dès 1999, Lawrence Lessig constate que le cyberespace est un nouveau régulateur susceptible de menacer nos libertés[1156]. L'auteur s'intéresse à la nature de ce cyberespace, et en

[1153] Selon le dictionnaire le Robert, le cyberespace (ou le cybermonde) se définit comme « *un espace de communication crée par l'interconnexion mondiale des ordinateurs (internet) ; espace, milieu dans lequel naviguent les internautes* » : LE ROBERT, Définition « Cyberespace », *Dictionnaire.lerobert.com* [en ligne]. [Consulté le 25 novembre 2020]. Disponible à l'adresse : https://dictionnaire.lerobert.com/definition/cyberespace

[1154] A cet égard, les anthropologues en lieu et place de la distinction monde virtuel/monde réel, s'accordent davantage sur la distinction terrain en ligne/terrain classique. Voir en ce sens, T. Boellstorff, *Coming of Age in* Second Life*: An Anthropologist Explores the Virtually Human*, *op. cit.*

[1155] *Infra*., n° 605 et s.

[1156] LESSIG L., Code Is Law : on liberty in cyberspace, *Harvard Magazine* [en ligne]. 1er janvier 2000 [Consulté le 29 mars 2020]. Disponible à l'adresse : https://harvardmagazine.com/2000/01/code-is-law-html : *« Ours is the age of cyberspace. It, too, has a regulator. This regulator, too, threatens liberty ».* Nous traduisons « Nous sommes à l'ère du cyberspace. Il a aussi

déduit que c'est le code logiciel ainsi que les infrastructures physiques permettant son exécution qui structurent ce cyberespace. En d'autres termes, il entend par « code », ce que nous pouvons également assimiler aux traitements algorithmiques[1157]. Le recours à ces outils numériques permet alors la mise en place d'architectures informatiques, incarnant une intention politique, économique ou encore d'intérêts divers, qui vont à leur tour conditionner l'exercice des droits et libertés. En effet, ces architectures techniques ne sont pas neutres et sont l'émanation d'un contexte, mais aussi de l'intention des concepteurs[1158]. Selon nous, cette crainte est renforcée dès lors que le positionnement des opérateurs économiques et de la puissance publique qui s'y affrontent n'est pas nécessairement visible, et ne peut qu'être difficilement démontré. La difficulté réside également dans le fait que nous utilisons des architectures techniques sans se soucier de leur philosophie et des incidences qu'elles ont sur les droits et libertés.

606. Mais qui est donc le véritable régulateur de ce « code » ? Lawrence Lessig précise que certaines architectures informatiques sont par exemple plus protectrices de la vie privée que d'autres, mais le choix d'une architecture par rapport à une autre repose finalement sur les programmeurs qui incarnent le positionnement des puissances du terrain classique qu'ils dupliquent sur le terrain en ligne. Chaque architecture dispose de ses avantages et inconvénients au regard de l'objectif poursuivi. Le choix des développeurs est cependant tributaire de certaines incitations[1159]. C'est le « code » qui fait la loi au sein du cyberespace, ce qui aboutira à l'adage « *Code is law* ».

607. La loi n'est donc plus suffisante. Pour qu'un Etat réglemente au sein de cette sphère, il faudra aussi le faire par l'intermédiaire du « code ». L'analyse de cet auteur est à notre sens primordiale dans la compréhension des enjeux relatifs au numérique, et constitue une grille de lecture du cyberespace. Toutefois, cet adage, « *Code is law* » est imparfait, et Lawrence Lessig en convient, le « code » n'est pas pour autant du véritable droit, en tout cas pas dans l'acception du code qu'il présente puisqu'il n'a pas d'effet normatif selon ses dires du début des années

---

un régulateur. Ce régulateur, aussi, menace la liberté ». Il est à noter que ce célèbre article est la retranscription des grandes idées développées par Lawrence Lessig dans le cadre de l'ouvrage *Code and Other Law of Cyberspace* publié en 1999, et dont la réédition et l'actualisation a été effectuée en 2006. Voir en sens, LESSIG L., *Code version 2.0*, Basic Books, 2006.

[1157] Est entendu par algorithme : « *L'objet de l'algorithmique est la conception, l'évaluation et l'optimisation des méthodes de calcul en mathématiques et en informatique. Un algorithme consiste en la spécification d'un schéma de calcul, sous forme d'une suite d'opérations élémentaires obéissant à un enchaînement déterminé.* », FLAJOLET P., COLLARD P., ALGORITHMIQUE, *Encyclopædia Universalis* [en ligne]. [Consulté le 7 juin 2017]. Disponible à l'adresse : http://www.universalis.fr/encyclopedie/algorithmique/

[1158] « *Il est en effet vain de demander aux algorithmes d'être « neutres » alors qu'ils sont généralement conçus pour choisir, trier, filtrer ou ordonner les informations selon certains principes* », CARDON D., « Le pouvoir des algorithmes », *op. cit.*

[1159] LESSIG L., *Code Is Law: on liberty in cyberspace*, *op. cit.* : *« Their choices depend upon the incentives they face. If protecting privacy is not an incentive--if the market has not sufficiently demanded it and if law has not, either--then this code will not provide it* ». Nous traduisons *«* Leurs choix dépendent des incitations auxquelles ils sont confrontés. Si la protection de la vie privée n'est pas une incitation du marché ou de la loi, alors ce code ne le fournira pas ».

2000[1160], bien que pour certains auteurs il puisse désormais en s'agir[1161]. En revanche, la certitude repose dans le fait que ce code va en réalité concurrencer le droit traditionnel. A notre sens, un exemple contemporain illustre parfaitement cette lecture du cyberspace : les cryptomonnaies. En effet, en reposant sur la « blockchain », c'est-à-dire une architecture technique décentralisée, la philosophie de ce système n'a pas initialement d'autre but que de proposer un modèle alternatif à l'émission de monnaie classique, afin de s'émanciper des banques centrales, et donc des Etats[1162]. Nous pouvons aisément comprendre qu'une telle technologie s'attaque à l'organisation étatique de la société. Son déploiement technologique demeure toutefois intéressant pour certains usages, mais elle concurrence par nature d'autres principes de notre droit si elle est utilisée dans le cadre du vote électronique par exemple. En effet, elle se heurte à des violations des principes du droit électoral, dans la mesure où, dans les faits, sous couvert d'une meilleure fiabilité du vote par correspondance, elle négligerait le rôle d'une autorité électorale en tant que tiers de confiance et ne pourrait garantir techniquement le secret du vote[1163]. Il conviendrait donc davantage de faire appel à des architectures techniques en fonction des objectifs souhaités, ce qui ne peut être poursuivi dès lors que l'on connait et prend en compte les tenants et aboutissants de l'architecture en question[1164], ce que permet la transparence.

608. Pierre Musso illustre par ailleurs très bien les manœuvres s'exerçant au sein de ce cyberespace :

> *« (…) dans le cyberespace, s'échangent des représentations sociales, se confrontent des « cartes mentales » d'acteurs, s'instituent des hiérarchies et des conflits d'image et de réputation. Dans ce second monde s'ordonnent des points de vue d'acteurs, des projets d'action, des conceptions du monde, des imaginaires et des valeurs ; ils s'y rencontrent, collaborent ou s'affrontent »*[1165].

[1160] LESSIG L., *Code version 2.0, op. cit*, p. 20.
[1161] BARRAUD B., « Le coup de data permanent : la loi des algorithmes », *op. cit*.
[1162] En effet, la « *blockchain* » a été pensée dans un contexte de défiance à l'encontre de l'Etat à la suite de la crise financière de 2008. Lire en ce sens, LUMINEAU L., Satoshi Nakamoto : qui se cache derrière le créateur du bitcoin, *Capital.fr* [en ligne]. 12 novembre 2018, mis à jour le 1er avril 2021. [Consulté le 17 juin 2020]. Disponible à l'adresse : https://www.capital.fr/entreprises-marches/satoshi-nakamoto-qui-se-cache-derriere-le-createur-du-bitcoin-1315353
[1163] DE LA RAUDIERE L., MIS J-M., Rapport d'information n° 1501 de l'Assemblée nationale sur les chaînes de blocs (blockchains), fait au nom de la mission d'information commune, enregistré à la Présidence de l'Assemblée nationale le 12 décembre 2018, *Assemblée-nationale.fr* [en ligne]. [Consulté le 1er juin 2021]. Disponible à l'adresse : https://www.assemblee-nationale.fr/dyn/15/rapports/micblocs/l15b1501. Selon ce rapport, les caractéristiques techniques de la blockchain n'offrent pas les garanties nécessaires dans le cadre du vote électronique. Il existe en effet un risque de retraçage du vote ou dans une tout autre hypothèse l'impossibilité de s'assurer que c'est le bon électeur qui est autorisé à voter. Le déploiement d'une telle architecture technique rendrait ineffectif des principes du droit.
[1164] *Infra*., n° 987 et s.
[1165] MUSSO P., « Critique de la notion de « territoires numériques », *op. cit.*, p. 25.

609. L'enjeu de la transparence est alors significatif pour observer ces positionnements, et le cas échéant les réglementer.

610. Lawrence Lessig rappelle que certains penseurs croient en la vertu d'un « code » qui se régulerait de lui-même, et qu'aucun autre acteur, ni même la puissance publique ne serait à même de le contrôler[1166]. Mais il évoque cependant que le code est par nature trop mouvant. Et si les architectures techniques devenaient compatibles avec une régulation d'ordre étatique, le code ne poserait pas autant de difficultés. Toutefois, force est de constater qu'en vertu d'une absence d'un universalisme des droits humains concernant les libertés économiques, il parait utopique d'aboutir par exemple à une structuration d'internet qui satisfasse tous les Etats du monde. Nous comprenons d'ailleurs la volonté d'exiger des architectures conformes à nos valeurs démocratiques dès lors que cela a été discuté et bénéficie de la légitimité politique. Et pour retranscrire cette volonté politique, et en contrôler la mise en œuvre, nous considérons que des institutions devront être dédiées à cette tâche[1167].

611. L'auteur de « *Code is law* » s'interroge : faut-il qu'une entité joue un rôle dans le choix de ce code, dans la mesure où les architectures conditionnent les valeurs ? Il évoque donc le rôle que pourrait jouer l'Etat dans ces choix. Il s'insurge particulièrement à l'encontre des partisans d'une non-intervention étatique[1168]. Pour lui, mettre à l'écart l'Etat reviendrait à laisser les choix de l'architecture d'internet aux développeurs, ce qui, convenons-en, n'est pas démocratiquement acceptable du point de vue de la légitimité politique[1169]. C'est sur une note relativement pessimiste que l'auteur termine ce célèbre article en craignant que le code ne mette à mal l'ordre juridique tout entier en affirmant que

> « *Nous devrions interroger l'architecture du cyberespace comme nous interrogeons le code du Congrès. Si nous ne le faisons pas, ou si nous n'apprenons pas à le faire, la pertinence de notre tradition constitutionnelle s'estompera. L'importance de notre engagement envers les valeurs fondamentales, par le biais d'une constitution adoptée de manière consciente, s'estompera. La menace que*

[1166] LESSIG L., *Code Is Law: on liberty in cyberspace*, *op. cit.*
[1167] *Infra.*, n° 690 et s.
[1168] Voir par exemple, BARLOW J-P., Déclaration d'indépendance du cyberespace, *in* BLONDEAU O., éd., *Libres enfants du savoir numérique. Une anthologie du "Libre"*. Paris, Éditions de l'Éclat, « Hors collection », 2000, p. 47 à 54. [en ligne] [Consulté le 2 mars 2020]. Disponible à l'adresse : https://www.cairn.info/libres-enfants-du-savoir-numerique--9782841620432-page-47.htm
[1169] Néanmoins, dans la dernière version de son ouvrage Code version 2.0 publié en 2006, à la suite des attentats du 11 septembre 2001 il prédit un nouvel âge du cyberespace qui serait celui de l'Etat. Bien que sa réflexion concernant « *Code is law* » ne change qu'assez peu, il demeure convaincu que l'Etat doit participer à l'élaboration de ce code, mais dans le respect du libéralisme politique. Voir en ce sens, LESSIG L., *Code version 2.0*, *op. cit.*, p. 7.

cette époque représente pour les libertés et les valeurs dont nous avons hérité nous échappera. La loi du cyberespace sera celle que le cyberespace codera, mais nous aurons perdu notre rôle dans l'établissement de cette loi »[1170].

612. L'étude de ces acteurs œuvrant au sein du cyberespace démontre qu'ils ne bénéficient évidemment pas de la même légitimité, ce qui aboutit naturellement à un choc des légitimités.

B - Le choc des légitimités

613. La réglementation du cyberespace passe également par le contrôle des concepteurs des architectures techniques, ce qui pose naturellement la question de la légitimité au regard des choix opérés par ces derniers et du contrôle plus ou moins fort qu'il est nécessaire d'exercer sur eux. Convient-il de laisser les programmeurs décider de tous les choix techniques opérés au sein du cyberespace ? Il n'est pas possible de répondre par l'affirmative, ne serait-ce pour des raisons de légitimité démocratique, et qui plus est parce que les technologies ne sont pas neutres[1171].

614. Afin de différencier l'intérêt général prétendument poursuivi par l'Etat, des intérêts économiques particuliers recherchés par les acteurs privés du numérique, il convient de revenir sur la notion d'intérêt général puisqu'elle est au cœur de la distinction entre ces deux puissances concurrentes.

615. La notion d'intérêt général est au fondement de l'Etat moderne, et particulièrement au cœur de notre système juridique, comme le rappelait l'étude annuelle du Conseil d'Etat de 1999[1172]. Même si ce concept est difficile à définir juridiquement, il convient tout de même d'admettre que l'Etat se justifie par la poursuite d'un intérêt général, ce qui n'est pas, par principe, l'objectif poursuivi par les entreprises privées. Ces sociétés privées peuvent bien entendu poursuivre des objectifs d'intérêt général à travers leurs prestations, mais cela n'est pas leur finalité première, qui demeure la réalisation d'activités lucratives. L'intérêt général a fait

[1170] Nous avons traduit de l'anglais « *We should interrogate the architecture of cyberspace as we interrogate the code of Congress. Unless we do, or unless we learn how, the relevance of our constitutional tradition will fade. The importance of our commitment to fundamental values, through a self-consciously enacted constitution, will fade. We will miss the threat that this age presents to the liberties and values that we have inherited. The law of cyberspace will be how cyberspace codes it, but we will have lost our role in setting that law* », LESSIG L., *Code Is Law: on liberty in cyberspace*, *op. cit.*
[1171] CARDON D., « Le pouvoir des algorithmes », *op. cit.*
[1172] Conseil d'Etat, *Rapport public, Etude annuelle sur l'intérêt général*, *La Documentation française,* études et documents, 1999, n° 50.

l'objet de nombreuses critiques[1173], y compris de la part des marxistes et des libéraux. Les premiers voyaient dans l'Etat non pas la poursuite de l'intérêt général, mais d'intérêts particuliers de la classe sociale dirigeante. Quant aux seconds, l'intérêt général est perçu comme la transcendance d'intérêts particuliers, et constituerait un risque potentiel de violation des libertés individuelles.

616. La naissance de la notion d'intérêt général apparaît au moment de la Révolution française à une période où la souveraineté, incarnée par la personne sacrée du roi qui était censé poursuivre le bien commun pour ses sujets prend fin, et est transférée au Peuple[1174]. Ce transfert de souveraineté du pouvoir royal vers un pouvoir laïcisé plus légitime, car ne reposant plus que sur le plan temporel, et entre les mains d'une seule entité appelée Peuple, est un tournant puisque la loi apparaît alors comme étant l'expression de la volonté générale[1175].

617. La vision *utilitariste*[1176], libérale, de l'intérêt général, qui consiste à cantonner l'organisation de la vie en société à l'activité économique, implique que le pouvoir politique soit amené à réguler le moins possible les relations entre les individus. Le régulateur principal ne peut être dans ce cas l'Etat, mais le marché. Le présupposé est ici que l'intérêt général ne peut émaner que des vices de l'humanité, constitués d'une propension à satisfaire, avant toute autre chose, l'intérêt purement personnel. Cet intérêt individuel est donc le socle naturel sur lequel devra reposer cet intérêt général, qui n'est autre que la somme d'intérêts privés. Dans ce cas de figure, les institutions publiques ne sont alors limitées qu'à des missions de nature régaliennes, qui n'ont pas d'autre utilité sociale que d'assurer la sécurité intérieure et extérieure, dans le but d'assurer la prospérité du marché, et donc des intérêts individuels[1177].

618. La vision *volontariste* de l'intérêt général poursuit quant à elle des objectifs de nature différente. Dans cette acception Rousseauiste[1178], « *l'intérêt général ne saurait se substituer sans que les individus n'acceptent, par un contrat social, de faire abstraction de leurs intérêts particuliers* »[1179]. L'objectif est de s'assurer que la somme d'intérêts privés, le plus souvent de nature économique, ne prennent l'ascendant sur l'intérêt commun. Ce nouvel ordre allie ainsi l'utilité du rassemblement des humains, qui peut parfois être aussi de nature économique, mais

[1173] *Ibid*.,
[1174] *Infra*., n° 624 et s.
[1175] Selon l'art. 6 de la DDHC 1789, « *La loi est l'expression de la volonté générale* ».
[1176] Conseil d'Etat, *Rapport public, étude annuelle sur l'intérêt général*, *op. cit*., p. 253 à 261.
[1177] *Ibid*., p. 254.
[1178] ROUSSEAU J-J., *Du contrat social*, *Marc-Michel Rey*, 1762.
[1179] Conseil d'Etat, *Rapport public, étude annuelle sur l'intérêt général*, *op. cit*., spec. p. 249.

tout en y associant l'idée de justice. Pour cela, le contrat social va permettre à l'individu d'être source du droit dans le cadre d'un débat démocratique, ce qui légitime de plus une telle société. C'est par l'intermédiaire de la raison que le Peuple, qui est désormais également le souverain, réduira les risques de poursuite d'un intérêt contraire à l'intérêt général. La volonté générale ne peut pas faire l'objet d'une représentation dans cette vision rousseauiste dans la mesure où le pouvoir législatif ne peut être exercé directement que par le Peuple. En ce sens, l'Etat jouit d'un haut degré de légitimité par rapports aux puissances concurrentes.

619. La démocratie libérale, telle que nous la connaissons actuellement en France, opère une synthèse de ces deux acceptions. Cela est tout d'abord justifié par le fait que la doctrine s'est accordée sur l'impossibilité matérielle d'organiser un exercice direct du pouvoir législatif par le Peuple, nécessitant un exercice du pouvoir par la voie de représentants. Ensuite, parce que le libéralisme économique l'a emporté, et qu'il convenait d'œuvrer au sein de ce paradigme, mais il a nécessité des régulations de marché en réponse aux dérives à ce qui était présenté comme un régulateur. Cette hybridation des théories est présente dans les démocraties libérales, mais la prééminence de la théorie volontariste est par exemple surtout présente en France, ce qui explique notamment le succès du droit public et la création de nombreux services publics dans notre Etat[1180]. A l'inverse, la théorie utilitariste l'emporte dans les Etats de culture anglophone expliquant que le secret l'emporte davantage sur la transparence des acteurs privés recourant à des outils numériques attentatoires aux libertés[1181], puisque l'Etat y est davantage appréhendé comme une menace.

620. Ces conceptions sont fondamentales tant elles influencent la manière dont le droit étatique se retrouve aujourd'hui concurrencé par des puissances privées à la légitimité tout autre que politique. Force est de constater qu'une Constitution est également la retranscription juridique de ces valeurs, et que certaines approches de l'intérêt général impactent nécessairement la manière d'appréhender la transparence juridique.

621. Même si l'Etat s'est engagé très fortement au sein du cyberespace du fait de la menace terroriste, cela ne fut assez souvent qu'une réaction à de tels événements, ou de gouvernance par les nombres[1182], et non dans une approche de maintien de droits et libertés face à l'émergence de géants privés du numérique par exemple. Ce choc des légitimités a été rendu

[1180] FRIER J-L, PETIT J., *Droit administratif*, 10e édition, *LGDJ*, spec. p. 222.
[1181] *Infra.*, n° 658.
[1182] SUPIOT A., *La gouvernance par les nombres, op. cit.*

possible par un désengagement de l'Etat dans le cyberespace sur la question du maintien ou de l'amélioration de la condition des libertés au sein de l'environnement numérique.

622. Dans le cadre de la gouvernance, la tentation est de mettre sur le même plan des légitimités de natures différentes, alors que rien ne devrait supplanter la légitimité politique.

623. Il apparaît que seul l'Etat est en mesure de pouvoir rivaliser avec de telles puissances économiques, bien qu'il se doive d'être en contrepartie irréprochable d'un point de vue démocratique pour assurer l'exercice des libertés.

PARAGRAPHE 2 – L'Etat comme outil de puissance garant de la transparence

624. La transparence des algorithmes est également un préalable à la suprématie de l'Etat, c'est-à-dire de « souveraineté numérique »[1183]. Cette notion, bien qu'elle repose sur la théorie générale de l'Etat, la transcende désormais sur certains points, car des acteurs non étatiques disposent parfois de prérogatives attribuées initialement à la puissance publique (A). En effet, sans la connaissance des positionnements des acteurs œuvrant au sein du cyberespace, il n'est pas possible de les réguler. Toutefois, il sera nécessaire par la suite de développer la manière dont il est impératif d'assurer une séparation des pouvoirs efficace permettant que l'intervention étatique ne se résume pas à attenter aux libertés dans cet environnement[1184], mais a pour but de les protéger. Mais cette souveraineté numérique ne se décrète pas, et elle ne peut être mise en œuvre que par une agrégation de puissances suffisantes à l'encontre des acteurs économiques remettant en cause les droits et libertés (B).

A - La Souveraineté numérique

625. C'est en cela qu'il est possible d'affirmer que les algorithmes sont capables d'affecter la présomption de suprématie de l'Etat. Frank Pasquale considère à cet égard qu'Amazon n'est plus seulement un acteur économique. Il est devenu, par sa taille et sa puissance, un régulateur sur la manière dont les marchands vendent les biens et services. Il y voit un déplacement des

[1183] TURK P., et VALLAR C. (dir.), *La souveraineté numérique : le concept, les enjeux, mare & martin,* Droit public, 2017.
[1184] *Infra*., n° 690 et s.

prérogatives étatiques, en particulier, le rôle normalement dévolu aux gouvernants, vers ces plateformes incontournables et monopolistiques, ce qui marque le glissement d'une souveraineté territoriale vers une souveraineté fonctionnelle[1185]. Même si on ne peut pas contester que ces plateformes offrent une meilleure visibilité à des commerçants, lorsque Amazon augmente les commissions des vendeurs tiers référencés sur sa plateforme, il affecte *de facto* la liberté d'entreprendre desdits commerçants. Et cela ne l'empêche pas de collecter des données sur eux pour ensuite mieux les concurrencer et asseoir davantage son positionnement[1186]. Ainsi, ne faut-il pas s'étonner de voir des Etats, comme le Danemark, nommer des « ambassadeurs » auprès des géants du numérique[1187]. En France, la création d'un commissariat à la souveraineté numérique a même été envisagée, et ce afin que « *les missions concourent à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège* »[1188].

626. La souveraineté numérique n'est pas à l'origine un concept juridique. Dans le cadre des relations internationales, la préoccupation officielle par certains Etats de leur emprise sur les réseaux de télécommunication accompagne l'émergence des nouvelles technologies. L'expression est cependant usitée par certains Etats lors de la Conférence mondiale sur les télécommunications internationales de 2012[1189]. Sur le plan national, elle apparaît sous la plume de Bernard Benhamou et Laurent Sorbier[1190] en 2006, même si Pierre Bellanger en popularisa ensuite l'expression[1191].

627. D'un point de vue juridique, elle s'inscrit dans le prolongement de la théorie générale de l'Etat, c'est-à-dire s'assurer de la suprématie technologique dans les rapports avec les autres Etats, mais aussi à l'encontre des opérateurs économiques. Même si certains auteurs, y compris

---

[1185] PASQUALE F., From territorial to functional Sovereignty: The case of Amazon, *op. cit*.

[1186] PIQUARD A., Amazon, accusé d'avoir enfreint les règles européennes de concurrence, visé par deux enquêtes de Bruxelles, *Le Monde* [en ligne]. 10 novembre 2020 [Consulté le 20 novembre 2020]. Disponible à l'adresse : https://www.lemonde.fr/economie/article/2020/11/10/bruxelles-accuse-amazon-d-avoir-enfreint-les-regles-europeennes-de-concurrence_6059246_3234.html

[1187] Voir en ce sens, UNTERSINGER M., Un ambassadeur dans la Silicon Valley pour « conserver du pouvoir à l'ère du numérique », *Le Monde* [en ligne]. 6 juin 2018 [Consulté le 23 août 2020]. Disponible à l'adresse : https://www.lemonde.fr/pixels/article/2018/06/06/un-ambassadeur-dans-la-silicon-valley-pour-conserver-du-pouvoir-a-l-ere-du-numerique_5310352_4408996.html

[1188] L'article 29 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a envisagé cette possibilité. Mais un rapport devait précéder cette éventuelle création. Sa version définitive a été remise le 1er octobre 2019. Il ne se prononce pas en faveur d'une telle création [en ligne]. [Consulté le 3 avril 2020]. Disponible à l'adresse : http://www.senat.fr/rap/r19-007-2/r19-007-21.pdf

[1189] ITU, Conférence mondiale des télécommunications internationales (CMTI-12), *Itu.int* [en ligne]. [Consulté le 3 août 2021]. Disponible à l'adresse : https://www.itu.int/fr/wcit-12/Pages/default.aspx

[1190] BENHAMOU B., SORBIER L., « Souveraineté et réseaux numériques », in *Politique étrangère*, 2006/3, p. 519 à 530.

[1191] BELLANGER P., De la souveraineté en général et de la souveraineté numérique en particulier, *Les Echos* [en ligne]. 30 août 2011. [Consulté le 3 septembre 2020]. Disponible à l'adresse : http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm

des juristes, décorrèlent cette notion de l'Etat[1192], elle nous paraît au contraire indissociable, ce qui n'empêche pas pour autant de modifier les modalités d'exercice du pouvoir politique au sein de l'environnement numérique[1193].

628. Il convient de rappeler que lorsque Jean Bodin théorisa la notion de souveraineté en 1576 dans les *« Six livres de la République »*[1194], le pouvoir royal était particulièrement affaibli aussi bien par les seigneurs locaux que par l'église catholique. Cette théorisation permit donc au titulaire de la souveraineté, en l'occurrence aux Rois de France successifs, d'affirmer progressivement leur emprise sur le royaume de France grâce notamment à la prérogative de puissance de commandement[1195]. La souveraineté fonde « *un droit à avoir le droit de commander* », associé à un principe de légitimité[1196]. Dans le paradigme de Jean Bodin la notion de souveraineté correspond davantage à un cadre terrestre, à savoir une suprématie rendue possible par l'agrégation de puissance. En effet, dans son acception, la loi naturelle demeure encore plus forte que les considérations terrestres[1197].

629. Mais en tant qu'outil, le numérique exerce des moyens de pression considérables sur la souveraineté des Etats. Comme le note Pauline Türk à juste titre :

> « *Fenêtre d'entrée sur le territoire étatique de données et d'informations de toutes provenances, sur lesquelles un contrôle des autorités publiques serait aussi mal jugé qu'il est techniquement difficile, Internet permet à des intervenants extérieurs, aux statuts divers, de s'immiscer dans les affaires d'un État* »[1198].

630. Les Etats qui se voient concurrencés par d'autres puissances sur ce territoire numérique doivent œuvrer dans la limite des architectures informatiques qui ne sont pas les leurs. Lorsque le souverain n'est pas son propre architecte, il cesse de l'être. Le danger provient également du fait que les gouvernants recourent à des technologies propriétaires dont ils n'ont pas la maitrise, et qui renforcent les opérateurs privés et leur vision politique et économique du monde.

[1192] DEROSIER J-P., « Les limites du concept de souveraineté numérique », TURK P., VALLAR C. (dir.), *La souveraineté numérique : le concept, les enjeux, mare & martin,* Droit public, 2017, p. 81.
[1193] *Infra*., n° 791 et s.
[1194] BODIN J., *Les Six livres de la République, Jacques du Puis*, 1576.
[1195] *Ibid*.
[1196] BEAUD O., *La puissance de l'Etat*, *PUF*, 1994, p. 20.
[1197] « *(…) La limite que représente la loi naturelle participant de la loi éternelle sera supprimée. Le pouvoir souverain conquiert son autonomie, purement terrestre. A partir de la volonté du prince manifestant ses droits, la route est ouverte à la volonté générale, expression du peuple souverain, créateur de son propre Etat. Bodin n'a pas le moins du monde voulu cela. Il n'en reste pas moins celui qui a doté l'Etat moderne du moyen qui, le désengageant de la théologie, l'a édifié en Etat de droit* », CHANTEUR J., *« La loi naturelle et la souveraineté chez Bodin », in Théologie et droit dans la science politique de l'État moderne*, Actes de la table ronde de Rome (12-14 novembre 1987), *École Française de Rome*, 1991, p. 283.
[1198] TÜRK P., « La souveraineté des Etats à l'épreuve d'internet », *RDP*, 2013, p. 1491.

Malheureusement, on peut regretter que ce phénomène soit exacerbé par les Etats eux-mêmes qui recourent à des logiciels développés par des entreprises qui sont au service d'autres puissances étatiques. L'affaire Snowden nous a, à ce titre, très bien renseigné sur le programme de surveillance PRISM au sujet des connivences qui pouvaient exister entre les entreprises américaines dont les « GAFA » et les Etats-Unis d'Amérique[1199].

631. Sur le plan national, le choix de recourir à l'hébergement du « *Heath Data Hub* »[1200] par la société Microsoft illustre une subordination technologique. Et lorsque le Conseil d'Etat[1201] considère qu'il n'existe qu'un risque de violation des données de santé des personnes malgré l'interdiction de transfert des données de l'Union européenne vers les Etats-Unis d'Amérique[1202], et non une violation manifestement grave de droits fondamentaux, il ne juge donc pas opportun de suspendre temporairement cet hébergement dans le cadre de l'urgence sanitaire notamment au prétexte qu'un avenant au contrat engagerait la société Microsoft à ne pas traiter ces données en dehors du territoire de l'Union[1203]. Le Conseil d'Etat a souligné la suprématie technologique de Microsoft et la nécessité d'utiliser des données de santé par l'intermédiaire de ces techniques pour une meilleure compréhension du SARS-COV-2, ce qui caractérise un intérêt public qu'il a jugé non disproportionné[1204]. Il en a par ailleurs confié l'analyse à la CNIL. Mais nous ne pouvons que nous interroger sur le fait que ce contrôle n'ait pas été opéré avant le déploiement d'une telle plateforme, dans la mesure où nous soutenons que c'est la technique qui conditionne l'exercice des droits et libertés si nous n'en maitrisons pas la conception[1205]. Il aurait donc fallu s'intéresser à la manière dont les droits et libertés auraient pu être protégées, et ce avec la transparence suffisante, voire à défaut, y renoncer si l'état de l'art ne le permettait pas. Cela illustre parfaitement comment l'opacité fait basculer la violation des droits et libertés sur une logique du risque, alors que des outils comme le référé liberté ne sont pas conçus pour cela, puisqu'il a été fondé sur l'observation factuelle d'une

[1199] A ce sujet, voir l'article du monde relatant les révélations d'Edouard Snowden à propos du programme de surveillance PRISM [en ligne]. [Consulté le 1 février 2019]. Disponible à l'adresse : https://www.lemonde.fr/international/infographie/2013/06/11/le-programme-prism-en-une-infographie_3427774_3210.html

[1200] Selon la CNIL, « *La Plateforme des données de santé, dite « Health Data Hub », est un système d'information qui a vocation à regrouper l'ensemble des données de santé de toute la population soignée en France. Cette centralisation, voulue par le législateur, doit notamment favoriser la recherche médicale. Pour les besoins de la gestion de la crise sanitaire, le Health Data Hub a été mis en service en avril 2020 de façon anticipée et sur un périmètre limité.* » in CNIL, « Le Conseil d'Etat demande au Health Data Hub des garanties supplémentaires pour limiter le risque de transfert vers les Etats-Unis », *Cnil.fr* [en ligne]. 14 octobre 2020 [Consulté le 4 décembre 2020]. Disponible à l'adresse : https://www.cnil.fr/fr/le-conseil-detat-demande-au-health-data-hub-des-garanties-supplementaires

[1201] CE, Ordonnance du 13 octobre 2020, n° 444937.

[1202] CJUE, Grande chambre, 16 juillet 2020, affaire C-311/18.

[1203] CLUZEL-METAYER L., « L'hébergement de la plateforme des données de santé par Microsoft : une validation sous surveillance », *AJDA*, 2021, p. 741.

[1204] CE, Ordonnance du 13 octobre 2020, n° 444937, spéc. cons. 18.

[1205] *Supra*., n° 605 et s.

violation, logique mise à mal par l'informatique, car univers difficilement observable. En d'autres termes, le juge, quel qu'il soit, doit être en capacité de les suspendre temporairement, sur simple faisceau d'indices, et ce au regard de ce qu'il connait des architectures techniques déployées, ou bien à défaut, ordonner leur suspension faute de garanties suffisantes dans la mesure où un traitement algorithmique serait susceptible de remettre en cause les droits et libertés dans la sphère numérique, et ce jusqu'à ce que les garanties nécessaires soient apportées.

632. Il existe un nouveau maître qui n'est pas un troisième prenant place aux côtés du pouvoir temporel et spirituel si nous devions reprendre Jean Bodin. Il s'agit d'une scission du pouvoir temporel. Le pouvoir temporel physique est affaibli par une sphère prenant son emprise sur celui-ci, mais créant un monde, un pouvoir nouveau, appelé cyberespace. Cette fenêtre issue de notre monde physique a ouvert un nouveau paradigme au sein du monde temporel, et la conciliation entre les libertés s'opérant au sein de cet environnement n'est plus nécessairement le même pour poursuivre l'objectif de protection des droits et libertés[1206]. Le monde temporel doit alors cohabiter entre d'une part les lois physiques inhérentes à notre monde, et d'autre part, un monde virtuel émulé à partir de notre monde physique, mais répondant à des règles différentes, de nature informatique. La crainte principale étant qu'une puissance prédominante ne prenne le contrôle du monde physique à travers ce cyberespace, et ce de manière douce par l'intermédiaire des traitements algorithmiques ; ce risque n'étant pas à exclure en raison de la multiplication frénétique du numérique dans tous les domaines de la société. En effet, comme nous l'avons constaté, les architectures informatiques concurrencent notre droit dans l'opacité la plus totale.

633. La question n'est pas tant de savoir si les algorithmes sont du droit, mais bien d'observer ce nouveau fait juridique, ce à quoi concourt la transparence de ces outils. L'échelon étatique ou le niveau européen apparaissent comme étant l'agrégation de puissances suffisante pour assurer notre ordre juridique, y compris sur le plan externe. En ce sens, pour assurer et exiger la transparence, nous avons besoin de fédérer le plus d'Etats possible. L'Union européenne est alors l'échelon adéquat comme ce fut le cas avec le RGPD, bien que les dispositions relatives à la transparence soient insuffisantes[1207]. Toutefois, pour l'heure, la conciliation qu'elle opère au regard des libertés économiques ne permet pas la transparence nécessaire. Nous devons donc

[1206] *Infra*., n° 987 et s.
[1207] *Supra*., n° 75 et s.

insuffler ce nouvel arbitrage à travers cette Union, mais en commençant par une constitutionnalisation nationale[1208].

B - L'outil juridique le plus à même d'accomplir la transparence des traitements algorithmiques : l'Etat

634. L'Etat est une institution indispensable permettant de garantir l'autonomie des citoyens en démocratie pour que « *nous n'obéissions qu'à nous-même ou au moins à la volonté de la majorité des citoyens librement exprimée* »[1209]. Principe fondamental dans nos démocraties, il permet notamment aux citoyens de s'organiser et de constituer un ordre juridique respectueux des droits et libertés. C'est aussi la garantie que les décisions prises par ces derniers à la majorité s'appliqueront indépendamment de la volonté des autres Etats et des techniques de gouvernance dans lesquelles les citoyens et leurs représentants ne sont pas conviés à l'élaboration de ce nouveau droit[1210]. Ceux qui rejettent l'entièreté de la notion de souveraineté s'opposent également de fait à ce principe pourtant essentiel dans le maintien d'un régime démocratique, puisqu'il est l'assurance que la légitimité des décisions qui s'imposent à tous est de nature politique, et donc censée poursuivre un objectif d'intérêt général[1211].

635. La souveraineté dans son acception moderne, inspirée par la théorie de Jean Bodin, n'est par ailleurs aucunement liée à l'idée d'absolutisme comme le rappelle Olivier Beaud, mais est bien une invention, une technique juridique développée dans le but de mettre fin à certains troubles, à savoir la guerre civile entre protestants et catholiques[1212]. Elle a donc une vocation fonctionnelle importante. A la Révolution française, lorsqu'il y eut laïcisation du titulaire de la souveraineté[1213], c'est-à-dire le transfert de la titularité de souveraineté du Roi vers le Peuple dans un but non plus de bien commun, mais d'intérêt général, l'Etat moderne bénéficiait donc d'une légitimité politique très forte, qui plus est lorsqu'un véritable suffrage universel fut instauré par la suite[1214].

[1208] *Infra*., n° 644 et s.
[1209] COHENDET M-A., *Droit constitutionnel*, *op. cit.*, p. 71.
[1210] *Infra*., n° 690 et s.
[1211] *Supra*., n° 613 et s.
[1212] BEAUD O., *La puissance de l'Etat*, *op. cit.*, p. 49.
[1213] CONSEIL D'ETAT, Rapport annuel, *Réflexions sur l'intérêt général*, La Documentation française, Etudes et documents, n° 50, 1999.
[1214] Art. 17. Ordonnance du 21 avril 1944 relative à l'organisation des pouvoirs publics en France après la Libération.

636. François Ost et Michel Van de Kerchove, dans leur célèbre article « *De la pyramide au réseau ? Vers un nouveau mode de production du droit ?* »[1215] constataient déjà un certain ébranlement de l'ordonnancement hiérarchique des pouvoirs. Parmi les éléments contribuant à l'affaiblissement de l'Etat tel que nous le connaissons, les auteurs soulèvent que la production de normes se retrouverait notamment concurrencée par des opérateurs privés. Ils notaient également que le droit étatique peinait à s'appliquer à la sphère internet, ce qui ne pouvait qu'affaiblir l'Etat. Force est de constater que la sphère numérique est aujourd'hui aussi sous l'influence des géants du numérique. Pour autant, il ne convient pas de déduire de la difficile applicabilité du droit à la sphère numérique la preuve de la disparition de l'Etat et de la souveraineté qui lui est associée, mais plutôt le fait qu'il convient de renouveler, réorienter les techniques juridiques afin d'agréger la puissance suffisante pour recouvrer cette suprématie.

637. En effet, l'ordre juridique est certes l'émanation d'un acte de souveraineté, et donc dans nos démocraties libérales, il résulte d'une légitimité politique poursuivant un objectif d'intérêt général[1216]. Mais la souveraineté ne peut se décréter, ne serait-ce car un ordre juridique en rencontre un autre[1217], et la validité juridique interne ne peut nécessairement emporter une validité globale de l'ordre juridique[1218]. La menace qui pèse aujourd'hui sur l'Etat n'est pas tant la remise en question de la validité interne de l'ordre juridique, qui répond à une logique juridique, en un système hypothéticodéductif, mais la question de sa validité globale[1219]. En effet, il ne convient pas d'apprécier la validité juridique de chaque norme prise isolément pour en déduire la validité interne. C'est cette validité globale, juridicisant l'ordre juridique, qui est menacée et risque de fissurer l'édifice étatique dans son entièreté au fur et à mesure que le numérique s'immiscera massivement dans toutes les activités humaines, sans que nous ne comprenions leur fonctionnement et les incidences qu'ils exercent sur notre ordre juridique. D'ailleurs, comme le rappelle à juste titre Guy Héraud, cette validité globale est réputée acquise sauf contexte de troubles extrêmes comme un coup d'Etat ou bien évidemment d'événements révolutionnaires. Mais si des puissances concurrentes deviennent telles qu'elles menacent le système juridique dans son ensemble, la validité interne peut être observée, mais elle n'a pas de sens puisque l'ordre juridique *in globo* n'est plu. Un ordre juridique est alors valable parce

[1215] OST F. VAN DE KERCHOVE M., *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Bruxelles, Publications des Facultés universitaires Saint-Louis, 2002, ch. IV (« Les sanctions en droit : un réseau complexe aux frontières incertaines »), p. 221.
[1216] *Supra*., n° 613 et s.
[1217] Chez Olivier Beaud, dans la puissance de l'Etat, « *la notion de souveraineté se caractérise donc par une asymétrie : elle est absolue dans sa sphère interne, et relative dans sa sphère externe, où elle rencontre son alter ego, la souveraineté de l'autre Etat* », BEAUD O., *La puissance de l'Etat*, *op. cit.*, p. 16.
[1218] HERAUD G., « *La validité juridique »*, *op. cit.*, p. 477.
[1219] DE BECHILLON D., *Qu'est-ce qu'une règle de Droit ?*, *op. cit.*, p. 84.

qu'il est soutenu « *par la plus grande force* »[1220]. Il s'agit de la « *force matérielle : économique, financière et, finalement, policière et militaire* »[1221]. Nous ajouterons bien entendu à ces puissances matérielles : le numérique. Le numérique, comme nous l'avons vu, est certes tributaire des installations physiques, mais il est un nouveau monde virtuel dans lequel l'Etat démocratique n'a que trop peu d'emprise ou lorsqu'il en a une, dessert bien souvent l'intérêt général[1222].

638. Toute la difficulté réside alors dans l'utilisation de la puissance étatique à des fins de transparence, tout en limitant son action pour qu'elle ne broie pas les libertés individuelles. Lorsque la suprématie n'est plus assurée par l'Etat, c'est la sanction de l'ordre juridique dans son ensemble qui est menacée[1223]. Il importe peu dans cette optique de savoir si chaque norme est sanctionnée individuellement (*in singuli*) et si l'ordre juridique interne est valide[1224], puisqu'il devient inopérant. L'accélération du recours aux traitements algorithmiques à tous les domaines de la société ne peut que laisser entrevoir que la puissance de l'Etat est morcelée par des opérateurs économiques, qui sont parfois les fers de lance d'Etats concurrents. C'est donc également en cela que le contrôle du numérique est un impératif afin de recouvrer la plus grande force, ou du moins suffisamment d'indépendance pour assurer les choix politiques décidés par les citoyens. Il convient donc de contribuer à la réunion des attributs nécessaires à cette fin[1225] par le corps légitime, en l'occurrence le Peuple, ce qui dans la sphère numérique correspond au contrôle des architectures matérielles et logicielles ; raison pour laquelle l'établissement d'un écosystème juridique favorable devrait être envisagé à l'échelon de l'Union européenne afin de bénéficier d'une agrégation de forces suffisantes.

639. En principe, la force *ut singuli* détenue par les personnes privées ne peut pas venir concurrencer la plus grande force détenue par l'Etat. Mais le danger apparaît lorsque l'Etat n'a pas pris conscience du positionnement des puissances concurrentes qui le menace, voire l'encourage. Dans l'hypothèse des traitements algorithmiques utilisés par les puissances étrangères, à travers les architectures informatiques produites par les puissances privées qu'elles

[1220] HERAUD G., « La validité juridique », *op. cit.*, p. 479.
[1221] *Ibid*.
[1222] Nous reviendrons toutefois sur la manière dont il convient de cadrer l'action des gouvernants par l'intermédiaire de contre-pouvoirs afin d'éviter cette déviance au sein de la sphère numérique.
[1223] En effet, de nombreux juristes ont selon nous considéré à tort que la validité d'un ordre juridique ne devait s'apprécier qu'au regard de sa validité interne.
[1224] Chez Olivier Beaud, dans la puissance de l'Etat, « la notion de souveraineté se caractérise donc par une asymétrie : elle est *absolue* dans sa sphère interne, et *relative* dans sa sphère externe, où elle rencontre son alter ego, la souveraineté de l'autre Etat », p. 16.
[1225] Guy Héraud précise d'ailleurs que « *l'ordre juridique bénéficie toujours de la plus grande force, parce que la force se fait droit si le droit perd la force* », HERAUD G., « La validité juridique », *op. cit.*, p. 479.

ont développées, c'est à une limitation de puissance normalement irrésistible de l'Etat à laquelle nous sommes confrontés.

640. Les conséquences de l'absence de la validité globale de l'ordre juridique est alors simple : l'inopérance des droits et libertés protégées. Si la validité globale est remise en cause par des puissances concurrentes dont la légitimité politique est nécessairement moindre, voire inexistante, cela rend l'ébranlement de l'Etat intolérable, et aboutit progressivement à une reféodalisation de la société[1226], ce que le numérique encourage par morcellement du pouvoir. C'est pourquoi, comme nous le verrons[1227], la transparence des outils numérique est une clé de voûte de la protection des droits actuels et à venir, afin d'observer cette sphère numérique et ainsi procéder à sa régulation de manière efficace. Au même titre que la hiérarchie des normes est un outil de structuration du droit étatique, car poursuivant des objectifs de prévisibilité, de lisibilité du droit, les algorithmes créateurs de droits utilisés par les entités privées ou publiques empêchent, du fait de leur opacité, cette intelligibilité, ce qui crée une difformité du droit. C'est également l'objectif de la transparence que de lever cette opacité, qui a des effets juridiques sur les personnes.

641. D'une part nous pensons que l'Etat perd la plus grande force par inaction, parce qu'il n'intervient plus dans de nombreux domaines. Les acteurs privés ont pris l'ascendant dans la création des architectures numériques qui, comme nous l'avons vu[1228], ont des incidences sur nos choix, mais aussi car il peine à observer les algorithmes et la conformité de ces derniers avec notre ordre juridique. D'autre part, si l'on considère que l'Etat n'est pas un délégataire, mais un distributeur de puissance par l'intermédiaire de la norme primaire conformément à ce que pense Guy Héraud[1229], l'Etat peut être amené à octroyer de la puissance aux sociétés privés. Et c'est effectivement une tendance vérifiable lorsque l'on observe la volonté des gouvernants à distribuer cette puissance à des architectes privés du numérique[1230]. Les projets de censure des propos tenus dans la sphère numérique par la voie des plateformes privées et des algorithmes opaques, qui conditionnent l'exercice de la liberté d'expression par ces acteurs, se multiplient[1231].

[1226] SUPIOT A., *La gouvernance par les nombres, op. cit.*, p. 310.
[1227] *Infra.*, n° 644 et s.
[1228] *Supra.*, n° 605 et s.
[1229] HERAUD G., « La validité juridique », *op. cit.*, p. 480.
[1230] BEAUCHESNE B., « La dépendance européenne et nationale face aux nouveaux acteurs du numérique », *Dalloz IP/IT*, 2021, p. 125 à 129.
[1231] En ce sens, voir la Proposition de loi visant à lutter contre les contenus haineux sur internet qui a été très largement censurée par le Conseil constitutionnel, *Supra.*, n° 338 et s. Afin que la puissance publique ne distribue pas cette puissance à un tel acteur

642. L'absence de validité globale peut aussi venir du fait que les corps constitués recourent trop souvent à l'automatisation[1232], ou ignorent sur quoi légiférer compte tenu de l'absence de transparence des actions de puissances concurrentes ou parce que le juge ne peut constater ce qui est, c'est-à-dire de multiples violations du droit par le truchement des algorithmes. Les positionnements des puissances du monde physique s'y affrontent en son sein dans l'opacité la plus totale, rendant de fait difficile voire impossible une éventuelle régulation. En effet, une régulation nécessite la connaissance des enjeux, ce qui est compromis dans la sphère du cyberespace sans cette transparence.

643. Un corps constitué devra avoir pour mission d'assurer la transparence des traitements algorithmiques, mais pour cela, il convient de lever les entraves juridiques pour que cette transparence puisse s'exercer.

SECTION 2 - VERS LA RECONNAISSANCE DE NOUVELLES TECHNIQUES CONSTITUTIONNELLES GARANTISSANT LA TRANSPARENCE JURIDIQUE DES ALGORITHMES

644. Comme nous l'avons vu précédemment, l'Etat est l'acteur bénéficiant du plus haut degré de légitimité démocratique. C'est donc par l'intermédiaire de la technique juridique qu'est la souveraineté qu'il va pouvoir contraindre, par sa force et sa puissance, les autres acteurs, et le cas échéant s'immiscer dans les choix qu'ils effectuent dès lors qu'ils ont une incidence sur les droits et libertés protégés. Cette régulation ne peut toutefois s'opérer que par la transparence du positionnement des acteurs ou du fonctionnement des outils que l'Etat utilise.

645. Mais pour ce faire, le pouvoir constituant se doit d'intervenir pour préciser, en réaction à l'émergence du fait juridique qu'est l'apparition des traitements algorithmiques, quelles sont les techniques juridiques les plus opportunes à déployer, ainsi que leurs conciliations. Dès lors, il est nécessaire d'aborder le panorama du droit existant dans le but de constater ses insuffisances (Paragraphe 1) pouvant aboutir à un risque d'absence de transparence juridique des algorithmes et la façon dont une nouvelle source constitutionnelle pourra prendre en compte

privé, il conviendrait de scinder l'activité de censure à une institution légitime publique, dont les critères seraient discutés, en opposition à la Cour suprême de Facebook déjà abordée précédemment. *Supra.*, n° 343.

[1232] RYAN C., KEATS CITRON D., The Automated Administrative State: A Crisis of Legitimacy, 9 Mars 2020, Emory Law Journal, Forthcoming, SSRN [en ligne]. [Consulté le 25 novembre 2020]. Disponible à l'adresse : https://ssrn.com/abstract=3553590

aussi bien la transparence des traitements algorithmiques déployés par l'Etat que les acteurs privés (Paragraphe 2), ce que le législateur sera ensuite amené à préciser[1233].

PARAGRAPHE 1 - Panorama du droit existant

646. Le panorama du droit existant nous permet d'une part de constater quelles sont les sources constitutionnelles actuelles susceptibles de concourir à la transparence des traitements algorithmiques (A), et d'autre part, d'observer que parmi ces sources, certaines d'entre elles sont en conflit lorsqu'il s'agit d'assurer une transparence juridique de ces algorithmes (B).

A - Les actuelles sources constitutionnelles concourant à la transparence des algorithmes

647. Plusieurs sources constitutionnelles[1234] sont susceptibles de concourir à la transparence des traitements algorithmiques, aussi bien de la part des justiciables, et c'est la raison pour laquelle nous aborderons certains arguments juridiques utilisés dans les moyens qui participent à la justice constitutionnelle, que ceux retenus par le juge constitutionnel. Ce phénomène n'est par ailleurs pas propre à la matière constitutionnelle et du numérique, puisque c'est une tendance que l'on retrouve dans d'autres domaines du droit à un niveau infra-constitutionnel comme l'a démontré Jean-François Kerléo[1235], et comme nous l'avons évoqué dans la première partie de ces travaux, en ce qui concerne par exemple le droit des plateformes en ligne[1236] ou des données à caractère personnel[1237], compte tenu des relations contractuelles inhérentes à ces réglementations, la transparence a fait une immixtion spectaculaire ces dernières années mais tout en étant combinée, le plus souvent, avec le principe de loyauté[1238], alors que cette dernière prend également sa source dans des principes tout aussi divers que la bonne foi par exemple[1239], mais aussi d'équité ou d'intelligibilité, voire de clarté et d'accessibilité. Il s'agit d'ailleurs

[1233] *Infra*., n° 742 et s.
[1234] Nous préférons retenir l'acception de « sources constitutionnelles » plus large à celles de « normes constitutionnelles » plus restrictives. En effet, comme l'indique Agnès Roblot-Troizier, *« Considérer que la source du droit constitutionnel se résume au « bloc de constitutionnalité », c'est oublier tout un pan du droit constitutionnel qui n'est pas justiciable devant le Conseil constitutionnel, correspondant à toutes les règles et principes non sanctionnés par le juge et résultant soit d'un article de la Constitution, soit d'une « convention de la Constitution »*, ROBLOT-TROZIER A ., Le Conseil constitutionnel et les sources du droit constitutionnel, *Jus Politicum*, n° 21 [en ligne]. [Consulté le 15 décembre 2020]. Disponible à l'adresse : http://juspoliticum.com/article/Le-Conseil-constitutionnel-et-les-sources-du-droit-constitutionnel-1261.html
[1235] KERLEO J-F., *La transparence en droit, Recherche sur la formation d'une culture juridique*, *op. cit*.
[1236] *Supra.*, n° 266 et s.
[1237] *Supra.*, n° 80 et s.
[1238] *Supra.*, n° 127 et s.
[1239] *Supra.*, n° 271, PETIT F. (dir.), *Droit et loyauté*, *op. cit*., p. 1. La notion de loyauté renverrait à la notion de bonne foi en matière contractuelle que l'on retrouve à l'article 1134 alinéa 3 du Code civil ; et plus précisément concernant la loyauté en lien en numérique, voir CONSEIL D'ETAT, *Le numérique et les droits fondamentaux*, *op. cit*., p. 26.

surtout de principes et non de droits, à l'exception du droit d'accès à ses données personnelles[1240], aux documents administratifs[1241], ou à l'explicabilité des décisions privées[1242] ou administratives individuelles[1243] notamment. Lorsque cela est possible techniquement, il est alors fondamental de permettre un droit à la transparence subjectif, c'est-à-dire offrir la faculté pour une personne juridique de s'en prévaloir, et non uniquement objectif, à savoir la simple norme juridique[1244]. Bien souvent, le législateur visait des objectifs qui étaient tout autre que la transparence de ces dispositifs technologiques, ce qui convenons-en, est logique dans la mesure où la problématique des traitements algorithmiques est relativement récente.

648. Les possibilités de normes constitutionnelles pouvant concourir à la transparence des traitements algorithmiques sont infinies tant ils s'immiscent dans tous les usages. Qu'il s'agisse en effet des droits de la défense, ou encore de non-discrimination par exemple, de nombreuses sources générales peuvent être invoquées devant le Conseil constitutionnel. Mais faudrait-il encore que le juge constitutionnel soit réceptif à cette problématique. Toutefois, force est de constater que les sources constitutionnelles se heurtant à la transparence sont nombreuses, ce qui rend la conciliation entre ces sources tumultueuse.

649. A l'heure actuelle, les sources privilégiées sont en lien avec le contrôle démocratique de l'Etat, ce qui n'est guère une surprise eu égard à la tradition juridique du libéralisme politique. Les tentatives de reconnaissance d'une transparence des traitements algorithmiques devant le juge constitutionnel sont créatives et démontrent l'absence d'unicité des principes constitutionnels pouvant participer à la transparence de ces systèmes.

650. Plus classiquement, elle est relative au droit d'accès aux documents administratifs puisque la doctrine de la CADA[1245] et la LRN[1246] ont associé les traitements algorithmiques à des documents administratifs. Il s'agit donc d'un droit en lien avec la transparence de la vie publique que le Conseil constitutionnel a rattaché à l'article 15 de la DDHC[1247] dans sa décision relative à la communication des traitements utilisés dans le cadre de *Parcoursup*[1248], ce qui

[1240] Il convient d'entendre par droit subjectif son acception dominante, c'est-à-dire la prérogative donnée à un individu de s'en prévaloir y compris devant les juridictions.
[1241] *Supra*., n° 410 et s.
[1242] *Supra*., n° 147 et s.
[1243] *Supra*., n° 435 et s.
[1244] En ce sens, voir DE BECHILLON D., *Qu'est-ce qu'une règle de Droit, op. cit.*
[1245] *Supra.*, n° 410 et s, voir notamment CADA, avis n° 20161989 du 23 juin 2016.
[1246] *Ibid*., art. L. 300-2 du CRPA.
[1247] Art. 15 DDHC 1789, « *la société a le droit de demander compte à tout agent public de son administration* ».
[1248] CC, décision n° 2020-834 QPC, 3 avril 2020, § 8.

demeure rare[1249]. Naturellement, la reconnaissance de la valeur constitutionnelle de ce droit d'accès, qui plus est dans le cadre d'une QPC relative à l'opacité des traitements algorithmiques, est certes un élément intéressant, mais comme nous le verrons, elle n'empêche aucunement le législateur d'y apporter des limitations au regard d'exigences constitutionnelles ou compte tenu d'un intérêt général, dès lors que cette atteinte n'est pas disproportionnée à l'objectif poursuivi[1250]. Il est donc difficile de s'en satisfaire dans l'hypothèse d'un nouveau paradigme permettant une transparence qui serait au moins assurée par une institution indépendante unique[1251]. L'*open data* aurait également pu être reconnu lors de ce contrôle de constitutionnalité comme le précise Jean-François Kerléo[1252], et ce dans la mesure où les données sont tout aussi importantes que les caractéristiques et paramétrages des algorithmes, surtout lorsque ce sont des algorithmes auto-apprenants.

651. L'article 16 de la DDHC de 1789[1253] et l'article 21 de la Constitution de la Vème République ont également été invoqués en second lieu afin de déduire de l'opacité de ces dispositifs que les dispositions du Code de l'éducation remettraient en cause le droit à un recours effectif, notamment *« en empêchant d'exercer avec succès un recours contestant l'absence de communication des informations en cause et en privant les justiciables des éléments nécessaires à la contestation effective du bien-fondé des refus d'inscription* »[1254]. C'est dans un style laconique que le Conseil constitutionnel a considéré que « *la restriction d'accès à certains documents administratifs relatifs aux traitements algorithmiques éventuellement utilisés par l'établissement ne prive pas d'effectivité les recours contre une décision de refus d'inscription* »[1255] alors pourtant que l'absence de transparence ne permet pas de s'assurer que le traitement est conforme au droit, et quand bien même il ne s'agirait uniquement d'une aide à la prise de décision, il pourrait également induire en erreur des équipes pédagogiques qui seraient susceptibles de se reposer sur ces recommandations.

652. Malgré la reconnaissance constitutionnelle d'un « droit d'accès », ayant été précédemment consacré concernant l'accès aux archives publiques dans les mêmes termes[1256],

[1249] En effet, ce n'est que la deuxième fois que le Conseil constitutionnel consacre un « droit d'accès » sur le fondement de l'article 15 de la DDHC de 1789.
[1250] *Ibid*.
[1251] *Infra*., n° 717 et s.
[1252] KERLEO J-F., « La constitutionnalisation d'un principe de transparence de la vie publique », *ADJA*, 2020, p. 1137.
[1253] Art. 16, DDHC 1789, « *Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution* ».
[1254] CC, commentaire de la décision du Conseil constitutionnel n° 2020-834 du 3 avril 2020, Union Nationale des Etudiants de France, p. 18, *Conseil-constitutionnel.fr* [en ligne]. [Consulté le 20 novembre 2020]. Disponible à l'adresse : https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2020834qpc/2020834qpc_ccc.pdf
[1255] CC, décision n° 2020-834 QPC, 3 avril 2020, § 20.
[1256] CC, décision n° 2017-655 QPC, 15 septembre 2017, § 4.

l'absence de transparence des algorithmes avait déjà été visée devant les sages à travers d'autres moyens invoqués. En effet, des requérants avaient notamment soutenu, au sujet des décisions administratives individuelles fondées exclusivement sur des traitements algorithmiques auto-apprenants[1257], que le recours à de tels outils méconnaitrait le principe de publicité des règlements et l'article 21 de la Constitution, particulièrement car les dispositions autorisant leur recours « *seraient contraires, par leur complexité, à l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi* »[1258]. L'idée d'un tel argumentaire était de souligner que les algorithmes puissent créer du droit et que cette absence de transparence empêcherait de connaitre la règle algorithmique. Nous avons en effet souligné que les programmes informatiques, bien qu'ils n'aient pas de volonté, ni la compétence juridique d'interpréter le droit, sont susceptibles de renfermer certains arbitrages juridiques effectués par les développeurs lorsqu'ils mettent sous forme algorithmique le droit pour l'appliquer, et plus encore peuvent d'eux-mêmes avoir des interprétations erronées du droit s'ils sont auto-apprenants. Ce moyen a finalement été rejeté par le Conseil puisqu'il a rappelé les garanties propres aux décisions administratives individuelles exclusivement automatisées posées par le législateur qui impliquent une transparence absolue[1259]. Il rappelle qu'elles doivent avoir la mention explicite prévue à l'article L. 311-3-1 du CRPA et qu'aucun secret ou intérêt protégé par la loi ne peut être opposé à la communication des principales caractéristiques du traitement[1260]. De plus, ces décisions doivent pouvoir faire l'objet d'un recours administratif ou contentieux. Pour le premier, l'administration doit pouvoir se prononcer sans recours à un traitement automatisé. En cas de contentieux contre la décision, le juge peut exiger la communication des caractéristiques de l'algorithme[1261]. Quant au responsable de traitement, il doit pouvoir expliquer à l'intéressé de manière intelligible son fonctionnement. Pour cela, il doit maîtriser le traitement et ses évolutions. Pour les algorithmes auto-apprenants, le Conseil ajoute que « *sans le contrôle et la validation du responsable du traitement* », ils ne peuvent fonder exclusivement une décision administrative individuelle[1262]. En l'état de l'art en informatique, cela revient à dire qu'ils doivent être exclus car la transparence du processus décisionnel ne peut être totale. Le Conseil est donc venu valider et préciser un régime juridique pour faire cesser une vulnérabilité juridique issus de ces algorithmes parce que la transparence

[1257] Les algorithmes autoapprenants sont « *des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement* », CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*, § 71.
[1258] *Ibid*., § 66.
[1259] *Supra*., n° 459 et s.
[1260] CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*, § 70.
[1261] *Ibid*.
[1262] *Ibid*, § 71.

juridique et technique ne peut être atteinte, ce qui aura une place significative dans nos raisonnements ultérieurs[1263].

B - Une délicate conciliation constitutionnelle et des limitations posées par le législateur

653. Du point de vue des sources constitutionnelles concourant à la transparence, force est de constater qu'elles émanent du libéralisme politique et économique et que certaines d'entre elles sont susceptibles de s'opposer à la transparence juridique des traitements algorithmiques. Se heurte à cette difficile conciliation, à ce conflit de normes, l'interprétation des sources constitutionnelles entre elles, mais également de la conciliation opérée par le législateur.

1 - La conciliation opérée par le Conseil

654. Comme nous l'avons constaté lors du contrôle de conformité de la loi relative à la lutte contre la manipulation de l'information opérée par le Conseil constitutionnel[1264], le législateur est venu proposer la mise en œuvre de mesures complémentaires, parmi lesquelles la transparence des algorithmes[1265] que les plateformes utilisent dans le cadre de cette mission[1266]. Pour les Sages, cette obligation de transparence des algorithmes utilisés par les plateformes, dans le cadre du signalement des *fake news,* n'est pas une atteinte disproportionnée à la liberté d'entreprendre au regard de l'objectif poursuivi[1267] qu'est la prévention des « *atteintes à l'ordre public et assurer la clarté du débat électoral et le respect du principe de sincérité du scrutin* ». Nous ne pouvons que regretter l'absence de développement du Conseil à ce sujet ; il s'agissait pourtant de la première conciliation opérée par le juge constitutionnel, entre la liberté d'entreprendre et la transparence des traitements algorithmiques. Bien que la liberté

[1263] *Infra*., n° 900 et s.
[1264] CC, décision n° 2018-773 DC, 20 décembre 2018, *Loi relative à la lutte contre la manipulation de l'information*.
[1265] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, art 11 : « *(…) Ils mettent également en œuvre des mesures complémentaires pouvant notamment porter sur :*
1° La transparence de leurs algorithmes ;
2° La promotion des contenus issus d'entreprises et d'agences de presse et de services de communication audiovisuelle ;
3° La lutte contre les comptes propageant massivement de fausses informations ;
4° L'information des utilisateurs sur l'identité de la personne physique ou la raison sociale, le siège social et l'objet social des personnes morales leur versant des rémunérations en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général ;
5° L'information des utilisateurs sur la nature, l'origine et les modalités de diffusion des contenus ;
6° L'éducation aux médias et à l'information ».
[1266] *Supra*., n° 528 et s.
[1267] CC, décision n° 2018-773 DC, 20 décembre 2018, Loi relative à la lutte contre la manipulation de l'information, § 89.

d'entreprendre soit garantie par l'article 4 de la DDHC de 1789[1268] comme a pu l'affirmer à plusieurs reprises le Conseil constitutionnel[1269], il existe une inconnue sur les limites de cette liberté ayant une valeur constitutionnelle et qui peut également nuire à l'application de la transparence des traitements algorithmiques. Et les arguments laconiques du Conseil dans ce domaine ne rassurent en rien sur l'avenir d'une telle transparence. De la même manière, le droit de propriété[1270] qui fonde le secret par l'intermédiaire de la propriété intellectuelle n'est pas en reste pour les mêmes raisons.

655. Véronique Champeil-Desplats soulignait déjà le risque que faisait peser l'introduction des libertés économiques en tant que droits fondamentaux pour le respect des autres libertés[1271]. Cette construction n'est pas anodine et illustre l'intention du juge constitutionnel à ce que le libéralisme économique soit protégé, et ce au risque qu'il entre en conflit, voire l'emporte sur les autres droits et libertés politiques. Ce ne sont pas les techniques dont jouit le Conseil constitutionnel en matière de contrôle qui sauraient rassurer tant il existe un aléa sur la possibilité d'une transparence des traitements algorithmiques dans de nombreux domaines. A cet égard, concernant les droits fondamentaux issus du libéralisme politique ou économique, « *en cas de conflit, chacun d'eux a une égale prétention à l'emporter : la résolution donne souvent lieu à une application partielle, non nécessairement équilibrée, des droits et libertés en jeu* »[1272]. Par ailleurs, l'incertitude demeure totale, y compris sur la constitutionnalité des propositions de Règlement européen susceptibles d'apporter une plus grande transparence des algorithmes. La probabilité que ces dispositions soient jugées contraires à la Constitution n'est pas à exclure.

656. En effet, à l'exception des mesures de transparence au regard de la clarté du débat électoral et le respect du principe de sincérité du scrutin, le juge constitutionnel ne s'est pas prononcé sur la constitutionnalité des techniques juridiques participant à la transparence des algorithmes dans le cadre de la proposition de loi contre les contenus haineux sur internet[1273] ou du projet de loi confortant le respect des principes de la République[1274] qui contient une

[1268] « *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui. Ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la loi* », art. 4, DDHC de 1789.
[1269] CC, décision n° 81-132 DC, 16 janvier 1982, *Loi de nationalisation*, § 16.
[1270] Art. 2 et 17 de la DDHC de 1789.
[1271] CHAMPEIL-DESPLATS V., « La liberté d'entreprendre au pays des droits fondamentaux », *RDT*, 2007, p. 19 à 25.
[1272] *Ibid*.
[1273] CC, décision n° 2020-801 DC, 18 juin 2020, *Loi visant à lutter contre les contenus haineux sur internet*.
[1274] CC, décision n° 2021-823 DC, 13 août 2021, *Loi confortant le respect des principes de la République*.

transposition par anticipation du règlement sur les services numériques[1275] parce qu'il n'avait pas été saisi sur cette question. Quand bien même la liberté d'entreprendre a été de très nombreuses fois restreintes dans le cadre de l'urgence sanitaire[1276], il ne s'agit en rien d'un gage qu'elle ne l'emportera pas de nouveau sur les autres libertés tant cette période est exceptionnelle par nature.

2 - La conciliation opérée par le législateur

657. Le législateur est amené à opérer une conciliation entre les différents intérêts, ce que le Conseil constitutionnel a par ailleurs rappelé lorsqu'il a eu à connaître l'appréciation de la conformité à la Constitution de la transparence des traitements algorithmiques en tant que document administratif confronté au secret des délibérations des équipes pédagogiques en considérant classiquement qu'« *il est loisible au législateur d'apporter à ce droit des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi* »[1277]. Il y a fort à parier que certaines conciliations opérées par le législateur, et qui paraissent tout à fait proportionnées pour le juge constitutionnel, pourraient en réalité nuire à l'équilibre de la transparence, notamment du fait de leur contrôle *in abstracto* opéré lors de la constitutionnalité de la loi[1278].

658. Dès lors, lorsque les sources constitutionnelles sont générales et non pensées initialement pour un domaine, ce qui est typique des « anciennes constitutions »[1279] où les sources doivent davantage faire l'objet d'interprétation de la part du juge constitutionnel, il existe un risque que l'opacité l'emporte sur la transparence, et ce même lorsqu'il en va normalement de la transparence de l'action administrative. Dans un Etat très libéral économiquement, c'est-à-dire qui a fait le choix de faire primer l'économie sur les autres libertés, il n'est pas anormal que le secret des affaires l'emporte, et ce au risque de fragiliser l'édifice de la protection de toutes les autres libertés. Le risque est que le secret soit amené à primer sur les autres libertés, alors même que le pouvoir constituant ne s'est pas prononcé sur certains arbitrages nécessaires à l'émergence de nouveaux faits juridiques. L'exemple le plus

[1275] 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.
[1276] BRAMERET S., « Les libertés économiques enfin admises au pays des droits fondamentaux », *AJDA*, 2021, p. 761 à 763.
[1277] En ce sens, CC, décision n° 2020-834 QPC, 3 avril 2020, § 8.
[1278] *Infra*., n° 660.
[1279] Le qualificatif de « *old constitutions* » est empruntés à SMITH E., *Constitutional justice under old constitutions*, *Revue internationale de droit comparé*, 1996, n° 4, p. 972 à 974.

frappant, mais aussi le plus médiatisé de ces dernières années, et ce malheureusement parmi d'autres[1280], concerne l'affaire « *Loomis* » aux Etats-Unis d'Amérique[1281]. En effet, qu'il s'agisse du prévenu ou de la juridiction qui recourt au logiciel *Compas*[1282], les informations sur le logiciel n'ont pas pu être communiquées dans leur intégralité car elles relèvent du secret commercial[1283], surtout lorsque l'on connaît les biais raciaux de ces algorithmes[1284]. En effet, les juges se voyaient uniquement communiquer les probabilités de récidive du prévenu sans connaître la manière dont ces dernières sont calculées, ce qui ne permet pas d'observer le comportement du logiciel. Bien qu'il s'agisse d'un outil d'aide à la prise de décision à la disposition des juges, c'est-à-dire que les juges peuvent tout à fait s'en émanciper, force est de constater qu'il exerce une influence sur la manière dont est rendue la justice. Cette absence de transparence n'a pas permis de remettre en cause l'utilisation d'un tel outil, notamment parce que la condamnation n'était pas exclusivement automatisée, mais a pu contribuer à un enfermement algorithmique des juges sans possibilité de contradictoire sur ce point.

659. Par ailleurs, les exemples de primauté du secret par le législateur sur la transparence des algorithmes sont légion, dénaturant en outre l'esprit de la LRN de 2016, puisque nous assistons à l'instauration de plus en plus de secrets. A titre d'exemple, le secret des délibérations des équipes pédagogiques à l'Université s'est ajouté aux secrets traditionnellement protégés par la loi concernant les prises de décision fondées sur des traitements algorithmiques[1285]. Cette tendance était déjà palpable dès les travaux préparatoires de la LRN[1286] qui ont mis en exergue un conflit entre la transparence et le secret des algorithmes. En effet, certains députés n'avaient pas hésité à déposer des amendements[1287] dans lesquels les logiciels utilisés par les services

[1280] RAMEY C., « A New York, un algorithme aide les juges à décider qui sera libre en attendant son procès », *in The Wall Street Journal & l'Opinion*, 22 septembre 2020.
[1281] SUPREM COURT OF WISCONSIN, State of Wisconsin v. Loomis, case 2015AP157-CR [en ligne]. [Consulté le 22 juin 2020]. Disponible à l'adresse : https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690
[1282] Les juridictions du Wisconsin ont recours au logiciel d'aide à la prise de décision appelé *Compas* afin d'étudier le taux de récidive des détenus dans le but de fixer la peine d'emprisonnement. Le taux de récidive de Monsieur Loomis a été considéré par un algorithme comme élevé, ce qui a pu influencer les juges dans la fixation de la poursuite de son emprisonnement. Or, ni la juridiction, ni Monsieur Loomis ne se sont vus communiquer les règles définissant le traitement algorithmique compte tenu du secret industriel et commercial argué par la société *Northpoint* qui développe le logiciel en question, rendant difficile la preuve de l'éventuelle violation des droits de la défense.
[1283] HARVARD LAW REVIEW, *State v. Loomis, Wisconsin Suprem Court Requiers Warning Before Use of Algorithmic Risk Assessments in Sentencing*, *Havard Law Review*, 2017, vol. 130, n° 5, p. 1530, Harvardlawreview.org [en ligne] [Consulté le 2 septembre 2020]. Disponible à l'adresse : https://harvardlawreview.org/2017/03/state-v-loomis/
[1284] MAYSON S, G., Bias In, Bias Out, The Yale Law Journal, 2019, n° 128, p. 2218, *Papers.ssrn.com* [en ligne]. [Consulté le 2 février 2020]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3257004#
[1285] *Supra* n° 465 et s.
[1286] La loi pour une République numérique de 2016 met en place une certaine transparence des décisions administratives individuelles prises sur le fondement de traitements algorithmiques. Pour plus de précisions, *Supra*., n° 435 et s.
[1287] Voir en ce sens, DURON P., FAURE O., amendement n° 462 et n°546 au projet de loi pour une République numérique, 14e législature, 16 janvier 2016, *Assemblée-nationale.fr* [en ligne]. [Consulté le 23 mai 2020]. Disponible à l'adresse : http://www.assemblee-nationale.fr/14/amendements/3399/AN/462.asp et http://www.assemblee-nationale.fr/14/amendements/3399/AN/546.asp (Amendement non soutenu pour O. Faure et retiré pour P. Duron).

publics industriels et commerciaux ne devaient pas être considérés comme des documents administratifs afin que leur code source ne soit pas communicable pour des raisons d'innovation, notamment parce que « *l'exception liée au secret en matière industrielle et commerciale ne constitue pas un rempart suffisant* »[1288] selon eux. Cette tendance pour le secret est également présente dans le RGPD et sa loi de transposition dans notre droit national dans la mesure où il fait primer la transparence sur la propriété intellectuelle[1289]. Et plus récemment, par la transposition de la directive sur le secret des affaires qui protège également le secret des algorithmes, et donc s'oppose à l'accès à l'information[1290]. Le penchant pour le secret de ces algorithmes est inhérent à la problématique de la protection de l'innovation[1291], notamment car le brevet n'est pas la voie la plus retenue par les acteurs économiques car il implique une publicité de nombreuses caractéristiques. Le secret a des incidences jusque dans les expertises ordonnées judiciairement puisqu'il n'est pas sans les entraver ou du moins les rends complexes du point de vue juridique[1292]. Notons tout de même que dans certaines hypothèses, le secret est nécessaire pour respecter les droits d'autrui, comme la vie privée, mais nous y reviendrons[1293]. Aujourd'hui, à un moment où le législateur européen et national donne une place de plus en plus importante au secret, il est impératif de pouvoir empêcher cette opacité constitutionnellement permise.

660. Il existe également des freins juridictionnels à la protection des droits et libertés à l'ère du numérique. Ces difficultés étaient déjà observables sur le terrain classique[1294], mais le numérique a renforcé ce constat. En l'occurrence cet échec repose notamment sur le contrôle abstrait effectué par le Conseil constitutionnel. Certes, dans le cas de la QPC, nous avons l'émanation d'un contrôle concret puisque ce contrôle de constitutionnalité de la loi va être déclenché par une affaire précise. Toutefois, elle va déboucher sur un contrôle théorique des normes entre elles mais sans prendre en considération le cas d'espèce[1295]. Comment est-il

[1288] *Ibid.*
[1289] Le considérant 63 du RGPD précise par exemple que le droit à l'information des personnes concernées par un traitement de données personnelles « ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel ».
[1290] Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires.
[1291] MARTY F., « *La protection des algorithmes par le secret des affaires, entre risques de faux négatifs et risques de faux positifs* », *Revue internationale de droit économique*, 2019/2, p. 211 à 237.
[1292] MIGAYRON S., « *Contradictoire et confidentialité dans les expertises des litiges du monde numérique : une mission impossible* », *op. cit.*
[1293] *Infra*., n° 690 et s.
[1294] RRAPI P., Le « contrôle abstrait » de constitutionnalité comme obstacle à l'identification des discriminations, *La Revue des Droits de l'Homme*, 2016, n° 9 [en ligne]. [Consulté le 23 mars 2020]. Disponible à l'adresse : https://journals.openedition.org/revdh/2060?lang=en
[1295] HAULBERT M., *L'interprétation normative par les juges de la QPC*, *Dalloz*, coll. Nouvelle Bibliothèque de Thèses, 2020, p. 89.

possible de considérer qu'une protection des droits fondamentaux ne puisse s'effectuer que de cette manière alors que tous les droits et libertés ne peuvent se valoir dans toutes les situations.

> « *Le Conseil constitutionnel procède à la transformation de la question de constitutionnalité initialement posée, en adoptant une posture de contrôle abstrait de constitutionnalité, qui devient un argument de justification de son autolimitation* »[1296].

661. En d'autres termes, ce contrôle abstrait empêche de considérer que la situation vécue par un requérant est inconstitutionnelle. La difficulté de ce type de contrôle est de pouvoir considérer que d'un point de vue abstrait il n'existe pas une violation des droits et libertés, alors que la situation provoquée par la loi au cas d'espèce l'est.

662. Il convient de reconnaître que compte tenu de l'immixtion croissante et des effets juridiques engendrés par l'utilisation de ces systèmes automatisés sur les individus, mais également sur les personnes morales de droit privée ou publique, l'opposabilité d'une autre exigence constitutionnelle ne doit pas faire triompher l'opacité.

663. Il existe un aléa significatif quant à la reconnaissance d'un principe de transparence des traitements algorithmiques par le juge constitutionnel et rien ne s'oppose dans notre ordre juridique à rendre inopérant un tel principe par la multiplication des secrets. Les secrets protégés par la loi et autres sources constitutionnelles empêchent qu'une transparence de ces traitements algorithmiques soient découvertes par le juge constitutionnel. La difficulté réside dans le fait que l'Etat ne doit pas plus assurer cette transparence par lui-même car il pourrait menacer d'autres libertés comme la vie privée. Le libéralisme s'est fondé contre l'Etat. La difficulté aujourd'hui réside dans le fait de concilier ce libéralisme avec la menace privée. L'Etat peut-il remplir ce rôle ? Du moins, il doit avaliser, par l'intermédiaire de la légitimité politique, une institution indépendante qui en aurait la charge[1297].

PARAGRAPHE 2 – Vers l'émergence de nouvelles sources constitutionnelles

664. Force est de constater qu'à l'échelon international de nouvelles sources sont en train d'émerger en réponse au fait juridique étudié, à savoir les traitements algorithmiques. La

[1296] RRAPI P., Le « contrôle abstrait » de constitutionnalité comme obstacle à l'identification des discriminations, *op. cit.*
[1297] *Infra*., n° 717 et s.

transparence des traitements juridiques y prend une part conséquente (A), mais nous proposons la constitutionalisation d'un principe unique de transparence hiérarchisant certaines sources afin d'empêcher que le juge constitutionnel ne dénature celui-ci (B).

A - Les principes candidats à la constitutionnalisation de la transparence

665. Les droits et libertés ne connaissent pas un destin linéaire. De nouvelles libertés sont susceptibles d'apparaitre, tandis que d'autres disparaissent, et ce au gré des rapports de force politiques, mais également de l'émergence de nouvelles technologies qui en modifient inéluctablement l'équilibre[1298]. D'une part, certaines libertés sont revendiquées par le corps social pour répondre à une problématique donnée, et d'autres ont un rôle également plus technique, notamment parce qu'elles ont vocation à les rendre effectives. La transparence est une clé de voûte et s'inscrit dans une réponse globale à l'émergence d'un fait juridique nouveau qu'est l'apparition du numérique. Il ne s'agit pas d'un simple principe ou parfois d'un droit, dans la mesure où il conditionne l'exercice des autres libertés, y compris celles d'autres générations.

666. A la manière de Karel Vasak qui fut l'un des premiers à théoriser l'idée de générations de droits[1299], Lawrence Lessig part également du postulat que chaque époque a été confrontée à un risque potentiel pour les droits et libertés nécessitant de fait une régulation[1300]. Pour justifier ses propos, il aborde une démarche chronologique. Tout d'abord il y eut selon lui le libéralisme politique qui permit d'obtenir de la part de l'Etat des garanties, une non-ingérence de la sphère publique pour que puisse s'exercer certains droits de l'individu ; ce que nous appelons en France, les droits civils et politiques. Mais les libertés ne peuvent pas être garanties uniquement parce que l'Etat aurait décidé de ne pas intervenir. Puis, il relève que face aux injustices économiques il fallut également réguler, ce qui donna lieu, si nous poussons le raisonnement, à ce que nous appelons en Europe les droits sociaux. Nous assisterions désormais à un nouvel âge, celui du cyberespace : âge dans lequel les puissances économiques jouent un rôle prédominant et contre lequel l'Etat a toute sa place pour limiter leur emprise sur les individus[1301]. Il s'oppose par ailleurs aux personnes qui considèrent que le seul ennemi des libertés individuelles ne peut être que l'Etat. Par ailleurs, les militants d'un cyberespace libre

[1298] LETTERON R., *Libertés publiques*, édition 2020, p. 21.
[1299] VASSAK K., « Les différentes catégories des droits de l'homme », *in* LAPEYRE A., DE TINGUY F., VASAK K. (dir.), *Les dimensions universelles des droits de l'homme*, UNESCO-Bruylant, 1990, p. 297 à 316.
[1300] LESSIG L., *Code version 2.0, op. cit.*
[1301] *Supra.*, n° 605 et s.

qui imaginaient le cyberespace comme une sphère refuge libérée de la contrainte des Etats ne fut qu'illusion comme le rappelle Félix Tréguer[1302]. En effet, nous constatons aujourd'hui que là où l'Etat n'était pas, le marché avait pris sa place, notamment en capitalisant sur la collecte de données personnelles[1303]. Et lorsque l'Etat a fait son immixtion dans la sphère numérique, et parfois par l'intermédiaire du code[1304] et donc de technologies le plus souvent opaques, c'est souvent dans l'optique d'une restriction des droits et libertés, ce qui ne trancha pas avec l'idée selon laquelle l'Etat peut également être une puissance brimeuse de libertés lorsque cette dernière n'est pas correctement encadrée.

667. Les personnes morales et physiques à la puissance moindre se retrouvent d'une part tiraillées entre la puissance de l'Etat, ne les protégeant pas dans cette sphère numérique, et d'autre part, les géants du numérique qui ont su agréger suffisamment de puissance, grâce parfois à d'autres Etats qui ont encouragé leur développement. Cela nécessite une prise en considération politique, et donc constitutionnelle, afin de les réguler. Il ne s'agit pas d'instituer ces géants du numérique, mais de considérer de manière pragmatique qu'ils sont tout aussi susceptibles d'affecter par les outils algorithmiques, les droits et libertés protégés par l'Etat dans un but d'intérêt général[1305].

668. Il ne fait guère de doute sur le fait qu'une Charte des droits et libertés à l'ère du numérique fera son apparition dans les prochaines années[1306]. En effet, de nombreux projets de Chartes constitutionnelles ont fait leur émergence aussi bien en France que dans le reste du monde. La question est donc de savoir quels sont les principes qui la constitueront. Comme nous l'avons vu, la transparence est fondamentale, mais il convient d'étudier quelle est la technique juridique, en l'occurrence, le ou les principes qui seront les plus à même d'y contribuer et méritent par là même une protection constitutionnelle.

669. Si nous nous concentrons sur les quelques tentatives d'établissement d'une Charte constitutionnelle des droits du numérique en France, la transparence de la technique, et donc des traitements algorithmiques, n'y figure pas expressément. Tel est le cas dans la proposition de Charte du numérique de 2018 qui fut retirée après discussion devant le Parlement[1307] ainsi

[1302] TREGUER F., *L'utopie déchue : une contre-histoire d'internet XVe-XXIe*, *Fayard*, 2019, 350 p.
[1303] ZUBBOF S., *L'âge du capitalisme de surveillance Le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, *Zulma*, 2020, 856 p.
[1304] GROFFE-CHARRIER J., « La loi est-elle dictée par le code ? », *Dalloz IP/IT*, 2020, p. 602.
[1305] *Supra.*, n° 613 et s.
[1306] LATIL A., « En attendant la Déclaration de droits fondamentaux du numérique », *op. cit.*, p. 593.
[1307] PAULA F., BAICHERE D et al., amendement n° 2169 au Projet de loi constitutionnelle pour une démocratie plus représentative, responsable et efficace, 15e législature, Assemblée nationale, enregistré à la Présidence de l'Assemblée

que dans la proposition de charte de l'IA et des algorithmes[1308] déposée en 2020. Cette dernière évoque certes la mise en place d'audit des systèmes algorithmiques[1309], mais qu'à des fins de mesure de l'autonomie décisionnelle.

670. Lorsque l'on étudie les projets de déclaration de droits numériques des autres Etats, il apparait que la transparence revêt également plusieurs dimensions, ce que nous avons par ailleurs pu constater en France et en Europe dans le droit infra-constitutionnel. En effet, dans une recherche du Berkman Klein Center[1310], répertoriant les principes de l'IA, il a été démontré que l'exigence de transparence des traitements algorithmiques fait consensus. Le principe de transparence figure d'ailleurs au premier plan des propositions, mais parfois il s'exprime à travers des principes divers. Il existe donc une bifurcation entre ce principe et d'autres pouvant y concourir. Certaines sources sont effectivement plus précises sur la façon dont la transparence doit s'opérer, ce que nous avons également constaté en droit national. A titre d'exemple, la transparence n'est pas explicitement désignée en tant que telle en droit public. Elle s'opère en effet à travers les principes existants du droit public et dont certains ont valeur constitutionnelle, ou à travers d'un droit d'information et d'explication[1311]. En revanche, en matière de donnée à caractère personnel, bien que la transparence existe, elle est associée à des concepts juridiques propres au droit des contrats tels que la loyauté, l'équité, et parfois à un droit à l'explicabilité. Dans cette étude, il est à noter que le principe de responsabilité apparaît distinctement de la transparence alors qu'elle y concourt comme nous avons pu le constater[1312].

671. Cette tendance n'est pas propre aux projets de déclaration des Etats, mais se retrouve également dans les propositions de chartes éthiques privées. La transparence est classiquement citée dans l'acception que nous avons étudiée en première partie. Nous y retrouvons également l'explicabilité, le droit à l'information, la notification qu'un système est intervenu dans la prise de décision, ou encore le fait qu'une interaction avec une IA a eu lieu.

---

nationale le 6 juillet 2018 [en ligne]. [Consulté le 23 avril 2021]. Disponible à l'adresse : http://www.assemblee-nationale.fr/dyn/15/amendements/0911/AN/2169

[1308] RAPHAN P-A., proposition de loi constitutionnelle relative à la Charte de l'intelligence artificielle et des algorithmes n° 2585, 15e législature, enregistré à la Présidence de l'Assemblée nationale le 15 janvier 2020. [en ligne]. [Consulté le 23 avril 2021]. Disponible à l'adresse : http://www.assemblee-nationale.fr/dyn/15/dossiers/charte_intelligence_artificielle_algorithmes

[1309] Art. 5 de la proposition : *« Il est nécessaire de mettre en place un système d'audit dont la fréquence de mise en œuvre est fondée sur celle d'évolution vers une autonomie décisionnelle du ou des algorithmes composant le système tel que défini à l'article premier ».*

[1310] FJELD J, ACHTEN N, HILLIGOSS H, NAGY A, SRIKUMAR M., Principled *Artifical Intelligence : Mapping Consensus in Ethical and Rights-Based Approches to Principles for AI*, Berkman Klein Center Research Publication, n° 2020-1 [en ligne]. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482

[1311] *Supra.*, n° 84 et s.

[1312] *Supra.*, n° 209.

672. Plus curieusement, certaines Chartes comme celle du Conseil de l'Europe en matière judiciaire[1313], associent un principe de transparence à l'utopie de la neutralité afin d'aboutir à l'absence de biais algorithmique, alors que l'état de l'art ne peut l'accomplir qui plus est parce qu'ils sont inhérents à l'humanité[1314]. L'objectif devrait être en revanche de tempérer leur exacerbation. Il est par ailleurs souligné que ce principe de transparence est à concilier avec la propriété intellectuelle selon cette charte[1315], tout en n'excluant pas qu'une transparence absolue doivent s'appliquer pour les applications les plus sensibles[1316].

B - La reconnaissance a minima d'une source générale et hiérarchisante

> « *comme le texte religieux, philosophique ou littéraire, le texte juridique est enjeu de luttes du fait que la lecture est une manière de s'approprier la force symbolique qui s'y trouve enfermée à l'état potentiel* »[1317].

673. La Constitution est un guide[1318] et elle n'a pas pour objet de régir toutes les situations. Néanmoins, force est de constater que l'émergence d'un nouveau fait juridique exige l'intervention du pouvoir constituant afin de lier l'interprète qu'est le juge constitutionnel, puisqu'en effet, lorsque les sources deviennent trop générales, voire contradictoires[1319], ce qui est normalement typique des anciennes constitutions, le travail d'interprétation devient trop conséquent et est susceptible de perdre en légitimité démocratique. Et lorsque le pouvoir constituant ou le juge constitutionnel laissent au législateur le soin de dénaturer l'équilibre des droits, parce que les sources constitutionnelles cessent d'être un guide, c'est tolérer le basculement d'un Etat de droit à un Etat légal.

674. Bien que nous ne pensions pas qu'il existe spécifiquement des générations de droit, le numérique exige une nouvelle conciliation des droits. L'enjeu est alors double : d'une part, il convient d'empêcher l'Etat de restreindre les libertés dans la sphère numérique, et par là même

---

[1313] CEPEJ, Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, principe n° 4 [en ligne]. [Consulté le 2 février 2021]. Disponible à l'adresse : https://rm.coe.int/charte-ethique-fr-pour-publication-4-decembre-2018/16808f699b

[1314] MAYSON S, G., Bias In, Bias Out, *op. cit.*

[1315] CEPEJ, Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, principe n° 4, *op. cit.*

[1316] *Ibid*.

[1317] BOURDIEU P., « La force du droit. Eléments pour une sociologie du champ juridique », *Actes de la recherche en sciences sociales*, 1986, 64, p. 3.

[1318] TROPER M., « L'interprétation constitutionnelle », *in* MELIN-SOUCRAMANIEN F. (dir.), *L'interprétation constitutionnelle*, *Dalloz*, 2005, p. 13.

[1319] Tel est par exemple le cas des différentes acceptions du droit de propriété présentes dans notre bloc de constitutionnalité. En ce sens, LETTERON R., *Libertés publiques*, *op. cit.*, p. 21.

celles du terrain classique, et d'autre part, utiliser la puissance de l'Etat pour contraindre l'agrégation de puissance privée, à savoir celles des géants du numérique, qui remet en cause l'autonomie des citoyens en démocratie ainsi que les libertés protégées. C'est donc d'un autre équilibre des droits et libertés dont nous avons besoin, que le seul libéralisme politique ne peut satisfaire. Par conséquent, les déséquilibres engendrés par les puissances technologiques privées doivent être prise en considération. Seule une source commune peut alors remplir cette mission. Il ne s'agit pas de libertés numériques à proprement parler car elles permettent également d'assurer que les arbitrages effectués dans le cadre du numérique n'aient d'incidences trop importantes sur les libertés du terrain classique.

675. Des auteurs comme Jean-François Kerléo souhaitent « *la reconnaissance d'un principe constitutionnel de transparence de la vie publique* »[1320] afin de centraliser en une source la multitude de principes ou d'objectifs à valeur constitutionnelle pouvant contribuer à la transparence de la vie publique. Un tel principe serait certes plus général que les sources actuelles, mais encore insuffisant sur la question des algorithmes publics, et ne permettrait pas de concourir à la transparence des algorithmes des puissances privées, y compris ceux utilisés par l'administration[1321]. En effet, il convient d'assurer une réponse à l'immixtion de ces nouvelles technologies, et pour ce faire, il est impératif de mettre en œuvre les techniques juridiques susceptibles de les observer, et le cas échéant de les réglementer.

676. Il ne suffit pas de proposer de simples déclarations d'intention, le plus souvent sur des technologies nommément désignées, et à l'ineffectivité juridique rapide et certaine, ainsi qu'à la valeur normative et à l'invocabilité discutable. Pourtant, il existe des candidats qui rempliraient un rôle juridique majeur de protection des droits et libertés. Plus qu'un principe et qu'un droit, lorsqu'elle est reconnue comme telle[1322], la transparence des traitements algorithmiques ne conditionnerait pas seulement l'exercice d'une nouvelle génération de droits, mais participerait également à l'effectivité de tous les droits remis en cause par la sphère numérique.

677. Nous déduisons de cela qu'une source générale inhérente à la transparence est la plus appropriée car elle contient *de facto* les différentes acceptions de la transparence, y compris des

[1320] KERLEO J-F., « La constitutionnalisation d'un principe de transparence de la vie publique », *ADJA*, 2020, p. 1137.
[1321] A titre d'exemple, les outils numériques les plus sophistiqués et les plus polémiques comme la reconnaissance faciale sont développés par des entreprises privées alors que l'Etat les déploie afin de prévenir les atteintes à l'ordre public.
[1322] Lorsque cela est possible techniquement, et qu'il convient de nécessiter une transparence juridique directe, c'est-à-dire sans tiers de confiance, il est alors fondamental de permettre un droit à la transparence subjectif, offrant la faculté pour une personne juridique de s'en prévaloir, comme c'est par exemple le cas aujourd'hui avec le droit d'accès à ses données personnelles.

principes qui y concourent, tout en permettant au législateur de déployer la technique juridique de la transparence qu'il jugera la plus opportune en fonction des secteurs. Dans cette hypothèse le secret ne s'opposerait pas à la transparence des algorithmes mais uniquement à une transparence directe, c'est-à-dire qu'une transparence par un tiers de confiance, institutionnellement garanti et indépendant, devra être effectuée dans le but d'un contrôle démocratique[1323].

678. Ainsi, de nouveaux principes pourront également être dégagés de cette source générale, et ce au fur et à mesure de la confrontation du juge à la technique, et surtout, il conviendra au législateur d'utiliser la technique juridique la plus adaptée à la matière concernée. De plus, le législateur se heurterait à l'incompétence négative au titre de l'article 34 de la Constitution combiné avec cette exigence constitutionnelle s'il n'épuisait pas sa compétence en la matière. La transparence algorithmique pourrait également être combinée avec les principes de transparence de la vie politique, ce qui offrirait des exigences de transparence plus strictes, à savoir directe des individus vis-à-vis de l'Etat, restreignant la possibilité de nombreux secrets protégés par la loi.

679. L'avantage de l'autonomisation d'un principe de transparence qui serait propre au numérique est qu'il permet la construction d'un régime juridique particulier. Dès lors, il est possible de répondre spécifiquement à l'émergence d'un fait juridique, ce qui implique en l'occurrence une nouvelle conciliation des droits et libertés propres à la sphère numérique. C'est d'ailleurs la force des constitutions récentes, par opposition aux vieilles constitutions, que de permettre au pouvoir constituant d'effectuer certains rééquilibrages, et par là même davantage cadrer l'interprétation du juge constitutionnel[1324]. Cette technique juridique de l'autonomisation est également l'occasion, lorsque c'est le pouvoir constituant qui la consacre, de faire primer certaines valeurs constitutionnelles sur d'autres. John Perry Barlow, qui fut certes libertarien assumé, et œuvrant pour un cyberespace libre et donc libéré de toute emprise étatique, avait émis l'hypothèse selon laquelle le cyberespace se détachait du monde physique, et que les droits du monde « matériel » ne s'y appliquaient pas[1325].

680. De manière pragmatique, une source constitutionnelle devra se prémunir des risques de primauté de la culture du secret sur la transparence des traitements algorithmiques, ne serait-ce

[1323] *Infra*., n° 694 et s.
[1324] DELPEREE F., « L'interprétation de la constitution ou la leçon de musique », *in* MELIN-SOUCRAMANIEN F. (dir.), *L'interprétation constitutionnelle*, *Dalloz*, 2005, p. 243.
[1325] BARLOW J-P., Déclaration d'indépendance du cyberespace, *op. cit.*

car le Conseil constitutionnel n'est pas actuellement un contre-pouvoir suffisant[1326]. La reconnaissance d'un principe général sur la question de la transparence de ces algorithmes n'est pas à espérer de la part du juge constitutionnel, sans doute parce que cela nécessiterait un travail d'interprétation inconsidéré au regard des multiples sources constitutionnelles, parfois contradictoires, et ce d'autant plus qu'il ne s'en sent peut-être pas la légitimité.

681. Notre temps exige une Charte venant préciser des droits et principes, et dont la transparence serait la clé de voûte afin de lever l'ambiguïté sur la conciliation entre les droits à l'ère du numérique, ce qui ne veut pas dire que cette conciliation serait identique concernant les droits du terrain classique. En effet, elle ne vaudrait que pour la sphère numérique, ce qui implique également de renoncer à une interprétation abstraite[1327] des droits et libertés par le juge constitutionnel[1328] puisque c'est non pas la règle de droit, mais la technique qui dénature l'équilibre entre les libertés. Certes, il convient de reconnaître que dans certains cas de figure les algorithmes privés ne pourront pas être publiés au regard d'autres impératifs, mais dans ce cas ils devront au moins être analysés par des services institués par l'Etat et indépendants. C'est pourquoi ce principe constitutionnel devra ensuite être mis en œuvre de la manière la plus adaptée, secteur par secteur, par un législateur dédié[1329]. Cette source n'empêchera toutefois pas la transparence juridique de ces outils numériques puisqu'elle devra avoir lieu d'une manière ou d'une autre, c'est-à-dire de façon directe, auprès des personnes physiques et morales, ou indirecte, par une institution.

682. Nous relevons que *« concilier, c'est faire aller ensemble des points de vue différents mais égaux. Là où l'intégration incite à une sorte de discrimination positive en faveur du dernier arrivé dans le bloc de constitutionnalité, la conciliation place tous les intérêts et objectifs à égalité* »[1330]. Sans pour autant considérer qu'un principe de transparence des traitements algorithmiques doive être absolu, cela implique donc une conciliation. Mais force est de constater que les intérêts et objectifs ayant valeur constitutionnelle ne peuvent être considérés à égalité[1331], au risque de conférer au juge constitutionnel des marges d'appréciation

[1326] *Infra*., n° 690 et s.
[1327] Il convient d'entendre par contrôle abstrait *« lorsque c'est la norme en elle-même qui est critiquée et non son application à un cas ou une situation précise »*, ROUSSEAU D., *La justice constitutionnelle en Europe*, *Montchrestien*, 3e éd, 1998, p. 79.
[1328] HAULBERT M., *L'interprétation normative par les juges de la QPC, op. cit.*, p. 89.
[1329] *Infra*., n° 745 et s.
[1330] HEDARY D., « Les surprises de la Charte de l'environnement : analyse des quatre années de jurisprudence », *Droit de l'environnement*, n° 171, septembre 2009, p. 11.
[1331] *« Toutes les dispositions constitutionnelles n'ont pas la même importance ni la même dignité morale ou politique »*, VEDEL G., « *Souveraineté et supra constitutionnalité »*, in *La souveraineté, Revue Pouvoirs*, n° 67, novembre 1993, p. 84. Pour autant, selon nous, le fait pour le pouvoir constituant de venir préciser la conciliation des droits en réaction à un fait juridique en

trop importantes, surtout lorsqu'il ne fait plus aucun doute que certaines libertés peuvent dénaturer l'exercice de certains droits et libertés s'ils sont appliqués de la même manière à la sphère numérique, ce que nous avons constaté avec le secret qui est de plus en plus opposé à la transparence des algorithmes par exemple. Dès lors, il apparaît nécessaire dans la rédaction de ce principe, qui concerne aussi bien la transparence des programmes utilisés par la puissance publique, que de ceux déployés par les géants du numérique, d'indiquer la primauté de cette transparence sur la propriété, les secrets protégés par la loi ou encore la liberté d'entreprendre.

683. Il ressort des projets de déclaration de droit du numérique à l'échelle mondiale[1332] que la transparence des outils numériques ne doit pas se heurter à la vie privée des individus, ce qui est tout à fait compréhensible dans une acception libérale. Et c'est également ce que nous soutenons. Il n'y a pas d'incompatibilité à promouvoir une transparence des autorités publiques ainsi que des grands acteurs privés bénéficiant d'une agrégation de puissances suffisante pour remettre en cause les droits et libertés, ce qui n'empêche pas le cas échéant de contrôler les acteurs plus faibles. L'individu doit bénéficier d'une protection particulière, car il en va de son épanouissement, et parce qu'il est par nature vulnérable aux autres puissances. Dès lors, il ne serait pas incompatible dans une Charte des droits et libertés à l'ère du numérique d'exiger la transparence tout en protégeant et assurant l'anonymisation des données nécessaires à la compréhension des traitements algorithmiques.

684. L'objectif d'un tel principe est alors de s'assurer que rien ne peut s'opposer juridiquement à cette transparence. Dans l'hypothèse où la transparence technique n'est pas assurée, nous évoquerons la manière dont il conviendra d'agir[1333].

hiérarchisant des principes constitutionnels par rapport à d'autres n'est pas de la supraconstitutionnalité, mais une volonté de limiter l'interprète qu'est le juge constitutionnel lui permettant ainsi de jouir d'un travail d'interprétation au sein de cette sphère.

[1332] FJELD J, ACHTEN N, HILLIGOSS H, NAGY A, SRIKUMAR M., Principled *Artifical Intelligence : Mapping Consensus in Ethical and Rights-Based Approches to Principles for AI*, *op. cit.*

[1333] *Infra*., n° 900 et s.

CONCLUSION DU CHAPITRE I

685. La transparence juridique ne doit pas constituer un frein à la recherche de la transparence technique des algorithmes dans la mesure où certaines technologies sont déjà opaques par nature[1334], ce qui complexifie leur étude.

686. Pour ce faire, il apparait que l'Etat est l'échelon le plus adapté et le plus légitime pour assurer aussi bien la transparence des traitements algorithmiques utilisés par les gouvernants que par les acteurs privés ayant la puissance suffisante pour concurrencer l'Etat. Il convient donc de reconnaître une nouvelle source constitutionnelle assurant la transparence juridique de ces algorithmiques, et ce dans la mesure où d'autres sources constitutionnelles pourraient actuellement facilement s'y opposer.

687. D'une part, la transparence permet d'élaborer l'architecture technique la plus en adéquation avec notre système juridique, et d'autre part, lorsque nous ne maîtrisons pas les architectures numériques déployées, parce que nous n'avons pas su nous immiscer dans leur conception, la conciliation des droits ne peut qu'être dynamique en fonction de la technique. Mais dans ce dernier cas de figure, seule la transparence est susceptible de guider la meilleure conciliation entre les libertés, afin de parvenir aux objectifs fixés ou le cas échéant d'exclure de tels traitements algorithmiques s'ils n'offrent pas les garanties suffisantes.

688. Il peut également arriver qu'une liberté, en fonction des considérations techniques du moment remettent en cause l'esprit d'une Constitution. Les interprètes doivent donc veiller à assurer cet équilibre en permanence, notamment en n'hésitant pas à opérer une conciliation différente du terrain classique, car propre à la sphère numérique. A ce titre, une nouvelle forme de contrôle de constitutionnalité opérée aussi bien par le juge constitutionnel qu'ordinaire pourrait être effectuée. Ce contrôle diffus permettrait par l'intermédiaire d'une juridiction spécialisée en droit numérique[1335], de mieux prendre en compte les spécificités du numérique et leur confrontation avec les normes constitutionnelles.

689. La constitutionnalisation de ce nouveau principe de transparence serait donc une clé de voûte garantissant les libertés actuelles et à venir, tout en offrant la possibilité, dans certains cas, d'en faire un nouveau droit subjectif dans les domaines ne nécessitant pas un tiers de

[1334] Tel est le cas de figure de certaines techniques d'apprentissage qui sont qualifiées de boîte noire. En ce sens, *Supra.*, n° 16.
[1335] *Infra*., n° 765 et s.

confiance, car le but serait d'assurer le respect du droit des tiers, tout en assurant la transparence auprès de la société.

CHAPITRE II - L'INDISPENSABLE EVOLUTION DES ORGANES DE CONTROLE ETATIQUE

690. Il serait optimiste et ambitieux d'imposer une méthode particulière afin d'obtenir la transparence des traitements algorithmiques. D'une part, car c'est souvent une question technique et non juridique, et d'autre part, car il convient d'obtenir une certaine neutralité juridique des moyens permettant d'y parvenir, ceci n'empêchant cependant pas de s'assurer que la théorie ne soit pas rendue ineffective par la réalité technique.

691. Dans la sphère numérique, la transparence est nécessairement fluctuante et nos travaux consistent à proposer une articulation entre le pouvoir politique et la technique afin qu'ils se nourrissent l'un l'autre, et que le régime démocratique s'adapte à ces enjeux en garantissant les droits et libertés fondamentales. Lawrence Lessig se demandait quelle forme l'Etat devrait prendre pour survivre[1336] dans ce nouvel univers. Nous proposons dans ces travaux l'un des modèles possibles d'articulation entre le pouvoir politique et informatique, et ce au service du principe de transparence des traitements algorithmiques constitutionnellement protégé[1337]. Comme nous l'avons vu lors du premier chapitre, l'Etat bénéficie d'une légitimité sans commune mesure par rapport aux acteurs privés, puisqu'il est l'incarnation de la souveraineté politique, et donc le préalable nécessaire à l'exercice de l'autonomie des citoyens en démocratie. Bien qu'il ne s'agisse pas de nier les progrès de l'informatique, et ses atouts lorsqu'il est au service des citoyens[1338], les pouvoirs constitués doivent s'adapter à ce fait juridique en permanente mutation.

692. Il apparaît que l'approche contemporaine, par une multitude d'autorités de régulation et de contrôle des traitements algorithmiques, affaiblit davantage la puissance publique plus qu'elle ne la renforce. Ainsi, nous proposons la création d'une autorité de contrôle unique dont la compétence sur la question de la transparence technique serait exclusive (Section 1).

693. Au regard du haut de niveau de technicité que nécessite la compréhension du numérique et de ses enjeux, et ce dans le but de respecter la traditionnelle séparation des pouvoirs, nous convenons qu'il serait préférable pour des raisons démocratiques qu'une troisième chambre

[1336] L'auteur constate que les institutions étatiques ne peuvent pas répondre en l'état à ce nouveau fait juridique, sans pour autant formuler une proposition : *« Liberty in cyberspace will not come from the absence of the state. Liberty there, as anywhere, will come from a state of a certain kind »*, nous traduisons, « La liberté dans le cyberespace ne viendra pas de l'absence de l'Etat. La liberté, là-bas, comme n'importe où, viendra d'un Etat d'un certain genre », LESSIG L., *Code version 2.0, op. cit.*, p. 4.
[1337] *Supra.*, n° 664 et s.
[1338] Art. 1 LIL modifiée indique que « *L'informatique doit être au service de chaque citoyen* ».

législative soit créée pour porter spécifiquement les débats sur ces sujets, et notamment sur la question de l'exercice du principe de transparence juridique des traitements algorithmiques. Enfin, une spécialisation de la justice dans ce domaine semble devenir également une évidence (Section II).

SECTION I - DE LA CREATION D'UNE AUTORITE DE CONTROLE UNIQUE

694. Alors que le législateur semblait convaincu, dans les années soixante-dix, par la création d'une autorité de régulation, force est de constater qu'au fil des décennies la CNIL a été affaiblie. Pour pallier ces insuffisances, de nombreux autres organes ont été créés et se sont vus confier une mission de transparence des traitements algorithmiques (Paragraphe 1). Ce modèle de régulation, en plus de heurter la traditionnelle séparation des pouvoirs, n'a pas su pour autant produire les résultats escomptés faute d'harmonisation. C'est la raison pour laquelle nous proposons une rationalisation de ces organes afin de concentrer une force publique suffisante, tout en offrant des garanties d'indépendance, et ce dans le but de concourir au mieux à la transparence des programmes informatiques ainsi que du matériel les exécutant, condition *sine qua non* à l'effectivité des droits à l'ère du numérique (Paragraphe 2).

PARAGRAPHE 1 – Une pluralité d'autorités de contrôle compétentes pour connaitre de la transparence des traitements

695. En appréhendant l'émergence d'un nouveau fait juridique à savoir le développement de l'informatique grand public, surtout au sein des administrations françaises, s'est très vite posée la question de la création d'une commission de régulation (A). Mais cette instance, spécialisée dans la protection des données à caractère personnel, a été concurrencée par d'autres organes chargés de la régulation des autres secteurs dans lesquels l'informatique a fait son immixtion, ce qu'il convient d'évoquer par l'intermédiaire de quelques illustrations (B).

A - Historique et rôle initial de la CNIL

696. Il nous paraît nécessaire de remonter à la création de la CNIL afin de comprendre quel est l'esprit qui sous tendait la première réponse à l'émergence du fait juridique étudié. Avant l'émoi suscité par l'affaire SAFARI révélée le 21 mars 1974 dans les colonnes du journal *Le*

Monde[1339], il était déjà question de réglementer l'informatique, en l'occurrence de doter la France d'un régime juridique sur les données à caractère personnel. En effet, en France, une proposition de loi est déposée par Michel Poniatowski à l'Assemblée nationale le 25 novembre 1970[1340]. Dans cette proposition, il est question de créer un comité de surveillance ainsi qu'un Tribunal de l'informatique. Puis, plus tardivement, en 1974, quelques semaines à la suite de l'article de Philippe Boucher, une nouvelle proposition de loi tendant à créer un directoire et un Tribunal de l'informatique est déposée au Sénat[1341]. Dans ce modèle, ce sont les propriétaires d'ordinateur qui doivent fournir à un directoire[1342] des informations sur le fonctionnement des traitements[1343]. Ce directoire aurait de plus bénéficié d'un pouvoir d'investigation concernant les traitements des organismes exerçant une mission de service public[1344], ce qui démontre que dans ce contexte, la première des menaces était la puissance publique. Il aurait été possible d'y enregistrer des plaintes, mais afin de respecter la traditionnelle séparation des pouvoirs, le directoire ne disposait pas de la compétence d'infliger des sanctions. En effet, cette autorité jouait uniquement un rôle de filtre afin de transmettre les plaintes fondées à un tribunal spécialement dédié à la matière informatique[1345]. Bien qu'intéressante, cette approche imparfaite ne sera pas retenue. Enfin, le 4 avril de la même année, une autre proposition de loi est déposée par Pierre-Bernard Cousté[1346], afin que soit uniquement créée *« une commission de contrôle des moyens informatiques* » dotée d'un pouvoir d'investigation et de la possibilité de transmettre des plaintes reçues au « *tribunal administratif de Paris siégeant en qualité de tribunal de l'informatique* »[1347].

697. Il faudra attendre l'élection présidentielle de 1974 et la constitution d'un nouveau gouvernement pour qu'un décret[1348] institue la Commission Informatique et Libertés en vue notamment d'aboutir à un nouveau régime juridique. La mission principale de cette commission

[1339] BOUCHER, P., « *Affaire SAFARI ou la chasse aux français* », *op. cit.*, p. 9.
[1340] Voir en ce sens, PONIATOWSKI M., proposition de loi tendant à la création d'un comité de surveillance et d'un tribunal de l'informatique n° 1454, 4eme législature, enregistré à la Présidence de l'Assemblée nationale le 25 novembre 1970.
[1341] CAILLAVET H., proposition de loi n° 144 tendant à créer un Directoire et un Tribunal de l'Informatique, seconde session ordinaire 1973-1974, Sénat, enregistrée à la Présidence du Sénat le 2 avril 1974.
[1342] Ce directoire aurait été composé de onze membres, à savoir deux membres nommés par le Président de la République, par l'Assemblée nationale, le Sénat, le Conseil d'Etat, par la Cour de cassation, ainsi que d'un Président nommé par les autres membres. *Ibid*., art. 1.
[1343] *Ibid*., art. 2.
[1344] *Ibid*., art. 3.
[1345] Le Tribunal de l'informatique aurait été composé de *« deux conseillers d'Etat désignés par le vice-président du Conseil d'Etat ; deux conseillers à la Cour de Cassation désignés par le premier président de la Cour ; un professeur agrégé de droit désigné par le Premier Ministre* ». *Ibid*., art. 5.
[1346] COUSTE P-B., proposition de loi n° 1004 tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens, 5eme législature, enregistré à la Présidence de l'Assemblée nationale le 4 avril 1974.
[1347] *Ibid*., art. 4.
[1348] Décret n° 74-938 du 8 novembre 1974 portant création de la commission Informatique et libertés.

était de proposer un régime juridique « *tendant à garantir que le développement de l'informatique, dans les secteurs publics, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques* »[1349]. Cette vision individualiste relative au respect de la vie privée correspondait essentiellement à la menace technologique de l'époque, mais n'appréhendait pas le risque collectif du recours aux traitements algorithmiques, alors même qu'il en était déjà question, certes de manière marginale et théorique, dans la doctrine[1350] et autres rapports[1351]. Le législateur s'est donc focalisé sur la problématique des données nominatives, car les incidences de l'informatique ne se limitaient essentiellement qu'à cela dans les années soixante-dix. Ainsi, l'esprit de cette décennie[1352], visant à garantir plus de transparence, s'est estompé et le législateur n'a pas su s'adapter à des problématiques nouvelles comme la gouvernance par les nombres[1353] ou encore la gouvernementalité algorithmique[1354], qui ont certes une incidence sur les individus, mais également sur la société, et sans qu'il s'agisse nécessairement de données à caractère personnel. En effet, comme nous l'avons vu, la société peut également être dans une situation de vulnérabilité vis-à-vis des traitements[1355].

698. Au-delà du travail de cette commission sur l'élaboration d'un cadre juridique, elle dispose dès sa création d'un pouvoir d'enquête afin de vérifier les traitements de données, sans qu'il ne soit précisé qu'il s'agisse de données à caractère personnel. Il existe donc dès 1974 l'existence des prémices d'une transparence juridique visant « *les répertoires et les fichiers informatisés* »[1356].

699. Dès 1975, date à laquelle le premier rapport de la Commission est rendu[1357] (le « rapport Tricot »), les bases de la future loi « informatique et libertés » sont posées[1358]. Toutefois, ce document met en exergue la nécessité que les missions de la future autorité de contrôle, à savoir la CNIL, ne devront pas porter seulement sur la question des traitements automatisés nominatifs

[1349] *Ibid*., art. 1.
[1350] BRAIBANT G., « La protection des droits individuels au regard du développement », *op. cit*.
[1351] Voir Rapport de la Commission Informatique et Libertés, *La Documentation Française*, 1975, et Rapport annuel du Conseil d'Etat, « Les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives », 1970.
[1352] Le législateur a su faire œuvre libérale dans les années soixante-dix avec la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, et enfin la loi n° 79-587 du 11 juillet 1979 relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public.
[1353] SUPIOT A., *La gouvernance par les nombres*, *op. cit*.
[1354] ROUVROY A., BERNS T., « Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation ? », *op. cit*.
[1355] DOUVILLE T., HERVOCHON C., NOEL E., PAQUIER Y., « Les vulnérabilités numériques », *op. cit*., p. 117.
[1356] Décret n° 74-938 du 8 novembre 1974 portant création de la commission Informatique et libertés, Art. 2.
[1357] Rapport de la commission informatique et libertés, La Documentation Française, 1975.
[1358] Nous y retrouvons par exemple le droit d'accès aux données nominatives, un des piliers en matière de transparence des traitements. *Supra.*, n° 127 et s.

opérés par les responsables de traitement publics et privés[1359]. En effet, les rapporteurs évoquent déjà leur souhait d'une extension des compétences de la future autorité aux « *libertés dans leur ensemble, et pas seulement à la protection de la vie privée* »[1360], ce qui ne sera cependant pas retenu dans la LIL de 1978. Ils avaient déjà d'ailleurs constaté dans leurs travaux qu'au-delà de la problématique des données à caractère personnel, des traitements algorithmiques pouvaient *« au moins indirectement, peser sur le sort des individus et des groupements et réduire en fait leurs libertés* »[1361]. Tout en proposant l'instauration d'un droit d'accès à ses données personnelles, un des piliers de la transparence de la future loi *« informatique et libertés* », les rédacteurs s'intéressent au fait qu'il conviendrait de discuter « *« les vérités » sorties des ordinateurs* »[1362]. Pour ce faire, il ne s'agit pas uniquement d'avoir accès à ses données pour le cas échéant les contester, mais discuter le processus informatique, et donc les résultats.

700. De ce point de vue, il est également question de mieux prendre en considération les données et décisions publiques. L'objectif est de pouvoir « *faire en sorte que les données enregistrées soient conservées sous une forme accessible, afin qu'il soit possible de vérifier que le traitement informatisé n'a pas reposé sur des bases fausses, incomplètes ou tendancieuses* »[1363] et que la « vérité » informatique doit être prouvée[1364]. De plus, la perspective des outils d'aide à la prise de décision informatisés, aussi bien publiques que privées, était appréhendée. Concernant ces outils, le rapport proposait qu'il « *serait nécessaire qu'obligation soit faite aux spécialistes de la construction et de la manipulation des modèles de faire connaître sans restriction la nature et la source des données qu'ils ont prises en compte, ainsi que toutes les démarches intellectuelles qui ont permis la construction des programmes* »[1365] et « *qu'il existe bien un danger de substitution de pouvoir ; les spécialistes du modèle tendent de facto à jouer un rôle majeur dans les processus de décision* »[1366].

701. Finalement, les travaux de cette commission ont été en grande partie repris par le Rapport Foyer[1367] de 1977 qui aboutira à la LIL de 1978[1368]. Nous ne pouvons que regretter

[1359] Rapport de la commission informatique et libertés, *op. cit.*, p. 89.
[1360] *Ibid.*, p. 71.
[1361] *Ibid.*, p. 21.
[1362] *Ibid.*, p. 80.
[1363] *Ibid.*, p. 80 et 81.
[1364] *Ibid.*
[1365] *Ibid.*, p. 83.
[1366] *Ibid.*, p. 82.
[1367] FOYER M., Rapport n° 3125 sur le projet de loi relatif à l'informatique et aux libertés de l'Assemblée nationale, 5e législature, fait au nom de la commission des Lois, enregistré à la Présidence de l'Assemblée nationale le 4 octobre 1977.
[1368] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

qu'au-delà du droit d'accès aux données nominatives ainsi que du pouvoir réglementaire, d'enquête et de recommandation et d'accueil des plaintes de la commission, le législateur ne soit pas allé aussi loin que le rapport Tricot en matière de transparence. Fait intéressant, un avis conforme concernant la création de données nominatives par les personnes publiques a été retenu, ce qui marque tout de même un embryon de contrôle *a priori* de ces traitements et la nécessité d'instauration d'un contre-pouvoir au pouvoir réglementaire par les techniciens composant la CNIL. Même si cette compétence a été retirée à la CNIL en 2004[1369], elle disposa en contrepartie d'un pouvoir de sanction administrative alors qu'initialement il n'était pas question qu'elle remplisse un rôle contentieux. En effet, dans les années soixante-dix, bien qu'elle soit considérée comme un contre-pouvoir technique, il existe un consensus sur le fait qu'elle ne doit pas empiéter sur les pouvoirs juridictionnels[1370].

702. La CNIL est donc la première AAI de l'histoire du droit français, du moins qualifiée en tant que tel par le législateur. Le pouvoir législatif souhaitait que cette commission soit indépendante du pouvoir politique dans le cadre de son budget, de sa composition ou encore de son fonctionnement. Comme nous l'avons vu, bien que les pouvoirs de la CNIL aient été renforcés au fil du temps, force est de constater qu'il existe de nombreuses insuffisances et que ce mode de régulation ne permet pas de juguler les menaces en matière de données à caractère personnel. Il est par ailleurs regrettable de constater que son champ d'intervention n'a que très peu évolué, dans la mesure où le législateur n'a pas su accompagner la CNIL dans la prise en considération de nouveaux enjeux[1371] et a préféré confier ces compétences à d'autres autorités.

B - Augmentation et concurrence des autorités de régulation en matière de transparence des algorithmes

703. L'affaiblissement de la CNIL s'explique par une conjonction de facteurs. Tout d'abord, comme nous l'avons vu, la commission n'a pas disposé d'une compétence générale sur les dispositifs informatiques, contrairement à ce qui était proposé par le rapport Tricot[1372], ce qui a encouragé la multiplication d'autres organes de régulation de la sphère numérique. Elle n'est donc plus apparue comme la seule institution garante de l'effectivité des droits et libertés au sein de l'environnement numérique. Son rôle était également devenu déstructuré d'un point de vue juridique à travers la reconnaissance d'un pouvoir de sanction alors qu'en contrepartie elle

[1369] *Infra.*, n° 748 et s.
[1370] Voir en ce sens, les propositions de loi étudiées ainsi que le Rapport Tricot, « *le comité ne doit pas être une juridiction* ».
[1371] *Supra.*, n° 697.
[1372] *Supra.*, n° 699 et s.

perdait ce qui faisait d'elle un véritable contre-pouvoir technique, à savoir l'avis conforme relatif à l'instauration par la puissance publique de certains traitements de données personnelles. La faiblesse de ses moyens humains et matériels alloués, qui dépendent également du législateur, n'est pas allé dans le sens d'une bonne observation des traitements algorithmiques publics et privés.

704. Lors de notre étude sur les principaux régimes juridiques œuvrant à une meilleure transparence des traitements algorithmiques[1373], nous avons pu constater que la réglementation était très sectorielle, ce qui n'est pas une mauvaise chose pour prendre en compte certaines particularités. Mais la concurrence entre les institutions de contrôle n'est pas saine[1374] puisque certaines d'entre-elles souhaitent étendre leurs prérogatives à la sphère numérique au détriment des autres, se décorrélant parfois de la poursuite de l'intérêt général. Et force est de constater que l'observation des algorithmes par une pluralité d'institutions, aboutit de fait à un éparpillement du contrôle public de ces derniers.

705. Toutes les instances de contrôle œuvrant pour une transparence des traitements algorithmiques ne bénéficient pas de la même autonomie, ni des mêmes compétences. Il est toutefois à noter que dans la continuité d'un élan de transparence de l'action administrative, la CADA a également été créée en 1978[1375]. Mais il a fallu attendre un avis du 8 janvier 2015 pour que le code source d'un logiciel de l'administration soit considéré comme un document administratif communicable, permettant à un administré d'effectuer une transparence directe, c'est-à-dire sans avoir à recourir à un tiers de confiance[1376], vis-à-vis d'un algorithme public. Il en va logiquement de même pour la communication de la documentation afférente à ces programmes afin de les expliquer, puisqu'en effet, sans ces compléments d'informations, le code source ne peut se suffire à lui-même. En revanche, lorsque des secrets sont protégés par la loi, cette transparence n'est pas garantie, ni opérée par cette instance en tant que tiers de confiance. De plus, la CADA ignore si les informations communiquées par les personnes publiques ou exerçant une mission de service public sont véridiques ou si un refus de communication est étayé dans la mesure où elle n'a pas accès aux documents et n'effectue pas

[1373] Il s'agit de la première partie de cette thèse. *Supra.*, n° 72 et s.
[1374] CHEVALLIER J., « L'intérêt général dans l'administration française », *Revue internationale des sciences* administratives, 1975, p. 329.
[1375] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.
[1376] CADA, avis n° 20144578 du 8 janvier 2015. Voir en ce sens les développements effectués dans le cadre de ces travaux, *supra.*, n° 415 et s.

d'enquête ou de contrôle[1377] pour s'en assurer. En interne, les services de l'Etat accompagnent cette mission de transparence des algorithmes publics, mais ne sont pas indépendants[1378].

706. Le défenseur des droits a déjà eu l'occasion de faire part de ses craintes en matière de discrimination au sujet de l'opacité entourant les traitements algorithmiques de la plateforme *Parcoursup*[1379].

707. Les techniques informatiques déployées en matière de renseignement sont en principe contrôlées par la Commission nationale de contrôle des techniques de renseignement (CNCTR), successeur de la Commission nationale de contrôle des interceptions de sécurité[1380]. Même si l'on considère que « *le secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire* »[1381], un contrôle démocratique doit être effectué afin de s'assurer que les algorithmes intervenant dans ce domaine sont conformes aux finalités autorisées par le Parlement, qui plus est lorsque certaines de ces prérogatives relevaient autrefois exclusivement de l'autorité judiciaire, alors qu'il s'agit désormais de prévenir des troubles à l'ordre public[1382]. La CNCTR est censée autoriser en amont, c'est-à-dire vérifier les techniques avant leur déploiement, ainsi qu'en aval, y compris, celles recourant aux traitements algorithmiques, puisqu'un important volet du renseignement est aujourd'hui numérique[1383]. En l'état, à défaut d'une transparence directe de ces dispositifs, la commission agit en tant que tiers de confiance, alors qu'elle n'est composée que d'un spécialiste en communications électroniques[1384]. Comme l'indique un rapport parlementaire, on ne peut pas considérer qu'elle remplit correctement sa mission[1385]. L'enjeu est de taille dans la mesure où, en plus des exigences liées à la protection

[1377] *Supra.*, n° 425.
[1378] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique, pour plus de précisions, *Supra*., n° 483.
[1379] Défenseur des droits, déc. n° 2019-021 du 18 janvier 2019. *Supra*., n° 471.
[1380] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.
[1381] CC, décision n° 2015-713 DC, 23 juillet 2015, *Loi relative au renseignement*, § 3.
[1382] Voir en ce sens, CATHERINE A., ALEXIA D., PAQUIER Y., POINSIGNON D., VICOMTE D., « Chronique de jurisprudence constitutionnelle française 2015 », *Les Cahiers de la Recherche sur les Droits Fondamentaux*, n° 14, 2016, p. 113 à 136.
[1383] Il s'agit de l'accès différé aux données techniques de connexion, de l'accès en temps réel aux données techniques de connexion, des traitements automatisés de données permettant de détecter des connexions susceptibles de révéler une menace terroriste, la géolocalisation en temps réel, les interceptions de sécurité, l'accès et le stockage de données informatiques ou encore l'interception des correspondances par la voie satellitaire. Voir en ce sens le Livre VIII du Code de la sécurité intérieure.
[1384] Cet unique spécialiste en communications électroniques est « *nommé[e] sur proposition du président de l'Autorité de régulation des communications électroniques et des postes.* », Art. L. 831-1 4° du Code de sécurité intérieure.
[1385] PAUL C., FERAL-SCHUHL C., Rapport n° 3119 Numérique et libertés : un nouvel âge démocratique de l'Assemblée nationale, 14e législature, fait au nom de la commission de réflexion et de propositions sur le droit et les libertés l'âge du numérique, enregistré à la Présidence de l'Assemblée nationale le 9 octobre 2015, p. 164 : « *Son contrôle devrait s'exercer sur l'ensemble des services de renseignement et l'intégralité des mesures et techniques qu'ils emploient, en amont de leur mise en œuvre sous la forme d'un avis préalable, durant leur application et en aval, sous la forme de contrôles sur pièces et sur place. Outre un pouvoir de recommandation, cette autorité devrait pouvoir transmettre au juge les cas dans lesquels elle estime que le pouvoir exécutif a méconnu les garanties accordées par la loi au citoyen.* », *Assemblée-nationale.fr* [en ligne]. [Consulté le 23 mars 2020]. Disponible à l'adresse : https://www.assemblee-nationale.fr/14/pdf/rapports/r3119.pdf

des droits et libertés des individus, les gouvernants sont susceptibles de mettre en œuvre des techniques informatiques développées par des opérateurs privés dont ils ne maitrisent pas les tenants et les aboutissants. La CNIL n'est de plus pas compétente pour contrôler ces traitements[1386], raison pour laquelle la CNCTR avait été instituée pour offrir plus de garanties. Dans le cadre des techniques de renseignement abordées, les trois algorithmes autorisés à ce titre sont encore en fonctionnement[1387]. Concernant spécifiquement les traitements automatisés de données permettant de détecter des connexions susceptibles de révéler une menace terroriste, ils ont récemment été pérennisés par le législateur[1388] alors qu'il s'agissait auparavant d'une expérimentation. Ils ont été étendus « *aux adresses complètes de ressources utilisées sur internet* »[1389]. Les pouvoirs de contrôle de la Commission à ce sujet n'ont pas été améliorés[1390]. Au-delà des lacunes juridiques de ce contrôle, c'est donc aussi l'absence de moyens matériels et humains suffisants qui empêchent la bonne réalisation de la conformité.

708. L'informatique a également été appréhendée par d'autres autorités administratives indépendantes, comme l'AMF, qui effectue un contrôle du *trading haute fréquence*[1391], ou encore l'autorité de la concurrence[1392], mais elles peinent à contrôler tous les flux de données dans ces domaines.

709. Le CSA s'est vu doter d'un pouvoir de régulation des réseaux sociaux afin d'assurer une plus grande transparence des traitements algorithmiques en matière de *fake news*[1393], ce qui a déjà abouti à des études sur l'observation du comportement de certains programmes[1394] par exemple. Le président du CSA avait notamment émis le souhait d'une fusion de la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI), pour

---

[1386] Art. 58 LIL et art. 85 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

[1387] COMMISSION NATIONALE DE CONTROLE DES TECHNIQUES DE RENSEIGNEMENT, 5e Rapport d'activité 2020, p. 39, *CNCTR.fr* [en ligne]. Avril 2021. [Consulté le 5 mai 2021]. Disponible à l'adresse : https://www.cnctr.fr/_downloads/0049e0dbcfea1c9ec2b060d2ef2ec1fe/NP_CNCTR_2021_rapport_annuel_2020.pdf

[1388] Art. L. 851-3 et suivants du Code de la sécurité intérieure modifié par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

[1389] *Ibid.*

[1390] A cet égard, « *La Commission nationale de contrôle des techniques de renseignement émet un avis sur la demande d'autorisation relative aux traitements automatisés et les paramètres de détection retenus. Elle dispose d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies. Elle est informée de toute modification apportée aux traitements et paramètres et peut émettre des recommandations* », art. L. 851-3 II du Code de la sécurité intérieure.

[1391] *Supra.*, n° 317 et s.

[1392] *Supra.*, n° 302.

[1393] *Supra.*, n° 341.

[1394] CONSEIL SUPERIEUR DE L'AUDIOVISUEL, Pourquoi et comment le CSA a réalisé une étude sur l'un des algorithmes de recommandations de YouTube, *Actualités du CSA* [en ligne]. 12 novembre 2019 [Consulté le 1er mars 2021]. Disponible à l'adresse : https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Pourquoi-et-comment-le-CSA-a-realise-une-etude-sur-l-un-des-algorithmes-de-recommandations-de-YouTube et CONSEIL SUPERIEUR DE L'AUDIOVISUEL, Observatoire de la haine en ligne : analyser pour mieux lutter, *Actualités du CSA* [en ligne]. 15 octobre 2020 [Consulté le 5 février 2021]. Disponible à l'adresse : https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Observatoire-de-la-haine-en-ligne-analyser-pour-mieux-lutter

étendre les compétences de l'institution dans l'univers numérique[1395]. Ainsi, une proposition de loi visant à fusionner le CSA et la HADOPI a été déposée en vue de créer une nouvelle AAI, à savoir l'Autorité de régulation de la communication audiovisuelle et numérique[1396], dont les futures compétences restent à déterminer.

710. L'Autorité de Régulation des Communications Electroniques, des Postes et de la distribution de la presse (ARCEP)[1397] effectue également dans le cadre de ses compétences des contrôles de conformité des traitements algorithmiques qui ont été récemment étendues au respect de la neutralité du net[1398]. Elle est pressentie pour contrôler les systèmes d'exploitation des terminaux ainsi que des algorithmes des grandes plateformes numériques[1399]. Elle intervient également en tant que tiers de confiance dans l'étude de la 5G avec l'expertise de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui est un service non indépendant, mais est susceptible de concourir à la transparence de certains appareils et logiciels du fait de ses compétences en matière de sécurité informatique. En effet, il existe un régime d'autorisation préalable concernant l'exploitation des équipements de réseaux radioélectriques. Pour des raisons de souveraineté numérique, c'est-à-dire en raison de la préservation des secrets de la défense et de la sécurité nationale, le Premier ministre, après avis de l'ARCEP, autorise « *tous dispositifs matériels ou logiciels, permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile, à l'exception des réseaux de quatrième génération et des générations antérieures, qui, par leurs fonctions, présentent un risque pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau, ou pour la confidentialité des messages transmis et des informations liées aux communications, à l'exclusion des appareils installés chez les utilisateurs finaux ou dédiés exclusivement à un réseau indépendant, des appareils électroniques passifs ou non configurables et des dispositifs matériels informatiques non spécialisés incorporés aux appareils* »[1400]. Ce régime juridique, souvent qualifié d'« *anti-*

[1395] QUERCIA Y., Le CSA pourrait étendre sa régulation aux réseaux sociaux, *Public Sénat.fr* [en ligne]. 30 janvier 2019 [Consulté le 15 janvier 2021]. Disponible à l'adresse : https://www.publicsenat.fr/article/societe/le-csa-pourrait-etendre-sa-regulation-aux-reseaux-sociaux-137387

[1396] Projet de loi n° 523 relatif à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique du 8 avril 2021.

[1397] Création par la loi n° 2005-516 relative à la régulation des activités postales du 20 mai 2005.

[1398] Voir en ce sens art. L. 33-1 du Code des postes et des communications électroniques et ARCEP, Réseaux du futur, Note n° 6, L'intelligence Artificielle dans les réseaux de télécommunications, *Arcep.fr* [en ligne]. 14 janvier 2020. [Consulté le 22 février 2020]. Disponible à l'adresse : https://www.arcep.fr/uploads/tx_gspublication/reseaux-du-futur-IA-dans-les-reseaux-janv2020.pdf

[1399] PRIMAS S., ARTIGALAS V., BABARY S et al., proposition de loi n° 48 2019-2020, visant à garantir le libre choix du consommateur dans le cyberespace, seconde session ordinaire de 2019-2020, Sénat, enregistrée à la Présidence du Sénat le 10 octobre 2019.

[1400] Art. L. 34-11 du Code des postes et des communications électroniques.

huawei », vise à s'assurer que les infrastructures matérielles[1401] et logicielles de 5G ne sont pas incompatibles avec les intérêts protégés. En plus de solliciter des informations très sensibles au moment de la constitution du dossier telles que les caractéristiques techniques de l'appareil et de son logiciel[1402], l'autorisation peut inclure l'obligation pour le demandeur d'informer périodiquement le Secrétaire général de la défense et de la sécurité nationale des modifications logicielles et matérielles de l'infrastructure[1403]. Il est toutefois à noter que cette transparence des opérateurs et des fabricants vis-à-vis de l'administration n'est pas tant garantie pour l'exercice des libertés individuelles puisqu'elle vise surtout à obtenir la conformité de ces dispositifs, à savoir qu'ils sont compatibles avec les techniques d'interception déployées dans le cadre de la loi relative au renseignement[1404].

711. La HAS est également compétente pour autoriser et vérifier la conformité les dispositifs médicaux, dont les outils d'aide à la prise de décision[1405]. Elle établit également à cette fin des procédures de certification de ces logiciels[1406].

712. De nombreuses agences non indépendantes concourent également à la transparence des traitements algorithmiques. Tel est le cas par exemple de l'Agence nationale de traitement automatisé des infractions[1407]. Cet établissement public administratif, sous la tutelle du ministère de l'intérieur, a notamment pour mission d'assurer *« la conception, l'entretien, la maintenance, l'exploitation et le développement des systèmes et applications nécessaires au traitement automatisé des infractions et des avis de paiement des forfaits de post-stationnement* »[1408]. Il effectue donc un travail de vérification des traitements algorithmiques qui peuvent par ailleurs parfois dysfonctionner comme le rappelle un de ses rapports[1409]. Il agit en tant que tiers

[1401] Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques.
[1402] Art. R. 20-29-11 2° et 4° du Code des postes et des communications électroniques.
[1403] Art. R. 20-29-13 I. du Code des postes et des communications électroniques.
[1404] « (…) *Les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre et celles qui sont nécessaires pour répondre, conformément aux orientations fixées par l'autorité nationale de défense des systèmes d'informations, aux menaces et aux atteintes à la sécurité des systèmes d'information des autorités publiques et des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ;* », art. L. 33-1 I e) du Code des postes et des communications électroniques.
[1405] Art. L. 161-38 et art. 161-39 du Code de la sécurité sociale.
[1406] Art. L. 161-38 du Code de la sécurité sociale.
[1407] Décret n° 2011-348 du 29 mars 2011 portant création de l'Agence nationale de traitement automatisé des infractions.
[1408] *Ibid*., art. 2 2°.
[1409] *« Chaque année, plusieurs milliers d'usagers reçoivent un avis de contravention du contrôle automatisé alors qu'ils n'ont pas commis l'infraction routière correspondante. La raison en est que la plaque d'immatriculation du véhicule identifié comme commettant l'infraction sur le cliché du contrôle automatisé (vitesse ou feux rouges) est celle de leur véhicule alors que ce n'était pas leur véhicule qui a été photographié. Plusieurs causes peuvent expliquer cette situation : usurpation de plaque, erreur dans la confection des plaques, dysfonctionnement de la chaîne de traitement, etc. »,* ANTAI, Rapport d'activité, 2018, p. 20.

de confiance non indépendant du pouvoir politique, mais la CNIL peut toutefois recourir à des contrôles puisqu'il s'agit de traitement à données à caractère personnel.

713. Un comité d'éthique spécifique[1410] a d'ailleurs été créé afin d'observer la plateforme nationale *Parcoursup*. Son rôle est d'apporter plus de transparence de ce système vis-à-vis du public, même si les algorithmes locaux ne sont pas concernés par ce contrôle. Comme il s'agit d'une manipulation de données à caractère personnel, la CNIL reste en ce domaine l'autorité maître. Dans le cadre de l'urgence sanitaire, la loi du 11 mai 2020 prorogeant l'état d'urgence avait institué un comité de contrôle et de liaison chargé notamment d'effectuer des audits réguliers des systèmes d'information intervenus à cette fin dans le but « *de vérifier tout au long de ces opérations le respect des garanties entourant le secret médical et la protection des données personnelles* »[1411]. Finalement son rôle n'a de plus été que consultatif.

714. Il en est de même pour la DGCCRF qui vise à empêcher que les règles du droit de la consommation soient violées. Bien qu'elle ne soit pas indépendante, car rattachée au ministère de l'économie[1412], elle s'est vue confier le contrôle des obligations de loyauté, de clarté et de transparence de certains opérateurs de plateforme en ligne qui effectuent par exemple « *du classement ou du référencement, au moyen d'algorithmes informatiques, de contenus, de bien ou de services proposés ou mis en ligne par des tiers* »[1413]. Pour ce faire, elle bénéficie d'un pouvoir d'enquête et de sanction administrative[1414], et collabore avec la CNIL en vue de partager des connaissances techniques[1415]. Bien que son pouvoir d'enquête lui permette de relever des absences de conformité des algorithmes utilisés par les plateformes en matière de

[1410] « *Il s'assure que les règles informatiques qui régissent son fonctionnement sont strictement claires, conformes aux normes en vigueur et transparentes. A ce titre, il est chargé : 1) D'émettre un avis sur toute évolution substantielle des règles de fonctionnement de la plateforme Parcoursup ; 2) D'analyser le fonctionnement de la plateforme et de faire toute proposition au ministre chargé de l'enseignement supérieur afin de l'améliorer ; 3) D'examiner les conditions d'ouverture du code source des traitements automatisés utilisés pour le fonctionnement de la plateforme Parcoursup ; 4) De veiller au respect des principes juridiques et éthiques qui fondent l'examen des candidatures réalisé par les établissements dispensant des formations initiales du premier cycle de l'enseignement supérieur*. », art 1, arrêté du 9 mars 2018 relatif aux missions, à la composition et aux modalités de fonctionnement du comité éthique et scientifique de la plateforme Parcoursup.

[1411] Loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, art. 11 VIII et arrêté du 26 mai 2020 portant nomination des membres du Comité de contrôle et de liaison Covid-19.

[1412] Décret n° 85-1152 du 5 novembre 1985 portant création d'une direction générale de la concurrence, de la consommation et de la répression des fraudes.

[1413] L. 111-7 du Code de la consommation.

[1414] *Supra*., n° 292 et s.

[1415] CNIL, La CNIL et la DGCCRF font évoluer leur protocole de coopération pour renforcer la protection des consommateurs et de leurs données personnelles, *CNIL.fr* [en ligne]. 31 janvier 2019 [Consulté le 3 février 2021]. Disponible à l'adresse : https://www.cnil.fr/fr/la-cnil-et-la-dgccrf-font-evoluer-leur-protocole-de-cooperation-pour-renforcer-la-protection-des

droit de la consommation[1416], elle indique que depuis 2018, sur 44 établissements visités, 32 d'entre elles n'étaient pas en conformité avec la nouvelle réglementation[1417].

715. Un pôle d'expertise de la régulation numérique des plateformes a de plus été créé par un décret en date du 31 août 2020[1418]. Il a « vocation à constituer un centre d'expertise en sciences des données reconnu et mutualisé entre les différents services de l'Etat et ceux de ses démembrements ». Une convention entre ce pôle, l'INRIA et la Direction générale des entreprises a récemment été signée afin de renforcer son expertise. Néanmoins, son effectif n'est pas à la hauteur des enjeux puisqu'il est question d'atteindre une équipe de seulement vingt personnes d'ici la fin 2021[1419].

716. Nous pouvons relever que cette multitude d'organes, dont certains se sont récemment vu confier des missions pour lesquelles ils n'étaient pas initialement taillés, conduit à un éparpillement de moyens matériels et humains et à un manque de visibilité. Certes, cette tendance répond par principe à une volonté de spécialiser la régulation afin qu'elle soit plus cohérente possible dans un domaine d'activité. Mais force est de constater que dans le cas des algorithmes, ce n'est rien d'autre qu'une faiblesse puisqu'il s'agit d'un éclatement de la puissance de l'Etat, mise au service de l'intérêt général[1420], dans le contrôle du numérique. A titre d'exemple, la CNIL, qui a été conçue pour assurer le suivi des traitements algorithmiques en matière de données à caractère personnel, et est encore la mieux dotée des instances de contrôle sur ces questions, dispose sur ses 225 agents, dont le département de la conformité ne représente que 24% de l'effectif[1421]. De plus, sur les 247 contrôles effectués en 2020, uniquement 74 l'ont été sur pièces[1422].

[1416] La DGCCRF a récemment identifié des pratiques trompeuses des sociétés Google Ireland et France, ce qui a abouti à un protocole transactionnel pénal d'un montant de 1,1 million d'euros. Voir en ce sens, DGCCRF, Classement trompeur des hébergements touristiques par Google : une enquête de la DGCCRF conduit au paiement d'une amende transactionnelle de 1,1M€, *Economie.gouv.fr* [en ligne]. 15 février 2021 [Consulté le 18 février 2021]. Disponible à l'adresse : https://www.economie.gouv.fr/dgccrf/classement-trompeur-des-hebergements-touristiques-par-google-une-enquete-de-la-dgccrf-0

[1417] Ces contrôles ont abouti à 21 mesures de police administrative, 8 avertissements et à 4 procès-verbaux d'amende administrative. Voir en ce sens, DGCCRF, Les obligations d'information des plateformes numériques, *Economie.gouv.fr* [en ligne]. 21 avril 2020 [Consulté le 5 février 2021]. Disponible à l'adresse : https://www.economie.gouv.fr/dgccrf/les-obligations-dinformation-des-plateformes-numeriques

[1418] Décret n° 2020-1102 du 31 août 2020 portant création d'un service à compétence nationale dénommé « Pôle d'expertise de la régulation numérique » (PEReN).

[1419] INRIA, Régulation des plates-formes numériques : le gouvernement français prend les devants, *inria.fr* [en ligne]. 6 mai 2021. [Consulté le 10 juillet 2021]. Disponible à l'adresse : https://www.inria.fr/fr/regulation-plateformes-numeriques-peren-regalia

[1420] *Supra*., n° 625 et s.

[1421] CNIL, Rapport d'activité 2020 de la Commission Nationale de l'Informatique et des Libertés, p. 7, *www.cnil.fr* [en ligne]. Juin 2020. [Consulté le 27 août 2021]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_41e_rapport_annuel_-_2020.pdf

[1422] *Ibid.*

PARAGRAPHE 2 - Vers une autorité de contrôle technique unique

717. La longue marche vers la transparence des algorithmes publics est toujours insuffisante à remettre en cause la tradition de l'opacité et du secret de l'administration[1423], et ce malgré de nombreuses améliorations dans ce domaine. De plus, il convient de prendre en considération la menace privée qui a émergé et nuit grandement aux libertés. Cet enjeu est d'autant plus important que la proposition de Règlement européen sur l'IA prévoit de nouvelles obligations de transparence à opérer vis-à-vis d'une autorité de contrôle nationale que les Etats membres devront désigner[1424].

718. Il n'y a certes rien de choquant à ce que des AAI soient créés au gré du hasard, comme a pu le reconnaître le Conseil d'Etat[1425], ne serait-ce parce que ce modèle institutionnel a une utilité et est le plus souvent une réponse à l'émergence d'un fait juridique nouveau. Mais force est de constater qu'il est temps qu'un tiers de confiance unique soit dédié à la question de la transparence de ces algorithmes (A). Cette autorité ne devra pas être que la chose de l'administration c'est-à-dire protéger les gouvernants dans leur action, et devra rendre compte. Car sa mission serait d'étudier aussi bien les algorithmes publics que privés. Elle jouerait par conséquent un rôle significatif en matière d'expertise et de certification des traitements algorithmiques (B).

A - Un tiers de confiance indépendant vis-à-vis des demandeurs

719. Nous assistons à la superposition d'instances de contrôle, dont les statuts ne sont pas similaires, surtout du point de vue des prérogatives et de leur indépendance. Certaines ont été pensées de prime abord pour assurer ce rôle de contrôle des algorithmes manipulant des données à caractère personnel, comme la CNIL, tandis que d'autres doivent effectuer de nouvelles missions du fait de l'immixtion des algorithmes dans leur domaine, sans toutefois bénéficier de moyens particuliers adoptés par le législateur. Ce mille-feuille nuit à la cohérence de l'action

[1423] « *Les liens entre les trois lois votées en 1978 et 1979 sont, en effet, étroits. Ils ne se tiennent pas seulement à la concomitance de ces textes. Ils ne se limitent pas non plus aux renvois d'un texte à l'autre inscrit dans plusieurs de leurs articles. Ils résultent surtout d'une communauté d'inspiration : ces trois lois ont pour objet d'améliorer et de rénover les rapports de l'administration et des citoyens en donnant à ceux-ci des droits nouveaux d'accès l'information ; elles visent à assurer plus d'ouverture et de transparence aux services publics* », LASSERRE B., LENOIR N., STIRN B., *La transparence administrative*, *op. cit.*, p. 1 à 2.

[1424] Selon l'article 30 § 1 la proposition de Règlement 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 du 21 avril 2021, « *Chaque État membre désigne ou établit une autorité notifiante chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle* ».

[1425] CONSEIL D'ETAT, *Rapport public, Les autorités administratives indépendantes*, 2001, spec. p. 261.

du contrôle des traitements, et l'absence de clarification n'est pas sans poser des difficultés aux personnes physiques et morales qui souhaiteraient recourir à ces instances.

720. Il convient de reconnaître que l'élargissement de certaines missions, comme c'est actuellement le cas pour le CSA, dénature sa mission première et concurrence les missions qui auraient dû revenir pour plus d'efficacité à une seule autorité, en l'occurrence à la CNIL, surtout lorsque l'on s'attache à la genèse de cette commission qui se voulait à compétence générale sur les problématiques relatives au numérique[1426]. En d'autres termes, il existe une perte de cohérence dans le contrôle de l'action administrative ainsi que des opérateurs économiques, et un effort de rationalisation doit être entrepris pour concourir plus aisément à l'effort de transparence des traitements.

721. Cet effort de rationalisation dans le cadre de la régulation numérique des opérateurs de plateforme est déjà soulevé par certains députés[1427]. Selon eux, il serait préférable de promouvoir une culture de la transparence des plateformes numériques, et donc de leurs algorithmes, y compris en défendant « *au niveau européen la mise en place d'une régulation ex ante exercée par un régulateur indépendant* »[1428], et ce dans l'attente d'une régulation internationale[1429]. Toutefois, ils insistent sur le fait qu'une autorité nationale devrait également remplir ces missions, soit en étendant les pouvoirs d'une autorité existante[1430], voire en créant une nouvelle qui jouerait le rôle d'autorité pilote spécialisée sur ces enjeux[1431]. En reprenant les conclusions du rapport du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies[1432], lesdits sénateurs sont favorables à la création « *d'un bureau spécialisé des technologies de contrôle de l'économie numérique* » rattaché à la DGCCRF[1433]. Bureau qui pourrait ensuite être saisi par les AAI souhaitant bénéficier de leur expertise, mais son caractère indépendant n'a toutefois pas été précisé.

[1426] *Supra.,* n° 696 et s.

[1427] FAURE-MUNTIAN V., FASQUELLE D., Rapport d'information n° 3127 sur les plateformes numériques de l'Assemblée nationale, 15e législature, fait au nom de la commission des affaires économiques, 15 e législature, enregistré à la Présidence de l'Assemblée nationale le 24 juin 2020, spec. p. 72 à 74, *Assemblée-nationale.fr* [en ligne]. 14 octobre 2020. [Consulté le 25 novembre 2020] : https://www.assemblee-nationale.fr/dyn/15/rapports/cion-eco/l15b3127_rapport-information

[1428] *Ibid*., proposition n° 20, p. 99.

[1429] *Ibid*., p. 100.

[1430] A la suite des auditions effectuées dans le cadre de cette mission d'information parlementaire, l'ARCEP « *a souligné qu'elle pourrait prendre en charge ce rôle, du fait de son expérience significative en matière de droit de la régulation des télécommunications. L'ARCEP étant déjà chargée de faire respecter la neutralité du réseau internet, l'extension de son contrôle aux terminaux paraît légitime et permettrait de capitaliser sur l'expérience préexistante de l'institution.* », p. 93.

[1431] *Ibid*., p. 92.

[1432] Cette proposition reprend la création de l'*Office of technology research and investigation* rattachée à la *Federal trade commission* en 2015 aux Etats-Unis d'Amérique « *pour promouvoir des travaux de tests d'algorithmes.* ». Voir en ce sens, Conseil général de l'économie, de l'industrie, de l'énergie et des technologies, Rapport *sur les modalités de régulation des algorithmes de traitement des contenus* du 13 mai 2016, p. 5.

[1433] LONGUET G., Rapport n° 7 sur le devoir de souveraineté numérique du Sénat, session ordinaire 2019-2020, fait au nom de la commission d'enquête, enregistré à la Présidence du Sénat le 1er octobre 2019, p. 51.

722. Dans son rapport « *Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle* », la CNIL relatait également les doléances des citoyens parmi lesquelles la création d'« *un organisme indépendant pour effectuer des tests scientifiques sur les algorithmes à l'image des médicaments avant la mise en vente sur le marché* » était souhaitable[1434].

723. Nous voudrions aller plus loin et englober l'intégralité de la problématique relative à la transparence des traitements algorithmiques. Pour ce faire, nous ne pensons pas qu'il faille dans un premier temps déstructurer les AAI exerçant déjà un rôle de régulateur des traitements algorithmiques, et donc de leur transparence. Mais cette instance de contrôle devra avoir le monopole en matière d'enquête et d'étude des traitements algorithmiques, ce qui implique de fait une centralisation des moyens matériels et humains nécessaires à l'accomplissement de cette mission.

724. Cette autorité pourrait suppléer les autres AAI n'ayant pas les moyens d'effectuer correctement leur rôle de régulateur, et dont le domaine de compétence n'est pas initialement celui du numérique, car rappelons que les algorithmes font leur immixtion dans tous les secteurs. Il convient désormais d'agréger la plus grande force possible pour contrôler les traitements algorithmiques, dont la complexité plaide en faveur d'une étude centralisée de ces derniers. Pour effectuer cette mission, le statut juridique des AAI est adéquat, car ces expertises doivent être effectuées de manière indépendante du pouvoir politique, ne serait-ce parce qu'il s'agit d'un travail purement technique, y compris sur les algorithmes participant à l'action administrative. En revanche, il n'est pas opportun qu'elles centralisent les pouvoirs relevant normalement d'autres organes telles que des compétences juridictionnelles ou règlementaires. Il est d'ailleurs primordial que ce travail soit effectué par des spécialistes, dont des équipes seraient pluridisciplinaires, c'est-à-dire représentatives des sciences informatiques et des sciences économiques et sociales.

725. La mission principale de cette instance serait de tenir un rôle de tiers de confiance lorsque la transparence ne peut être opérée de manière directe par les utilisateurs, qu'ils soient des personnes physiques ou morales. Il est d'ailleurs à noter qu'à l'exception de certains régimes juridiques comme celui des décisions administratives fondées sur des traitements

[1434] CNIL, Comment permettre à l'Homme de garder la main ?, p. 54, *Cnil.fr* [en ligne]. Décembre 2017. [Consulté le 25 août 2020]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

algorithmiques[1435], les entreprises ne peuvent pas bénéficier des dispositions de la LIL en matière de transparence, puisqu'elles ne sont pas des personnes physiques[1436]. Mais nous comprenons dans le même temps que des opérateurs économiques souhaiteraient sous couvert de transparence des algorithmes accéder à des secrets industriels et commerciaux. Comme nous l'avons rappelé, et comme l'a affirmé le Conseil d'Etat dans son étude annuelle de 2014[1437], les algorithmes sont souvent protégés par le secret industriel et commercial. Toutefois, il n'est pas concevable d'imaginer que la communication des principales caractéristiques ou des éléments de référencement aux intéressés par les responsables de traitement permette d'assurer haut niveau de transparence. Et faudrait-il encore que les informations communiquées soient véridiques, c'est-à-dire conformes. Ce travail de conformité ne peut pas dans la majorité des cas être opéré par l'utilisateur lui-même, le plus souvent par manque de compétences ou d'informations suffisantes. Cette opération se complexifie nécessairement lorsque le résultat ne peut pas être vérifiable du fait de l'opacité de l'architecture technique, comme c'est le cas avec les algorithmes auto-apprenants, ou bien parce que la transparence juridique a par exemple lieu sur algorithmes, et non sur la documentation explicative de l'algorithme, ou plus encore sur les données qui seraient protégées par le droit des tiers et sur lesquelles ce dernier repose. Dès lors, force est de constater que cette transparence ne pouvant s'effectuer techniquement ou d'un point de vue juridique, c'est sur un tiers de confiance indépendant que doit reposer cette tâche, notamment pour contrôler que les éléments communiqués par le responsable du traitement aux intéressés sont véridiques, mettant fin à toute asymétrie informationnelle. C'est notamment grâce au principe de transparence des traitements algorithmiques, constitutionnellement protégé[1438], que la transparence juridique peut s'opérer par cette instance.

726. Par ailleurs, il existe certes des services de l'Etat exerçant un contrôle sur certains algorithmes publics ou privés. Mais ne disposant pas des garanties suffisantes d'indépendance, notamment du fait d'une emprise hiérarchique de l'administration[1439], ces services devront également faire l'objet de vérifications de leurs travaux tels que les audits par notre autorité de contrôle. Des comités spécialisés au sein de l'institution pourraient être habilités à accéder aux secrets comme la défense nationale, notamment pour effectuer une surveillance des opérations

[1435] *Supra.*, n° 435 et s.
[1436] *Supra.*, n° 80 et s.
[1437] CONSEIL D'ETAT, *Le numérique et les droits fondamentaux*, *op. cit.*, p. 279.
[1438] *Supra.*, n° 664 et s.
[1439] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique, art. 4.

de renseignement[1440]. L'absence d'emprise hiérarchique est une des conditions nécessaires à l'instauration d'un véritable tiers de confiance légitime.

727. Certains pourraient arguer à juste titre que la centralisation de telles compétences engendrerait à terme une « cannibalisation » des autres AAI, car le numérique pénètre tous les secteurs. Or, l'instance que nous évoquons n'aurait qu'un rôle d'expertise, de contrôle, et non de sanction, le but étant de dissocier le pouvoir réglementaire et de sanction, quand bien même ces sections seraient institutionnellement réputées étanches. Les sanctions administratives resteraient du ressort des AAI ou des agences de rattachement. Et concernant les secteurs ne faisant pas l'objet d'une instance de contrôle, la commission pourrait tout de même recevoir des plaintes, enquêter, et ainsi transmettre le cas échéant les dossiers à un tribunal compétent. Le Conseil d'Etat s'était également prononcé en faveur du maintien d'instances sectorielles pour apprécier les particularités de chaque réglementation[1441].

728. Cette autorité pourrait cibler les secteurs qui sont dans l'angle mort des agences déjà en place. C'est l'avantage d'une instance généraliste, comme avait été pensée la CNIL dans le rapport Tricot[1442], car cela permet une réactivité plus importante.

B - Un rôle d'expertise et d'agrément en matière de certification

729. Ce tiers de confiance institutionnel bénéficierait de plusieurs missions. Son rôle serait de référencer les traitements algorithmiques aussi bien publics que privés, bien que pour ces derniers un seuil d'évaluation de la puissance de la plateforme doive être défini par le législateur afin de les étudier puisque, comme nous l'avons évoqué, la tenue d'un tel registre contribue à la transparence[1443]. Il est nécessaire qu'une telle instance classifie les traitements pouvant faire l'objet d'une transparence directe, à savoir pouvant faire l'objet de la diffusion du code source au public ainsi que de la documentation afférente pour la compréhension de ce dernier s'il s'agit de traitements algorithmiques publics non couverts par les secrets protégés par la loi. Elle

[1440] En effet, comme nous l'avons vu, la CNCTR ne remplit pas correctement cette mission. PAUL C., FERAL-SCHUHL C., Rapport n° 3119 Numérique et libertés : un nouvel âge démocratique de l'Assemblée nationale, 14e législature, fait au nom de la commission de réflexion et de propositions sur le droit et les libertés l'âge du numérique, enregistré à la Présidence de l'Assemblée nationale le 9 octobre 2015, p. 164 : *« Son contrôle devrait s'exercer sur l'ensemble des services de renseignement et l'intégralité des mesures et techniques qu'ils emploient, en amont de leur mise en œuvre sous la forme d'un avis préalable, durant leur application et en aval, sous la forme de contrôles sur pièces et sur place. Outre un pouvoir de recommandation, cette autorité devrait pouvoir transmettre au juge les cas dans lesquels elle estime que le pouvoir exécutif a méconnu les garanties accordées par la loi au citoyen.* », *Assemblée-nationale.fr* [en ligne]. [Consulté le 25 février 2021]. Disponible à l'adresse : https://www.assemblee-nationale.fr/14/pdf/rapports/r3119.pdf

[1441] CONSEIL D'ETAT, *Le numérique et les droits fondamentaux*, *op. cit.*, p. 281.

[1442] *Supra.*, n° 699 et s.

[1443] *Supra.*, n° 232 et s.

préviendrait en amont de la diffusion l'institution ou la personne concernée de cette publication. En cas de désaccord, le litige serait tranché par la justice et nous passerons à une transparence indirecte. Toutefois, dans les hypothèses où il existerait un secret protégé par la loi ou plus largement la remise en cause potentielle du droit des tiers, la commission pourrait tout de même accéder aux informations nécessaires afin de s'assurer de la conformité des déclarations de l'administration dans notre exemple, ce que la CADA n'a pas la compétence de faire[1444]. Si la transparence directe ne peut être assurée pour les raisons évoquées, nous basculerons sur une transparence de nature indirecte pour les demandeurs, c'est-à-dire assurée par l'autorité et dont l'explicabilité consisterait à communiquer des informations sur la logique générale de l'algorithme.

730. Elle bénéficierait toutefois de toutes les informations nécessaires au bon déroulement de sa mission. Il s'agit de la condition *sine qua non* pour mettre fin à toute asymétrie informationnelle. En effet, il serait tentant pour une administration ou une personne privée de déclarer la conformité d'un traitement aux exigences normatives, sans qu'il ne soit possible pour une autorité de le contrôler, ce qui rappelons-le, s'applique déjà aux données à caractère personnel.

731. Les droits des tiers seraient naturellement garantis dans la mesure où les agents effectuant ces opérations seraient habilités et tenus à des exigences de confidentialité comme c'est par exemple actuellement le cas pour des membres de la CNIL[1445], et au secret concernant la CNCTR[1446].

732. Naturellement, il convient de considérer que cette instance ne pourra pas contrôler tous les traitements algorithmiques, tant ils sont nombreux et parce que l'intérêt y est souvent insignifiant, bien qu'elle puisse également conseiller les organismes privés ou publics qui solliciteraient son aide. En revanche, cela n'empêche pas de cibler ses efforts sur les systèmes d'information les plus susceptibles d'exercer une incidence sur les personnes ainsi que sur la société. Nous étudierons toutefois plus loin sur quels types de traitements il conviendra de porter les efforts[1447].

[1444] *Supra*., n° 425.
[1445] Art. 19 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1446] Art. L. 832-5 du Code de la sécurité intérieure.
[1447] *Infra*., n° 900 et s.

733. Certains traitements pourraient avant leur déploiement nécessiter un audit permettant de s'assurer qu'ils sont conformes à la réglementation ou ne comportent pas par exemple des discriminations[1448]. Il serait à cet égard préférable que la chambre législative dédiée à la matière numérique décide quels seraient les systèmes d'information concernés par cette exigence[1449]. Dans cette hypothèse il s'agirait d'un contrôle *a priori* des algorithmes.

734. Plus classiquement, les efforts doivent être portés sur la surveillance des traitements algorithmiques déjà déployés. Pour ce faire, dans son rapport annuel de 2014 relatif au numérique et aux droits fondamentaux, le Conseil d'Etat préconisait la création d'une nouvelle profession « *d'algorithmiste* », agrée par l'Etat, pour effectuer un contrôle sur les algorithmes prédictifs[1450]. Il semble toutefois discutable de considérer qu'un commissaire pourrait à lui seul auditer des algorithmes complexes, c'est-à-dire vérifier la conformité d'un traitement algorithmique, surtout en matière d'IA. En effet, l'effort de compréhension de ces algorithmes concernant certains traitements nécessite des équipes de plusieurs membres sur un temps non négligeable. A titre d'exemple, l'affaire du *dieselgate* a mis au jour un programme informatique modifié implanté dans un véhicule automobile afin de faire paraître une conformité aux réglementations européennes et américaines lors des essais d'homologation. Le logiciel était capable de déceler lorsque le véhicule se retrouvait en phase d'évaluation de ses émanations Nox[1451], afin qu'il les réduise par rapport à un usage classique. Il a fallu un an à une équipe de chercheurs pour reconstituer le code source par rétroingénierie[1452]. Fort heureusement, des expertises judiciaires ont également permis de constater l'existence d'un tel logiciel frauduleux par l'étude comportementale du véhicule dans des situations différentes sans que cela ne nécessite l'analyse précise du code informatique, ce qui est suffisant pour démontrer la tromperie[1453]. Mais il existe des hypothèses dans lesquelles la rétroingénierie[1454] trouve ses

[1448] CHAPENET J., LEQUESNE ROTH C., « Discrimination et biais genrés : les lacunes juridiques de l'audit algorithmique », *op. cit.*, p. 1852.
[1449] *Infra*., n° 745 et s.
[1450] CONSEIL D'ETAT, *Le numérique et les droits fondamentaux*, *op. cit*., p. 239.
[1451] MANDARD, S., Cinq ans après le « Dieselgate », les constructeurs bénéficient toujours d'une « clause de confidentialité », *op. cit.*
[1452] CONTAG, M. *et al*., « How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles », in *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2017, p. 231 à 250, doi: 10.1109/SP.2017.66 ; UC SAN DIEGO, Researchers find Computer Code that Volkswagen Used to Cheat Emissions Tests, in *Jacobsschool.ucsd.edu* [en ligne]. [Consulté le 16 janvier 2021]. Disponible à l'adresse : https://jacobsschool.ucsd.edu/news/release?id=2213
[1453] INFOCURIA JURISPRUDENCE, Renvoi préjudiciel – Rapprochement des législations – Règlement (CE) n° 715/2007 – Véhicules à moteur – Émissions de polluants – Dispositif d'invalidation – Programme agissant sur le calculateur de contrôle moteur – Technologies et stratégies permettant de limiter la production des émissions de polluants – Moteur diesel, *Curia.europa.eu* [en ligne]. 30 avril 2020. [Consulté le 22 février 2021]. Disponible à l'adresse : http://curia.europa.eu/juris/document/document.jsf?text=&docid=226006&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=1563682
[1454] Interview de Daniel Le Métayer : GUILLAUD H., Algorithmes et responsabilités, *Internetactu.net* [en ligne]. 16 mars 2016. [Consulté le 2 avril 2021]. Disponible à l'adresse : https://www.internetactu.net/2016/03/16/algorithmes-et-responsabilites/

limites et dont la constatation par comparaison pour déduire l'existence d'un logiciel truqué nécessite bien plus que quelques experts judiciaires, tant le niveau de technicité est élevé. C'est notamment pour cette raison que des équipes de chercheurs doivent être dédiées au sein de cette institution à l'étude sur le long terme des traitements algorithmiques.

735. Nous rejoignons davantage l'idée selon laquelle il conviendrait d'instaurer des commissaires aux algorithmes concernant les traitements algorithmiques au sens large et non seulement en matière d'IA ou d'algorithmes prédictifs[1455], et ce dans le but de les auditer. Ils seraient rattachés à notre institution. La commission supérieure du numérique et des postes préconisait que, concernant les algorithmes auto-apprenants, dès qu'ils ont une incidence sur les individus,

> « *la fourniture d'un accès aux algorithmes et* dataset *de tests permettant de vérifier la reproductibilité des traitements algorithmiques, l'absence de dérives et de biais dans le temps et leur contrôle, par des autorités indépendantes nationales ou européennes associant des représentants de la société civile. Ces nouvelles missions pourraient être exercées par des autorités indépendantes existantes, notamment celles en charge de la protection des données personnelles, à condition qu'elles soient dotées des moyens matériels, financiers et humains leur permettent d'exercer un contrôle effectif* »[1456].

736. Un rapport du Sénat traitant des enjeux de souveraineté numérique, mais spécifiquement sur la question des plateformes numériques privées, abonde dans le sens d'une « auditabilité » des algorithmes plutôt qu'en faveur d'une publication de ces derniers[1457]. Les sénateurs constatent que les autorités publiques ne disposent pas des moyens techniques et humains nécessaires à l'accomplissement de cette tâche, c'est-à-dire à la possibilité dans le cadre de leurs fonctions d'accéder « *aux principes et méthodes de constitution des algorithmes ainsi qu'aux données sur lesquels ils se basent pour éviter l'asymétrie d'information entre les régulateurs et les régulés* »[1458]. Le rapport Villani de 2017 *« Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne* »[1459] évoquait également des pistes de réflexion relatives

[1455] COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES, avis n° 2020-08 du 12 juin 2020, p. 5.
[1456] *Ibid.*
[1457] LONGUET G., Rapport n° 7, *op. cit.*, p. 50.
[1458] *Ibid.*, p. 51.
[1459] VILLIANI C., SCHOENAUER M., BONNET Y., et al., Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne, mission confiée par le Premier ministre Edouard Philippe, *Vie-publique.fr* [en ligne]. 28 mars 2018 [Consulté le 16 juin 2020]. Disponible à l'adresse : https://www.vie-publique.fr/rapport/37225-donner-un-sens-lintelligence-artificielle-pour-une-strategie-nation

à l'opacité de certains systèmes, raison pour laquelle elles sont appelées « boîtes noires », car au regard de l'état de l'art en informatique il n'est pas possible de recourir à la traçabilité de l'ensemble des processus de ce dernier : « *au-delà de la transparence, il est nécessaire d'accroître l'auditabilité des systèmes d'IA. Cela pourrait passer par la constitution d'un corps d'experts publics assermentés, en mesure de procéder à des audits d'algorithmes, des bases de données et de procéder à des tests par tout moyen requis. Ces experts pourraient être saisis à l'occasion d'un contentieux judiciaire, dans le cadre d'une enquête diligentée par une autorité administrative indépendante ou suite à une demande du Défenseur des droits.* »[1460] . Cette mission prendrait part dans un écosystème de recherche en matière d'explicabilité grâce à des investissements conséquents[1461]. Cette hypothèse avait également été avancée par la CNIL dans l'un de ses rapports puisqu'elle proposait la création d'une « *plateforme nationale d'audit des algorithmes* »[1462] composée d'un corps d'experts publics, ou bien par délégation d'experts privés homologués[1463].

737. Toutefois, force est de constater que malgré des normes protectrices en matière de transparence, de nombreux traitements algorithmiques sont effectués par des opérateurs économiques étrangers qui ne souhaitent pas se soumettre à des audits. Cette instance aurait donc pour mission de contrôler par l'observation certains comportements de l'algorithme. A titre d'exemple, sans avoir accès aux algorithmes et aux données d'apprentissage de Google concernant sa plateforme Youtube, le CSA a pu mener une étude empirique sur les recommandations de contenus, ce qui a permis de prendre connaissance de quelques caractéristiques de l'algorithme[1464]. Aurélie Jean s'est par ailleurs prononcée en faveur d'une « police des algorithmes » automatisés[1465] afin de déceler les biais algorithmiques. Cette automatisation de la surveillance peut être intéressante pour effectivement observer le comportement des algorithmes auto-apprenants ou non, mais il nous semble évident que cela

[1460] VILLIANI C., Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne, p. 21, in *Vie-publique.fr* [en ligne]. Mars 2018 [Consulté le 16 avril 2020]. Disponible à l'adresse : https://www.vie-publique.fr/sites/default/files/rapport/pdf/184000159.pdf. Cette possibilité d'effectuer des tests et d'obtenir des statistiques de la part des plateformes pour comprendre les algorithmes sans en exiger le code source et les données d'apprentissage est également repris par le rapport de la mission « *Régulation des réseaux sociaux – Expérimentation Facebook* » remis au secrétaire d'Etat en charge du numérique en mai 2019, p. 25 à 26. Certains spécialistes évoquent également la possibilité d'associer cette méthodologie à des testings : BINAIRE, Le testing algorithmique de la discrimination à l'embauche (2), *Le Monde.fr* [en ligne]. 10 janvier 2020 [Consulté le 12 juin 2021]. Disponible à l'adresse : https://www.lemonde.fr/blog/binaire/2020/01/10/le-testing-algorithmique-de-la-discrimination-a-lembauche-2/

[1461] *Ibid*., p. 140.

[1462] CNIL, *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, comment permettre à l'homme de garder la main : les enjeux éthiques des algorithmes et de l'intelligence artificielle*, 2017, Recommandation 4, p. 57.

[1463] *Ibid.*, p. 58.

[1464] CSA, *Etude, capacité à informer des algorithmes de recommandation : une expérience sur le service YOUTUBE*, novembre 2019, p. 58.

[1465] JEAN A., *De l'autre côté de la machine : Voyage d'une scientifique au pays des algorithmes, op. cit.*, p. 140 à 141.

ne peut être qu'un outil à la disposition de notre autorité et non se substituer à un contrôle humain, qui plus est car des algorithmes pourraient contourner en théorie ces systèmes de surveillance.

738. De manière plus contraignante, cette autorité référente en matière de surveillance des algorithmes bénéficierait d'un pouvoir d'investigation. Il s'exercerait dans certaines conditions par l'intermédiaire d'une autorisation préalable de l'institution judiciaire dédiée que nous aborderons ensuite[1466], afin que la justice ordonne l'accès à des locaux avec les garanties adéquates au respect d'un Etat de droit protégeant les droits et libertés fondamentales comme le ferait la CNIL en matière de données à caractère personnel, à l'exception qu'il serait élargi possiblement aux systèmes d'information de tous les secteurs.

739. Au-delà de l'auditabilité, elle pourrait également, comme le fait la CNIL[1467], élaborer des référentiels en matière de certification des algorithmes, tout en délivrant des agréments à des entreprises pouvant remplir cette mission, ce qui ne l'empêchera pas le cas échéant de contrôler que ce travail a correctement été effectué.

740. Pour conclure, il est tout aussi important qu'elle intervienne en tant qu'expert judiciaire sur demande d'intervention des juridictions. En effet, les expertises judiciaires sont très couteuses pour les parties, en plus d'être techniquement complexes à opérer, notamment pour des raisons d'exigences juridiques de confidentialité[1468]. Dans l'hypothèse où il existe un doute sérieux qu'un traitement algorithmique a pu porter préjudice, ou bien a une incidence manifeste sur des libertés fondamentales au sens large, cette instance serait appelée à intervenir, bien qu'il soit naturellement possible d'effectuer des contre expertises judiciaires. Ce système permettrait à des justiciables sans connaissances informatiques particulières, voire qui ne soupçonneraient pas une telle intervention algorithmique dans le contentieux, d'obtenir des garanties. L'avantage de cette instance est qu'elle bénéficie en la matière d'une expérience importante ainsi que des études déjà effectuées sur les programmes en cause. Il est primordial de considérer que le contentieux a également pour mission de concourir à la transparence de ces logiciels, ce qui est actuellement assez peu le cas car nous ignorons bien souvent leurs incidences. L'enjeu probatoire est problématique en matière d'informatique et explique également pourquoi le contentieux est si peu quantitatif.

[1466] *Infra*., n° 765 et s.
[1467] *Supra*., n° 202 et s.
[1468] MIGAYRON S., « *Contradictoire et confidentialité dans les expertises des litiges du monde numérique : une mission impossible* », *op. cit.*

741. Après avoir évoqué en quoi il était nécessaire de se doter d'une autorité indépendante exclusivement technique en matière de transparence des algorithmes, il convient de considérer que la nature, et le degré de transparence de ces derniers, est également une question institutionnelle et démocratique.

SECTION 2 - Une nouvelle organisation des pouvoirs constitués œuvrant pour une plus grande transparence

742. Nous plaidons pour une autorité de contrôle des traitements algorithmiques dont la mission ne sera pas de bénéficier à la fois d'un pouvoir réglementaire et de sanction. En effet, le schéma traditionnel des AAI de régulation tend à concentrer de nombreuses prérogatives, et constitue une rupture dans la manière d'appréhender la séparation des pouvoirs telles que conçues initialement au sein des démocraties libérales[1469], ce qui n'est pas sans incidence sur l'effectivité de la transparence.

743. Il y a des époques qui nécessitent davantage d'adaptation du point de vue institutionnel, et celle que nous vivons, en fait partie. A défaut, les institutions ne peuvent plus remplir leur rôle démocratique, notamment parce qu'il convient d'appréhender un monde virtuel émulé à partir d'un monde physique, mais dont les incidences sur les libertés et la conciliation des droits n'est pas nécessairement la même entre ces deux sphères.

744. Concernant la nature et le degré de transparence que nécessite l'application du principe de transparence constitutionnellement protégé, il convient d'évoquer une réforme institutionnelle aussi bien législative (Paragraphe 1) que judiciaire (Paragraphe 2). Ces contre-pouvoirs seraient par ailleurs conseillés techniquement par notre commission.

PARAGRAPHE 1 - Une chambre législative relative aux enjeux numériques

745. La transparence des traitements algorithmiques n'est pas qu'une problématique technique. Il s'agit notamment d'un sujet éminemment démocratique portant aussi bien sur la nature ou le degré de transparence à mettre en œuvre par secteur, voire le cas échéant,

[1469] PERROUD T., *La fonction contentieuse des autorités de régulation en France et au Royaume-Uni*, Nouvelles bibliothèques de thèses, *Dalloz*, 2013.

l'interdiction de certaines techniques lorsqu'un domaine exige une transparence absolue (A), ce qui ne peut être débattue que par le Parlement. Pour ce faire, nous proposons une spécialisation du Parlement dans ce domaine (B).

A - Un contrôle démocratique insuffisant sur la mise en œuvre des traitements algorithmiques

746. Les critiques relatives à la multiplication des AAI ou de leurs compétences ne sont pas nouvelles[1470]. Elles soulèvent par ailleurs bien des interrogations qui ne sont pas propres au numérique. Le Président du Sénat, Gérard Larcher, y voit par ailleurs un affaiblissement du pouvoir législatif, voire un Etat dans l'Etat[1471]. Des auteurs, comme Thomas Perroud, considèrent que les AAI participent à l'instauration d'une légalité néolibérale[1472]. Ces institutions posent naturellement la question de l'exercice du pouvoir politique, mais force est de constater que l'indépendance vis-à-vis de ce pouvoir est une qualité essentielle, notamment pour exercer un rôle de contrôle purement technique, ce qui nous intéresse particulièrement dans le cadre des traitements algorithmiques et a abouti à notre proposition de commission de contrôle. Mais nous n'avons pas fait le choix de proposer une AAI générale qui disposerait à la fois du pouvoir d'édicter des règlements et de les sanctionner tout en assurant la fonction de contrôle des algorithmes. De plus, l'argument initial plaidant en faveur des AAI telles que la rapidité et l'efficacité, en tant que mode de régulation, est de plus en plus discutable[1473] puisqu'elles sont elles-mêmes soumises à des contraintes procédurales de plus en plus strictes, ce que nous encourageons, ainsi qu'à des moyens inadaptés.

747. La problématique démocratique relative aux enjeux du numérique a sans doute été éludée car le Parlement se suffisait à lui-même, et avait démontré qu'il pouvait faire œuvre libérale en votant de nombreuses lois participant à la transparence de l'action administrative dans les années soixante-dix[1474]. Et surtout, l'informatique était appréhendée comme une discipline purement technique, et donc d'experts.

[1470] MEZARD J., Rapport n° 126 sur le bilan et le contrôle de la création, de l'organisation, de l'activité et de la gestion des autorités administratives indépendantes du Sénat, session ordinaire de 2015-2016, fait au nom de la commission d'enquête, enregistrée à la Présidence du Sénat le 28 octobre 2015.

[1471] « *Il faudra aussi nous poser la question de la multiplication des autorités indépendantes, qualifiées de tel parce que non issues de l'élection*. », JACQUOT G., Autorités administratives indépendantes : le Sénat s'interroge à nouveau sur leur « multiplication », *Public Sénat.fr* [en ligne]. 23 janvier 2019 [Consulté le 26 novembre 2020]. Disponible à l'adresse : https://www.publicsenat.fr/article/parlementaire/autorites-administratives-independantes-le-senat-s-interroge-a-nouveau-sur

[1472] PERROUD T., « Essai sur les caractères néolibéraux du droit administratif contemporain », *in Mélanges en l'honneur de Serge Regourd*, 2018.

[1473] MANANCOURT V., Have a GDPR complaint ? Skip the regulator and take it to court, *op. cit.*

[1474] *Supra.*, n° 75 et s.

748. Comme nous l'avons vu, il était initialement question de confier à la CNIL le rôle de contre-pouvoir technique en matière d'informatique[1475]. Raison pour laquelle, indépendamment des avis à portée consultative, il existait une procédure d'avis conforme de la commission prévue par la loi pour la création de traitements d'intérêt public de données personnelles dits sensibles[1476] ou pour les actes réglementaires autorisant les personnes morales gérant un service public de « *procéder au traitement automatisé des informations nominatives concernant les infractions, condamnations ou mesures de sûreté* »[1477].

749. Cet avis a par ailleurs été retiré en 2004[1478], et de nombreux traitements n'ont été subordonnés qu'à un avis simple de la CNIL, notamment parce qu'un rapport évoquait dès 2002 qu'un avis simple n'affaiblirait pas « *pour autant, les pouvoirs de cette autorité, car la publicité donnée à cet avis sera telle qu'il sera difficile pour l'administration de s'en affranchir* »[1479]. Mais le droit souple n'est pas le droit dur, et la CNIL n'est plus un contre-pouvoir efficace face au pouvoir politique dans l'instauration de tels traitements[1480]. De plus, le pouvoir de sanction administrative de la CNIL n'intervient qu'a posteriori de la mise en œuvre du traitement, ce qui n'empêche pas son déploiement.

750. L'affaiblissement de la CNIL en tant que contre-pouvoir technique, corrélée à une dérive présidentialiste de la Ve République, ne constituait plus un frein suffisant à l'instauration de traitements algorithmiques liberticides publics. Cette prise de conscience s'est par ailleurs manifestée lors de la crise sanitaire de la Covid-19 lorsque des parlementaires ont prorogé l'état

---

[1475] *Supra.*, n° 699.

[1476] « *Il est interdit de mettre ou conserver en mémoire informatisée, sauf accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes. Toutefois, les églises et les groupements à caractère religieux, philosophique, politique ou syndical peuvent tenir registre de leurs membres ou de leurs correspondants sous forme automatisée. Aucun contrôle ne peut être exercé, de ce chef, à leur encontre.*
Pour des motifs d'intérêt public, il peut aussi être fait exception à l'interdiction ci-dessus sur proposition ou avis conforme de la commission par décret en Conseil d'Etat »., Art. 31 ancien de la LIL.

[1477] Art. 30 al. 1er ancien de la LIL.

[1478] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1).

[1479] GOUZES G., Rapport n° 3526 sur le projet de loi n° 3250 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés de l'Assemblée nationale, 11e législature, fait au nom de la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République, enregistré à la Présidence de l'Assemblée nationale le 9 janvier 2002, p. 26 à 27.

[1480] Bien que la CNIL n'aie jamais utilisée ce droit de blocage, un rapport a évoqué l'éventualité qu'« *On peut aussi supposer qu'il y avait négociation préalable pour que le fichier soit conçu de telle façon qu'il n'y ait pas de problèmes justifiant le veto de la CNIL*. », ce qui tranche évidemment avec le fait que la CNIL apprenne de nos jours l'existence de nouveaux projets de systèmes d'information tardivement, voire par la voie de presse, mettant fin à une sorte de collaboration entre pouvoirs. Voir en ce sens, DETRAIGNE Y., ESCOFFIER A-M., Rapport d'information n° 441 relatif au respect de la vie privée à l'heure des mémoires numériques du Sénat, session ordinaire 2008-2009, fait au nom des lois constitutionnelles, de législation, du suffrage universel, Règlement et d'administration générale, enregistré à la Présidence du Sénat le 27 mai 2009, p. 25, *Sénat.fr* [en ligne]. 27 mai 2009. [Consulté le 3 avril 2020]. Disponible à l'adresse : https://www.senat.fr/rap/r08-441/r08-4411.pdf

d'urgence sanitaire une première fois[1481]. Le législateur a voté la création de systèmes d'information de données personnelles à des fins de santé publique, et ce sans le consentement des personnes concernées. Toutefois, les modalités d'application de ces traitements relevant du pouvoir réglementaire, c'est-à-dire pris par décret en Conseil d'Etat, devaient être subordonnés à un avis conforme de la CNIL[1482]. Mais ce contrôle technique, prenant la forme d'un droit de blocage, a été déclaré inconstitutionnel puisque le Conseil constitutionnel a estimé classiquement qu'« *en vertu de l'article 21 de la Constitution et sous réserve de son article 13, le Premier ministre exerce le pouvoir réglementaire à l'échelon national. Ces dispositions n'autorisent pas le législateur à subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire* »[1483].

751. Il existe d'autres menaces concernant les pouvoirs constitués, comme le risque qu'ils se prononcent en faveur d'un traitement automatisé de données personnelles ou non, qui ne serait pas parfaitement celui qui a été mis en œuvre, aboutissant aussi bien à une vulnérabilité à l'encontre des individus que des personnes morales dont l'Etat lui-même[1484]. En effet, la CNIL a par exemple eu à se prononcer au sujet de « *Stopcovid* »[1485] par l'intermédiaire d'un avis simple ; avis pris sur des éléments lacunaires non représentatifs de l'architecture réelle puisqu'elle n'était pas encore intégralement développée. De la même manière, le Parlement peut être amené à se prononcer sur des spécifications différentes du programme final. En ce sens, François Lesueur note[1486] qu'il s'agit d'un problème démocratique lorsque les caractéristiques annoncées, c'est-à-dire théoriques, ne correspondent pas à l'implémentation

---

[1481] ASSEMBLEE NATIONALE, 15e législature, projet de loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, adopté le 9 mai 2020, *Assemblée-nationale.fr* [en ligne]. 4 octobre 2020. [Consulté le 25 octobre 2020]. Disponible à l'adresse : https://www.assemblee-nationale.fr/dyn/15/textes/l15t0418_texte-adopte-seance

[1482] *Ibid*., art. 11 V.

[1483] CC, décision n° 2020-800 DC, 11 mai 2020, *Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions,* §. 77. Avait également été déclaré inconstitutionnel pour les mêmes raisons la subordination de l'exercice du pouvoir réglementaire du Premier ministre à un avis conforme de la CNIL concernant spécifiquement les modalités de gestion et d'utilisation d'un traitement de la sécurité sociale. En effet, une AAI peut être habilitée par le législateur à exercer le pouvoir réglementaire national qu'à la condition que cette habilitation reste *« de portée limitée tant par leur champ d'application que par leur contenu »* CC, décision n° 2006-544 DC, 14 décembre 2006, *Loi de financement de la sécurité sociale pour 2007,* cons. 35 et suivant.

[1484] DOUVILLE T., HERVOCHON C., NOEL E., PAQUIER Y., « Les vulnérabilités numériques », *op. cit.*, p. 117.

[1485] CNIL, Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « *StopCovid* ».

[1486] « *L'implémentation remet en cause des hypothèses de la spécification, hypothèses utilisées pour analyser la privacy, analyse de privacy utilisée par la CNIL et par le parlement lors du vote par exemple* », LESUEUR F., Privacy de StopCovid : La dure réalité de l'implémentation face à la théorie de la spécification, *Flesueur.medium.com* [en ligne]. 11 juin 2020. [Consulté le 26 janvier 2021]. Disponible à l'adresse : https://flesueur.medium.com/privacy-de-stopcovid-la-dure-r%C3%A9alit%C3%A9-de-limpl%C3%A9mentation-face-%C3%A0-la-th%C3%A9orie-de-la-sp%C3%A9cification-9021a4ca2b6a. L'auteur note également dans un autre de ses articles que « *La fourniture d'un code source génère une fausse impression de confiance. Ce programme s'exécute en dehors de la zone contrôlée par l'utilisateur et l'open-source n'apporte donc aucune transparence. Aucune preuve que c'est bien ce programme qui tourne réellement. Aucune preuve que les données ne sont pas récupérées en chemin par un autre programme.* », LESUEUR F., Pourquoi l'open-source n'apporte (presque) rien face aux critiques contre StopCovid », *Flesueur.medium.com* [en ligne]. 13 mai 2020 [Consulté le 25 novembre 2020]. Disponible à l'adresse : https://flesueur.medium.com/pourquoi-lopen-source-n-apporte-presque-rien-face-aux-critiques-contre-stopcovid-24a9dcbb68fe

réelle dans le programme, alors que le vote du Parlement ou l'avis de la CNIL a reposé sur des hypothèses de spécification. Il est toujours possible de considérer que la CNIL peut effectuer des contrôles a posteriori afin de s'assurer de la conformité de l'application à la réglementation, ce qu'elle a par ailleurs fait dans le cadre de « *Stopcovid* »[1487], mais en attendant un tel contrôle, l'outil reste déployé, trahissant de fait le choix démocratique tandis que le traitement a pu produire des effets pendant une certaine durée telle qu'une violation de droit et libertés fondamentales.

752. Par ailleurs, dans le cadre du numérique, le pouvoir réglementaire est susceptible de nuire, voire de rendre ineffective la transparence des traitements algorithmiques, et ce quand bien même la mise en œuvre de ces derniers aurait été votée par le Parlement. En effet, soit le pouvoir réglementaire n'intervient que trop tardivement pour appliquer la loi, comme c'est par exemple le cas en matière d'*open data* des décisions de justice[1488], ou bien il peut dénaturer par l'intermédiaire du décret d'application de la loi son esprit, et donc la mise en œuvre de la transparence en favorisant une technologie plus opaque qu'une autre. En effet, le choix de la mise en œuvre des systèmes d'information autorisée par le Parlement, c'est-à-dire lorsqu'il n'est pas de la compétence du pouvoir réglementaire, est précisé par l'intermédiaire d'un décret d'application. Il y a d'ailleurs fort à parier que si la loi était trop précise dans la mise en œuvre de la transparence, elle serait déclarée inconstitutionnelle par le Conseil.

753. Toutefois, la question de la transparence et du numérique ne peut se résoudre à des ajustements purement techniques. Le numérique, et la manière dont il convient d'assurer sa transparence, voire son exclusion en fonction des secteurs si elle ne peut être assurée, est un débat de nature politique. Ce débat ne peut avoir lieu que dans un cadre démocratique, c'est-à-dire constitutionnellement établi.

754. Les AAI posent un problème de nature démocratique. Et cette problématique n'est pas neuve puisqu'elles confortent l'idée selon laquelle le numérique, et également la transparence de ces systèmes, ne pourrait s'opérer qu'à travers des spécialistes. Il est évident que l'expertise, comme nous l'avons vu, n'est pas politique, raison pour laquelle une institution indépendante du pouvoir politique doit s'en charger. Toutefois, force est de constater qu'au-delà de l'analyse en elle-même des logiciels, l'enjeu démocratique est de taille. Ainsi, comme nous l'avons déjà

[1487] Décision n° MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des solidarités et de la santé. Cette mise en demeure fut par ailleurs clôturée après régularisation par la décision n° 2020-015 du 3 septembre 2020.
[1488] Voir en ce sens au sujet de l'*open data* des décisions de justice, CE, 21 janvier 2021, req. n° 429956.

étudié, toutes les architectures techniques ne se valent pas pour parvenir à un objectif et il convient également d'aborder la manière dont la transparence juridique doit prendre forme. Et nous ne pouvons ignorer le juridique est bien souvent l'émanation d'une intention politique. Hans Kelsen n'a-t-il d'ailleurs pas dit que « *le contenu d'un ordre juridique déterminé prend, dans un cas donné, dépend entièrement du législateur, c'est-à-dire des rapports de puissance existant au moment donné, des individus ou des groupes sociaux qui ont le pouvoir de déterminer le droit* »[1489].

B - Nature de l'organe législatif nouvellement constitué et compétences

755. Il convient d'établir de nouveaux mécanismes d'équilibre des pouvoirs, y compris pour obtenir une meilleure collaboration entre ces derniers. Historiquement[1490], le Parlement est apparu comme l'organe assurant la protection des droits et libertés. Bien qu'il existe une crise de la représentation politique, le Parlement demeure l'organe à la plus grande représentativité. Le pouvoir législatif a été initialement perçu, sous l'influence de l'observation du régime constitutionnel britannique, comme le garant des libertés individuelles, surtout dans la période de l'Etat légicentrique[1491], ce qui se retrouvait dans l'esprit de la DDHC de 1789, notamment par l'intermédiaire d'une loi sacralisée et en tant qu'expression de la volonté générale[1492] avant qu'elle ne le soit que dans le respect de la Constitution[1493]. Le bicamérisme, qu'il soit égalitaire ou non, incarne l'idée selon laquelle la société est scindée en plusieurs ordres, nécessitant la création d'un corps législatif constitué de plusieurs organes, comme c'est le cas au Royaume-Uni avec la participation des lords et du Peuple, dans la formation de l'expression de la volonté générale. Dans d'autres systèmes constitutionnels, comme c'est le cas aux Etats-Unis d'Amérique, il ne s'agit pas de prendre en compte différentes composantes de la société, mais d'offrir en plus du Peuple dans sa dimension nationale, une participation des Etats fédérés[1494].

756. Au-delà de la représentation, l'existence de différents organes au sein du corps législatif est une vertu en ce qu'elle implique une balance des pouvoirs[1495]. Il convient naturellement de

---

[1489] KELSEN H., *Controverses sur la Théorie pure du droit. Remarques critiques sur Georges Scelle et Michel Virally*, *Editions Panthéon-Assas*, 2005, p. 65.
[1490] L'Angleterre était qualifiée de « *mère des parlements* ». Voir en ce sens, ACHAINTRE C., *L'instance législative dans la pensée constitutionnelle révolutionnaire (1789-1799)*, Bibliothèque parlementaire et constitutionnelle, Dalloz, 2008, p. 40.
[1491] REDOR M-J., *De l'Etat légal à l'Etat de droit, l'Evolution des Conceptions de la Doctrine Publiciste Française 1879-1914*, *op. cit*.
[1492] Art. 6 de la DDHC de 1789.
[1493] CC, décision n° 85-197 DC, 23 août 1985, *Loi sur l'évolution de la Nouvelle-Calédonie*, cons. 17.
[1494] HAMILTON A., JAY J., MADISON J., *Le Fédéraliste*, PolitiqueS, Classiques Garnier, réedition, 2012, 648 p.
[1495] DE MONTESQUIEU C., *De l'esprit des lois*, *Barrillot & fils*, 1748 ; TROPER M., *La séparation des pouvoirs et l'histoire constitutionnelle française*, Anthologie du droit, *LGDJ*, 2014, 250 p.

ne pas considérer que le Parlement se suffirait à lui-même, mais il est possible de mieux concevoir la confrontation entre les deux chambres. En France, l'organe législatif est composé de l'Assemblée nationale qui représente le Peuple, et du Sénat qui *« assure la représentation des collectivités territoriales de la République.* »[1496]. De plus, la Vème République a conservé le Conseil économique et social[1497] -représentant de la société civile - en tant qu'auxiliaire du Parlement, puisqu'à défaut de lui avoir confié de la puissance législative, il n'a qu'un rôle purement consultatif[1498]. Cela étant, il était déjà question d'enrichir la représentativité de la chambre haute en la fusionnant avec le Conseil économique et social, même s'il ne s'agissait finalement pas d'en faire un véritable contre-pouvoir à l'Assemblée nationale[1499]. Pourtant, en 1946, le Général de Gaulle dans sa critique du projet de constitution, qui donnera lieu à la IVe République, se prononçait en faveur d'une telle chambre permettant de prendre en considération des enjeux « *qu'une Assemblée purement politique a fatalement tendance à négliger* »[1500]. Enfin, il précisait par ailleurs en ce sens lors du discours de Bayeux du 16 juin 1946 sa volonté qu'elle soit composée notamment « *des représentants des organisations économiques, familiales, intellectuelles, pour que se fasse entendre, au-dedans même de l'État, la voix des grandes activités du pays* »[1501]. Bien que le rôle de la société civile soit essentiel, y compris pour participer à la transparence des algorithmes, raison pour laquelle il conviendra d'établir un écosystème favorable à cet égard comme nous serons amenés à l'aborder[1502], nous ne souhaiterions toutefois pas prendre la direction d'une revalorisation du Conseil économique, social et environnemental, du moins à cette fin.

757. Tout d'abord, force est de constater que la dérive présidentialiste de notre régime constitutionnel, couplée à l'inflation législative et à la complexité des débats dans des domaines de plus en plus pénétrés par des considérations techniques, comme celle du numérique, rend envisageable et opportun un contre-pouvoir politique aux chambres existantes que l'on pourrait qualifier de généraliste. D'autre part, il serait problématique du point de vue de la légitimité politique que des représentants de la société civile puissent bénéficier d'une faculté d'empêcher les propositions de la chambre basse représentant la Nation. Enfin, l'instauration d'une nouvelle

[1496] Art. 24 de la Constitution du 4 octobre 1958.
[1497] Depuis la réforme constitutionnelle de 2008, il a été renommé en Conseil économique, social et environnemental, art. 69 de la Constitution du 4 octobre 1958.
[1498] HAMON F., TROPER M., *Droit constitutionnel*, *LGDJ*, 36e édition, p. 627.
[1499] Il a été question de le fusionner avec le Sénat en 1969. Voir en ce sens, Décret n° 69.296 du 2 avril 1969 décidant de soumettre un projet de loi au référendum, annexe, *Projet de loi relatif à la création de régions et à la rénovation du Sénat*.
[1500] DE GAULLE C., Discours prononcé à Epinal 29 septembre 1946, *Mjp.univ-perp.fr* [en ligne]. [Consulté le 2 janvier 2021]. Disponible à l'adresse : https://mjp.univ-perp.fr/textes/degaulle29091946.htm
[1501] DE GAULLE C., Le discours de Bayeux (1946), *Elysee.fr* [en ligne]. [Consulté le 25 janvier 2021]. Disponible à l'adresse : https://www.elysee.fr/la-presidence/le-discours-de-bayeux-194
[1502] *Infra*., n° 788 et s.

commission parlementaire permanente dédiée aux enjeux du numérique ne saurait pallier les travers de l'absence d'un contre-pouvoir législatif suffisant.

758. Le corps législatif l'a déjà démontré, il est susceptible de voter des dispositions relatives à la transparence des traitements algorithmiques. Tel est par exemple le cas avec le droit d'accès à ses données personnelles[1503], une plus grande transparence des plateformes numériques et de leurs algorithmes[1504], ou encore le droit à l'explicabilité des décisions administratives individuelles fondées sur un traitement algorithmique[1505]. Ainsi, aux vues de la nécessaire constitutionnalisation d'un principe de transparence des traitements algorithmiques, il revient au Parlement de préciser le degré et la nature de la transparence par secteur, c'est-à-dire s'il s'agit parfois d'un droit à une transparence directe ou le cas échéant si elle doit s'accomplir par l'intermédiaire du tiers de confiance que nous proposons, à savoir par une autorité de contrôle technique. Mais le Parlement ne fait pas toujours œuvre libérale comme il a pu le démontrer, et le Conseil constitutionnel ne joue pas toujours pleinement son rôle de contre-pouvoir sur la question des systèmes d'information[1506].

759. La création d'une nouvelle chambre dédiée aux enjeux du numérique est justifiée par la nécessité de prendre en compte des compétences particulières. Au même titre qu'il a fallu créer la CNIL, comme institution technique, des représentants spécialisés sur ces questions seraient les plus à même d'effectuer un meilleur arbitrage entre les droits et libertés fondamentales dans l'environnement numérique. En effet, la conciliation à opérer au sein de cette sphère et le terrain classique n'est pas forcément la même pour parvenir à un objectif défini[1507].

760. La création de tout traitement automatisé de données, publics et privés sous un certain seuil de connexion, engendrant des effets sur la société ou les droits et liberté, nécessiterait l'aval de cette chambre. Il s'agirait donc d'un régime d'autorisation. Dans ce cas de figure, il conviendrait d'une révision constitutionnelle pour que l'instauration de ces traitements soient exclusivement du domaine de la loi au titre de l'article 34 de la Constitution. Il existe certes une compétence d'attribution du pouvoir législatif en matière de libertés publiques, mais les algorithmes exercent parfois des incidences sur l'ensemble de la société sans que cela n'ait de

[1503] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1504] La loi pour une République numérique de 2016 prévoit des dispositions relatives à la transparence des opérateurs de plateforme numérique, Loi n° 2018-1202 du 22 décembre 2018 *relative à la lutte contre la manipulation de l'information*.
[1505] La loi pour une République numérique de 2016 offre une certaine transparence des décisions administratives individuelles prises sur le fondement de traitements algorithmiques.
[1506] *Supra*., n° 653 et s.
[1507] *Infra*., n° 987 et s.

prime abord une incidence sur les personnes[1508]. C'est uniquement parce que le pouvoir législatif sera compétent dans ce domaine que cette chambre spéciale aura ensuite une emprise sur ladite matière. Une fois le texte voté, il resterait toutefois au pouvoir règlementaire le soin de préciser la loi et de veiller à son bon respect sous le contrôle du juge[1509], qui plus est spécialement dédié pour apprécier que les architectures techniques sont bien respectueuses des principes imposés par le législateur[1510]. Cette attribution de compétence en faveur du Parlement aurait également pour but d'éviter que le pouvoir réglementaire ne dénature pas les exigences de transparence comme cela a pu être le cas avec l'application « *Stopcovid* » dans la mesure où il était question, lors de sa mise en œuvre, de publier un rapport sur son fonctionnement, au plus tard le 30 janvier 2021[1511]. Cette exigence n'a finalement pas été accomplie, et un nouveau décret est venu supprimer cette obligation initiale[1512].

761. Toutefois, bien qu'elle soit élue au suffrage universel direct[1513], cette chambre n'aurait pas vocation à remplacer l'Assemblée nationale et le Sénat. Les parlementaires qui composeraient cette chambre ne bénéficieraient pas de l'initiative des lois, ni ne pourraient les voter, mais serait obligatoirement consultés sur les textes comportant un volet numérique et pourrait soit s'opposer totalement à une disposition numérique, soit conditionner son application au respect de principes particuliers comme l'explicabilité par exemple, voire en exclure certains usages, y compris pour motif d'absence suffisant de transparence. En effet, certaines technologies doivent être exclues comme en matière de vote électronique, car elles ne répondent pas aux exigences de principes du droit[1514]. Ces amendements lieraient les chambres principales et elles n'auraient pas d'autres choix que de les adopter ou de purement renoncer à un volet numérique. En effet, si nous prenons l'exemple d'une loi relative à la prévention de l'ordre public[1515], ne pourraient être adoptés des dispositifs de surveillance numérique qu'avec

[1508] Le vote électronique peut par exemple exercer une vulnérabilité sur le corps électoral sans qu'il n'ait d'incidence au premier abord sur les individus. Pour plus de précisions, *Supra*., n° 538 et s.

[1509] A titre d'exemple, tel est déjà le cas concernant le déploiement d'algorithmes utilisés dans le cadre de l'action administrative : « *Il appartiendra notamment, à ce titre, au pouvoir réglementaire, sous le contrôle du juge, de veiller à ce que les algorithmes utilisés par ces traitements ne permettent de collecter, d'exploiter et de conserver que les données strictement nécessaires à ces finalités.* », CC, décision n° 2019-796 DC, 27 décembre 2019, *loi de finances pour 2020*, § 92.

[1510] *Infra*., n° 765 et s.

[1511] *« Le responsable de traitement rend public un rapport sur le fonctionnement de StopCovid dans les trente jours suivant le terme de la mise en œuvre de l'application, et au plus tard le 30 janvier 2021. »*, Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « *StopCovid* », art. 5.

[1512] Décret n° 2021-157 du 12 février 2021 modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « *StopCovid* ».

[1513] Nous recommandons des élections propres à la matière pour assurer une représentation plus fine sur ces enjeux.

[1514] Certaines technologies sont opaques, empêchant de constater la nature de l'altération de la sincérité du scrutin, tandis que d'autres technologies sont plus transparentes, mais elles permettent en contrepartie de retracer le vote de l'électeur, et donc remettent en cause le secret du vote. La transparence plébiscitée dans ces travaux n'est pas celle des personnes juridiques mais du fonctionnement des logiciels, *Supra.*, n° 538 et s.

[1515] Tel pourrait être le cas des technologies particulièrement liberticides comme la reconnaissance faciale ou encore du recours à la police prédictive. Pour ce dernier exemple, voir en ce sens, CASTETS-RENARD C., BESSE P., LOUBES J-M., PERRUSSEL L.,

l'accord de cette chambre. Sans son accord, le législateur « généraliste » serait contraint à poursuivre son objectif que par l'intermédiaire d'une surveillance opérationnelle humaine. Il s'agit donc de créer un contre-pouvoir technique tout en bénéficiant d'une légitimité démocratique, ce que la gouvernance habituelle en matière de numérique ne parvient pas à réaliser.

762. Lorsque des intérêts particuliers sont en jeu, cet auxiliaire législatif pourrait préciser certaines modalités de mise en œuvre des traitements au nom de la souveraineté numérique. Tel serait le cas sur le fait d'exiger de la part de l'administration que des logiciels puissent être déployés qu'à la condition qu'ils s'exécutent sur du matériel fabriqué sur le territoire national ou européen, et dont la chaîne de valeur est contrôlée, afin d'éviter d'aboutir à des interceptions de données de la part de puissances étrangères, ou bien à la neutralisation du système par exemple. Il en serait de même concernant les données de santé[1516]. Cela implique par ailleurs dans le respect de ce nouvel équilibre des pouvoirs que cette matière ne pourrait pas faire l'objet d'habilitation à légiférer par ordonnance.

763. L'autorité de contrôle que nous avons proposé serait à même de conseiller cette chambre sur le chemin de la transparence, ce que sont notamment censées effectuer les études d'impact des lois. En effet, il existe aujourd'hui des hypothèses où les parlementaires doivent se prononcer sur la pérennisation ou l'instauration de dispositifs algorithmiques, comme ce fut le cas pour les algorithmes utilisés dans le cadre du renseignement, sans bénéficier d'analyse d'impact complète ou de rapport précis sur les technologies sur lesquelles ils devaient débattre du fait qu'elles sont confidentielles[1517]. Cette transparence doit au moins être assurée par la commission technique vis-à-vis des parlementaires afin d'apporter des informations suffisantes et véridiques nécessaires au travail législatif.

764. Au-delà de la question de la transparence, cette chambre pourrait également débattre, lorsqu'elle est saisie d'un texte, dans le sens de l'exclusion de certains usages quand bien même les garanties relatives à la transparence seraient atteintes, dans la mesure où la question du

Centre des Hautes Etudes du ministère de l'Intérieur, Rapport relatif Encadrement des risques techniques et juridiques des activités de police prédictive, *Papers.ssrn.com* [en ligne]. 2019 [Consulté le 6 juin 2020]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3418855 et FERET C., POINTEREAU R., Rapport d'information n° 621 sur l'ancrage territorial de la sécurité intérieure du Sénat, session ordinaire 2019-2020, fait au nom de la délégation aux collectivités territoriales, enregistré à la Présidence du Sénat le 9 juillet 2020, et faisant état du développement d'un logiciel de police prédictive par la gendarmerie afin d'anticiper les cambriolages.

[1516] Voir en ce sens la critique sur l'hébergement du *Health data hub*, *supra.*, n° 631 et s.

[1517] FORTEZA P., L'utilisation des nouvelles technologies par les pouvoirs publics, *Site de la Fondation Jean Jaurès* [en ligne] 1er juin 2021. [Consulté le 14 novembre 2020]. Disponible à l'adresse : https://www.jean-jaures.org/publication/lutilisation-des-nouvelles-technologies-par-les-pouvoirs-publics/

numérique ne se cantonne pas qu'à cette problématique. Une technologie réputée parfaite, bien qu'elle n'existe pas à ce jour, c'est-à-dire transparente, sécurisée et sans biais par exemple, n'empêcherait pas des menaces systémiques sur les libertés[1518]. C'est admettre que c'est au politique de façonner l'informatique, et d'utiliser les outils adaptés à l'objectif poursuivi, et non à l'informatique de faire sa loi.

PARAGRAPHE 2 - UNE NOUVELLE REORGANISATION DE LA JUSTICE

765. La justice n'est pas en reste et est amenée à évoluer davantage pour prendre en considération le fait juridique étudié. Le modèle des autorités de régulation en matière de numérique a échoué. Il peine notamment à garantir l'effectivité des droits et libertés, et plus largement de l'ordre juridique. Le pouvoir juridictionnel est précieux, et concourt déjà à la transparence des traitements algorithmiques (A), mais il gagnerait pour plus d'efficacité à se spécialiser (B).

A - L 'actuelle articulation

766. Que l'on considère le pouvoir juridictionnel comme la fonction étatique participant à donner une signification à la norme, ou bien en tant que simple « *bouche de la loi* »[1519], cette puissance est sans doute la plus indépendante des corps constitués. En d'autres termes, les juridictions participent à la transparence des traitements algorithmiques, qui comme nous l'avons vu, est une clé de voûte des droits et libertés, y compris de ceux conceptualisés sur le terrain classique.

767. En matière de transparence, cette fonction, comme pour les autres domaines, va lui donner corps. Les juridictions judiciaires ont déjà eu à connaître, même si cela demeure encore rare, certains contentieux comme cela a par exemple été le cas en matière de droit de la consommation[1520] concernant les exigences de loyauté et de transparence des plateformes numériques. Le juge judiciaire est allé, conformément à son rôle, jusqu'à venir préciser ledit régime juridique. Il est toutefois à noter qu'au regard des algorithmes les plus difficilement observables, le pouvoir juridictionnel se heurte à des difficultés probatoires, qui affectent la

[1518] Tel est par exemple le cas de certains usages comme la reconnaissance faciale.
[1519] De MONTESQUIEU C., *De l'esprit des lois*, *op. cit*.
[1520] TGI de Paris, jugement du 17 décembre 2019, RG 17/06223 ; TGI de Paris, jugement du 24 novembre 2020, association consommation, logement et cadre de vie c/ Be Labo.

bonne tenue des expertises judiciaires. A titre d'exemple, un TGI s'est déjà prononcé en faveur d'une condamnation de la Poste à transmettre une liste de documents à un cabinet d'expertise afin de faire toute la lumière sur le fondement d'un logiciel[1521] suspecté d'avoir dégradé les conditions de travail des salariés.

768. Quant aux juridictions administratives, elles interviennent en tant que juge d'appel des sanctions administratives des AAI, et donc effectuent un contrôle de celles-ci, y compris sur les décisions portant sur les obligations de transparence[1522]. L'ordre administratif a eu de plus à connaître d'un important contentieux relatif aux algorithmes utilisés dans le cadre de l'action administrative, et ce depuis le nouveau régime juridique des décisions administratives individuelles fondées sur un traitement algorithmique[1523]. Le juge administratif est venu entériner la doctrine de la CADA afin d'assimiler les codes sources à des documents administratifs communicables[1524] avant l'adoption de la LRN. Puis la plateforme *ABP*, suivie de *Parcoursup*, a généré un important contentieux. Néanmoins, il apparaît que le Conseil d'Etat n'est pas le plus protecteur en la matière puisqu'il a choisi de retenir une interprétation moins favorable que celle du défenseur des droits ou du TA de Guadeloupe au sujet de la transparence de ces traitements algorithmiques[1525]. Il en est de même en matière électorale où il n'a pas souhaité reconnaître un principe de vérifiabilité des systèmes de vote, alors que l'absence de transparence ne peut que limiter l'émergence d'un contentieux, et sur lequel le juge électoral ne peut plus appréhender le degré d'altération de la sincérité du scrutin[1526], voire du non-respect des autres principes du droit électoral. Pourtant, le juge vérifie dans certaines affaires la documentation des machines à voter, ainsi que les audits privés effectués sur le site de fabrication de ces ordinateurs, mais ce n'est nullement de nature à s'assurer le jour du scrutin que le système fonctionne correctement. De plus, c'est accepter qu'une transparence directe ne peut être opérée par l'électeur lui-même.

769. Le Conseil constitutionnel n'est pas en reste et il a joué un rôle significatif dans la construction du régime juridique de la transparence des traitements algorithmiques, surtout ceux relatifs aux algorithmes auto-apprenants utilisés par l'administration dans le cadre de décisions administratives individuelles exclusivement automatisées en y exigeant une

[1521] TGI de Paris, ordonnance de référé du 13 juin 2017, RG 17/51830.
[1522] A titre d'exemple, voir CE, 19 mai 2017, n° 396698, *Supra*.
[1523] TGI de Paris, jugement du 24 septembre 2019, RG 17/06224.
[1524] TA de Paris, 10 mars 2016, M. X, n° 1508951.
[1525] *Supra.*, n° 473.
[1526] Voir en ce sens, MEKHANTAR J., « Le citoyen, la machine à voter et le juge », *op. cit.*, p. 125 à 146, *Supra*., n° 570 et s.

transparence absolue, dans l'esprit de la loi, ou à défaut leur exclusion[1527]. Et encore plus récemment avec la reconnaissance de la valeur constitutionnelle du droit d'accès aux documents administratifs dans une affaire relative aux algorithmes publics[1528].

770. Toutefois, malgré la forte immixtion des algorithmes dans tous les domaines de la société, le contentieux nous semble anormalement faible. Cette situation émane sans doute d'un problème de nature probatoire. En effet, en dehors de quelques rares affaires médiatisées, ou mises en évidence par des contrôles, les justiciables sont dans l'incapacité de prouver quoi que ce soit, voire ignorent l'étendue des violations de leurs droits. Cet effet est inhérent à l'opacité de ces systèmes, ce qui est d'autant plus regrettable car sans la transparence de ces derniers, les juridictions sont affectées dans leur fonction de juger.

771. La faible spécialisation des juridictions pour la matière numérique handicape nécessairement leur action. Si l'on peut ajouter que de nombreuses AAI[1529] bénéficient non pas d'un rôle juridictionnel, mais contentieux[1530], néanmoins « *réguler n'est pas juger* »[1531]. A titre d'exemple, le pouvoir de sanction des AAI, comme celui de la CNIL depuis 2004, vise également à faire respecter le principe de transparence des traitements algorithmiques[1532]. D'autres services qui ne disposent pas d'une fonction contentieuse participent également à la bonne application de ce principe[1533].

772. Au-delà des sanctions des AAI dans ce domaine, force est de constater que les juridictions jouent déjà un rôle notable et sont d'ailleurs parfois éclairées par la CNIL dans ce domaine par exemple. La LIL[1534] permet en effet aux juridictions de solliciter la CNIL pour des demandes d'avis. Il est à noter qu'en matière pénale elle doit saisir le procureur de la République dès lors que sont portés à sa connaissance des faits criminels ou délictueux, et ce conformément à l'article 40 du CPP[1535]. S'ajoute à cela la possibilité de « *présenter des observations dans les procédures pénales* »[1536], mais également devant toute autre juridiction si le contentieux est

[1527] CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*, § 71.
[1528] CC, décision n° 2020-834 QPC, 3 avril 2020, § 8.
[1529] *Supra*., n° 703 et s.
[1530] PERROUD T., *La fonction contentieuse des autorités de régulation en France et au Royaume-Uni*, *op. cit*.
[1531] QUILICHINI P., « Réguler n'est pas juger », *AJDA*, 2004, p. 1060.
[1532] A titre d'exemple, pour la CNIL, voir 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. Cette délibération a par ailleurs été confirmée par le Conseil d'Etat dans un arrêt du 19 juin 2020, n° 430810. Pour l'AMF, voir par exemple, AMF, déc, du 4 décembre 2015. De plus, selon le Conseil d'Etat, l'enquête de l'AMF au sujet de l'analyse du flux de ces algorithmes a été correctement étayée pour caractériser la manipulation du marché, CE, 19 mai 2017, n° 396698.
[1533] *Supra*., n° 703 et s.
[1534] Art. 8 e) LIL modifiée.
[1535] Art. 8 f) LIL modifiée.
[1536] *Ibid*.

relatif à la protection des données à caractère personnel[1537]. Ainsi, *« La juridiction d'instruction ou de jugement peut appeler le président de la Commission nationale de l'informatique et des libertés ou son représentant à déposer ses observations ou à les développer oralement à l'audience »*[1538].

773. Bien que les juridictions et les AAI ne remplissent pas initialement le même rôle[1539], l'avantage des régulateurs était leur agilité du fait de leur spécialisation et de l'allégement des procédures, en vue notamment d'aboutir à une meilleure fluidité du marché. Mais en plus de poser question vis-à-vis de la traditionnelle séparation des pouvoirs, cette modalité de régulation économique semble également souffrir d'un manque de moyens matériels et humains. De plus, d'un point de vue réaliste, il est possible d'affirmer, sur le fondement de la conception fonctionnelle de la notion de juridiction, notamment utilisée par le juge de Strasbourg[1540], que de nombreuses AAI ne bénéficient pas seulement d'un rôle contentieux mais également juridictionnel[1541]. Puisqu'il existe une convergence en matière procédurale entre les AAI et les juridictions traditionnellement établies, il convient selon nous de considérer que la justice se doit avant tout d'être rendue de manière impartiale et indépendante. Dès lors, cette requalification, qui vise légitimement à rendre effectives les garanties procédurales, fait nécessairement converger les autorités de régulation avec les juridictions traditionnelles, alors que le principal argument de l'existence de ces organes était de réguler rapidement pour plus de fluidité, ce que la justice n'était pas capable de correctement effectuer du fait de sa présumée lenteur. Mais cette lenteur alléguée, que nous contestons par ailleurs, n'est-elle pas plus la conséquence d'une faible spécialisation des traditionnelles juridictions ainsi qu'une faiblesse des moyens alloués pour correctement remplir la mission de dire le droit ? Sans compter que l'étanchéité entre les sections d'enquête et contentieuse est parfois discutable, alors qu'elle est censée assurer l'impartialité et l'indépendance dudit organe. Il est à noter que nous ne devrions pas nous habituer à tout système amené à centraliser plusieurs fonctions de l'Etat[1542].

[1537] Art. 8 5.
[1538] Art. 41 LIL modifiée.
[1539] OCHOA N., *Le droit des données personnelles, une police administrative spéciale*, Thèse de doctorat, présentée et soutenue publiquement le 8 décembre 2014 à l'Université Paris I -Panthéon -Sorbonne, p. 238.
[1540] Voir en ce sens, art. 6 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales relatif au droit à un procès équitable.
[1541] MILANO L., « Qu'est-ce qu'une juridiction ? La question a-t-elle encore une utilité ? », *RFDA*, 2014, p. 1119.
[1542] A ce titre, certaines instances, dont la CNIL, sont amenées à sanctionner les interprétations des textes qu'elles font au titre de leur pouvoir réglementaire. Bien que d'un point de vue organique ce travail n'est pas effectué par les mêmes sections, laissant apparaître une certaine étanchéité, l'institution demeure petite et des pratiques sont susceptibles de nuire à cette séparation théorique comme cela est le cas avec le Conseil d'Etat.

774. De plus, si nous prenons exemple de la CNIL, elle s'inscrit davantage dans une tradition pédagogique que dans celle du répressif[1543] puisque sur l'année 2019, elle n'a infligé que huit sanctions[1544]. Cette situation, qui n'est pas propre à la France, explique sans doute pourquoi certains justiciables préfèrent se tourner vers les tribunaux pour faire respecter les dispositions relatives au RGPD, et donc à la transparence, plutôt que de recourir à un régulateur[1545].

B - Concourir autrement à une meilleure transparence des traitements algorithmiques par la spécialisation juridictionnelle

775. Il ne fait aucun doute que le pouvoir juridictionnel participe déjà à la construction d'un régime juridique en matière de transparence des traitements algorithmiques. Néanmoins, la complexification des technologies, dont leur transparence est par ailleurs parfois incertaine du point de vue technique, rend l'effectivité des droits humains difficile. Et même au-delà de la transparence, tous les usages du numérique ne sont pas juridiquement acceptables[1546]. En d'autres termes, comment convient-il d'adapter la justice à ce nouvel enjeu ?

776. L'enjeu de la transparence des systèmes d'information est double puisqu'il permet à la justice de venir appliquer le régime juridique du principe de transparence des traitements algorithmiques protégé par la Constitution et précisé par le législateur, voire en l'absence d'une telle intervention, participer à l'élaboration de ce cadre juridique lorsqu'il juge les cas d'espèce. La neutralité du droit par rapport à la technologie, c'est-à-dire ce que nous appelons le processus visant à développer des concepts juridiques sans nécessiter le recours à une technologie particulière pour y parvenir, est une qualité essentielle du législateur. C'est notamment de cette manière que la LIL a su s'adapter à travers les différents âges de l'informatique, et est applicable à l'algorithme le plus simple, jusqu'aux techniques les plus sophistiquées en matière d'IA. Toutefois, cette neutralité de la norme juridique implique nécessairement un rôle du juge en matière de transparence afin de s'assurer que, quel que soit la technologie, elle soit conforme à la réglementation.

777. Mais pour ce faire, nous ne sommes pas favorables au rôle croissant des AAI dans ce domaine pour les raisons explicitées[1547]. D'une certaine manière, la justice est concurrencée

[1543] OCHOA N., « *Le droit des données personnelles, une police administrative spéciale* », *op. cit*., p. 240.
[1544] CNIL, *Rapport d'activité 2019 de la Commission Nationale de l'Informatique et des Libertés*, juin 2020, p. 4.
[1545] MANANCOURT V., Have a GDPR complaint ? Skip the regulator and take it to court, *op. cit*.
[1546] LEQUESNE ROTH C., « De l'éthique et des algorithmes : pour une juridicisation des enjeux », *Recueil Dalloz,* 2020, p. 1833.
[1547] *Supra*., n° 773 et s.

dans son rôle juridictionnel par une pluralité d'autorités de régulation disposant d'un pouvoir de sanction. Dans le cadre de la régulation du numérique, et donc notamment de la conformité aux règles de transparence des traitements de données à caractère personnel, la CNIL ne bénéficiait initialement pas, par exemple de ce pouvoir répressif apparu seulement en 2004[1548] lors de la transposition de la directive 95/46/CE[1549]. Pouvoir qui a d'ailleurs été renforcé avec l'adoption du RGPD, y compris quant aux montants de ces sanctions[1550]. Pourtant, lors des discussions relatives à l'instauration d'une AAI pour connaître certains enjeux relatifs à l'informatique, il était précisé que le Comité devant être créé ne serait pas une juridiction, ne serait-ce que « *s'il en était une, il retirerait sans motif décisif une partie de leur compétence aux juridictions judiciaires et administratives et il en résulterait, outre des inconvénients psychologiques, des conflits de compétences et des délais dans des domaines où il faut au contraire agir vite* »[1551]. Paradoxalement, comme nous l'avons vu, les AAI se juridictionnalisent, y compris dans ce domaine[1552]. Favoriser des organes de régulation au prétexte que les organes traditionnels seraient incapables de s'adapter à l'émergence de nouveaux faits juridiques n'est rien d'autre qu'une démission politique et démocratique.

778. La spécialisation des juridictions pour appréhender le phénomène du numérique n'est pas une idée nouvelle puisqu'il s'agissait déjà d'une volonté initiale. Les premiers projets de loi[1553] tendant à la création d'un comité de surveillance de l'informatique proposaient également le recueil de plaintes et leur traitement non pas par ladite autorité, mais par une juridiction spécialisée, et le plus souvent par une section dédiée du Conseil d'Etat appelée Tribunal de l'informatique. Par ailleurs, force est de constater que nous assistons depuis quelques années à la multiplication des tentatives de spécialisation de la justice. En matière pénale, des parquets ont été créés, comme le parquet national financier[1554], et plus récemment un tribunal judiciaire spécialisé dans la répréhension des contenus haineux tenus sur les réseaux sociaux[1555]. Cette tendance est également observable en matière de droit de l'environnement avec l'instauration

[1548] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1549] 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.
[1550] *Supra.*, n° 201 et s.
[1551] COMMISSION INFORMATIQUE ET LIBERTES, Rapport, *La Documentation française*, 1975, p. 73.
[1552] *Supra*., n° 766 et s.
[1553] *Supra*., n° 696 et s.
[1554] Loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière.
[1555] Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (1), art. 10 ; et création d'un pôle national de lutte contre la haine en ligne au tribunal judiciaire de Paris, circulaire du ministre de la Justice en date du 24 novembre 2020, *Legifrance.gouv.fr* [en ligne]. [Consulté le 15 décembre 2020]. Disponible à l'adresse : https://www.legifrance.gouv.fr/download/pdf/circ?id=45086

de juridictions spécialisées[1556]. Ces tentatives, s'il est encore trop tôt pour savoir si elles seront des réussites, visent à notamment répondre à l'inflation de normes sectorielles, mais également à l'émergence de nouveaux faits juridiques ou au rejet de leur acceptation. Et nous ne pouvons pas nier que le numérique, auquel la question de la transparence est rattachée pour une meilleure effectivité des droits et libertés, mérite réflexion.

779. Il n'est pas certain que la création d'une juridiction spécialisée ait aujourd'hui un sens car le numérique fait son immixtion dans tous les secteurs, mais il semble a minima opportun que chaque juridiction soit dotée d'une chambre spécialisée dans la question du numérique. Cela se justifie par le fait que les juges soient spécialement formés sur ces sujets. Ces chambres seraient suppléées d'un point de vue technique par l'expertise de notre autorité de contrôle unique nouvellement créée[1557], et qui aurait pour objectif de cartographier les architectures et leurs incidences sur les libertés. Ainsi, les juges auront la capacité d'effectuer un contrôle a posteriori de ces algorithmes afin de s'assurer qu'ils sont conformes au droit.

780. Les interprètes doivent veiller à assurer l'équilibre entre les droits et libertés en permanence, notamment en n'hésitant pas à opérer une conciliation différente du terrain classique, car propre à la sphère numérique, pour parvenir à l'objectif préalablement fixé. Et c'est d'autant plus le cas lorsque les technologies déployées n'ont pas été créées pour ledit usage. A titre d'exemple, concernant spécifiquement la question de l'application des lois, ce qui revient au pouvoir réglementaire en vertu de l'article 21 de la Constitution, le juge sera mieux armé pour contrôler le bon respect des principes fixés par le Parlement, par les choix techniques opérés par le gouvernement comme l'a déjà jugé le Conseil constitutionnel. Il a en effet considéré que concernant le déploiement d'algorithmes utilisés dans le cadre de l'action administrative : « *Il appartiendra notamment, à ce titre, au pouvoir réglementaire, sous le contrôle du juge, de veiller à ce que les algorithmes utilisés par ces traitements ne permettent de collecter, d'exploiter et de conserver que les données strictement nécessaires à ces finalités* »[1558]. Les juges pourraient également donner mandat à cette autorité afin qu'ils suivent sur une période déterminée l'évolution du traitement, et ce afin de s'assurer que des mises à jour logicielles ne remettraient pas en cause les constatations opérées lors du procès. Pour ce faire, il est nécessaire de contrôler avec précision les architectures sélectionnées et leur mise en

[1556] Loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée.
[1557] *Supra*., n° 717 et s.
[1558] CC, décision n° 2019-796 DC, 27 décembre 2019, loi de finances pour 2020, § 92.

œuvre, ce qui relève du pouvoir réglementaire. Cela nécessite donc une formation ainsi qu'une importante réactivité.

781. Il est nécessaire de ne pas dissocier l'algorithme de la norme, ne serait-ce parce qu'il est le plus souvent l'une des interprétations de celle-ci. Comme nous l'avons évoqué, soit des programmes ont été spécialement développés pour opérer certaines conciliations entre les droits et libertés, soit ils ont été déployés alors qu'ils étaient pensés pour des usages différents, auquel cas il adviendra de faire cesser ce type de logiciel pour une finalité particulière. Les programmeurs ne doivent pas être les véritables interprètes des normes, car bien qu'ils codent le droit, les juges doivent avoir la capacité d'effectuer des contrôles de légalité, voire de constitutionnalité des logiciels affectant les droits et libertés fondamentales. Les algorithmes sont un des supports possibles de la norme et il convient de le prendre en considération, raison pour laquelle, sans transparence, ce contrôle ne peut être effectué. Il convient d'appréhender ces algorithmes pour ce qu'ils sont parfois, c'est-à-dire des interprétations du droit nécessitant qu'ils sont conformes à la norme qui leur est supérieure. A titre d'exemple, de nombreux organismes précisent que les algorithmes qu'ils utilisent « *sont la traduction de la réglementation en vigueur* »[1559].

782. Enfin, concernant l'enjeu probatoire inhérent au numérique, puisque les violations du droit y sont difficilement observables par nature, les justiciables doivent pouvoir sur simple faisceau d'indices saisir la division « expertise » de l'autorité technique que nous préconisons afin qu'elle se prononce sur ces doutes, et le cas échéant décide de transmettre la plainte à la juridiction compétente. Bien évidemment, cette faculté s'effectuerait dans les règles de l'impartialité et de l'indépendance des expertises judiciaires, conformément au droit à un procès équitable[1560]. Naturellement, les recours collectifs, comme cela se fait désormais en matière de données à caractère personnel[1561], doivent être élargis à tout traitement remettant en cause les droits et libertés, ou ayant des incidences sur la société pour prendre en compte la dimension collective des algorithmes. En effet, les logiciels ont parfois des effets systémiques sur le droit et les personnes, et il est nécessaire de les comprendre avec le plus d'agrégation de données possibles, ce que permet le recoupement d'informations dans la constitution des dossiers.

[1559] En ce sens, voir POLE EMPLOI, Algorithmes. Tout savoir sur les algorithmes publiés par Pôle emploi, *op. cit.*
[1560] Art. 6 § 1, Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentale.
[1561] Art. 37, loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

783. L'articulation entre la division « expertise » et les juridictions spécialisées a une importance significative, puisque la transparence joue un rôle dans le contentieux de la responsabilité, du moins lorsque les technologies sont intelligibles. Elle permet en effet d'identifier la responsabilité des acteurs ayant utilisés les algorithmes, alors que la tentation est aujourd'hui de créer des fonds d'indemnisation qui déresponsabiliseraient ces derniers comme cela est le cas en robotique[1562], et donc leur ôteraient toute pression sur leurs agissements et choix algorithmiques, bien que tous les problèmes de traitement ne résultent pas toujours de l'intention. Les magistrats spécialisés seraient les plus à même de saisir les traitements pour savoir quel est le régime juridique qui leur est applicable[1563]. Le juge pourrait le cas échéant mettre un terme au traitement si l'inadéquation est constatée par notre autorité de contrôle unique à compétence générale. Face au risque systémique de certains algorithmes, surtout lorsque ces derniers sont inexplicables ou qu'ils ont une incidence sur de nombreuses situations individuelles, le pouvoir juridictionnel doit avoir la capacité de mettre fin à de tels traitements pour faire cesser ce risque collectif.

CONCLUSION DU CHAPITRE II

784. Le principe de transparence des traitements algorithmiques, nécessaire à l'observation des faits juridiques induits par l'informatique, ne peut s'exercer et être effectif que par l'intermédiaire d'institutions spécialisées. La multiplication des AAI ou l'élargissement de leurs compétences à la matière numérique sur la question de l'observation des algorithmes aboutit à un éclatement de la puissance publique dans la compréhension de ce phénomène. Au lieu de proposer une instance suprême dans ce domaine, qui bénéficierait à la fois d'un pouvoir de contrôle, réglementaire et de sanction, il nous a semblé plus opportun d'être davantage respectueux de la traditionnelle séparation des pouvoirs. Pour ce faire, sans modifier le tissu actuel des AAI déjà présentes, et dont l'approche sectorielle est intéressante, une autorité dédiée à la surveillance des traitements algorithmiques publics et privés fait sens. Toutefois, pour donner corps à l'exercice de cette transparence, une réforme institutionnelle ambitieuse impliquant la création d'une chambre législative, dont le rôle serait de préciser la nature et le

[1562] Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique, 2015/2103(INL), § 59. Voir également, NEVEJANS N., *Traité de droit et d'éthique de la robotique civile, LEH édition*, 2017, 1232 p.

[1563] Les *lootbox* sont-elles des jeux de hasards ? Les *lootbox* sont « *un terme qui désigne des pochettes surprises à contenu virtuel aléatoire et obtenues dans des jeux vidéo* ». En fonction des jeux vidéo, le régime juridique applicable n'est pas le même. Tout dépend du fonctionnement des algorithmes. Voir en ce sens, réponse du Secrétariat d'État, auprès du Premier ministre, chargé du numérique publiée dans le JO Sénat du 08/02/2018, Microtransaction, loot boxes et jeu vidéo, p. 558.

degré de cette dernière par secteur, voire l'exclusion de la technologie lorsqu'elle ne respecte pas les droits et libertés, est indispensable. Bien que cette création ne suffise pas à évincer les risques de l'illibéralisme[1564] au sein de la sphère numérique, elle serait justifiée par un renforcement de la balance des pouvoirs au sein du pouvoir législatif, ce qui constituerait un contre-pouvoir de nature aussi bien démocratique que technique. Enfin, la spécialisation de la justice est un enjeu de taille, car il s'agit du corps constitué dont la mission est d'assurer avec plus d'efficacité l'effectivité de la transparence permettant ensuite d'appliquer les régimes juridiques adéquats aux faits.

[1564] JAUME L., « « Démocratie illibérale » : une nouvelle notion ? », *op. cit.*

CONCLUSION DU TITRE I

785. Une clarification d'ordre constitutionnel est impérative afin d'éviter un conflit de normes empêchant la transparence des traitements algorithmiques, surtout vis-à-vis des libertés économiques, principales entraves à l'épanouissement de la démocratie dans un monde toujours plus numérique. Même s'il n'est pas question d'assurer la transparence de tous les algorithmes, c'est au législateur qu'il reviendrait de mettre en œuvre un principe général de transparence de ces outils numériques. Néanmoins, le fonctionnement actuel des institutions connait un certain nombre de limites à cet égard.

786. Ainsi, nous nous prononçons en faveur d'une nouvelle chambre législative dédiée aux enjeux du numérique. Des juridictions spécialisées seraient également un atout certain afin de participer à cette transparence dans le but de se saisir de l'application des règles de droit au sein de l'environnement numérique. Une autorité de contrôle unique bénéficiant du monopole au sujet de l'étude de ces outils est par ailleurs indispensable à l'effectivité des droits et libertés, mais aussi de façon à mieux conseiller les pouvoirs constitués sur les incidences des algorithmes sur les personnes et la société.

787. La réponse institutionnelle n'est toutefois qu'un des éléments participant à la levée de l'opacité de ces traitements. Ainsi, la société civile concourt également à ce principe, et il convient de développer un écosystème juridique favorable à cette quête.

Titre II – LA MISE EN ŒUVRE DU PRINCIPE GENERAL DE TRANSPARENCE DES TRAITEMENTS ALGORITHMIQUES

788. La nécessaire adaptation du droit constitutionnel à des fins d'accomplissement d'une transparence des traitements algorithmiques ne peut occulter que des règles d'un rang normatif inférieur sont nécessaires à la mise en œuvre d'un principe de transparence général des outils numériques. Ainsi, il existe naturellement plusieurs façons de venir préciser ce principe qui serait une exigence constitutionnelle.

789. Même si nous avons choisi de traiter cet objet d'un point de vue étatique pour les raisons de souveraineté que nous avons abordé[1565], l'Etat devrait penser un écosystème juridique concourant à la transparence de ces technologies (Chapitre I). Qu'il s'agisse de la société civile ou des professionnels du numérique, ils jouent déjà un rôle significatif dans la compréhension de ces systèmes, ce qu'il convient d'encourager.

790. Par ailleurs, de nouvelles obligations en matière de transparence des algorithmes sont susceptibles d'être déployées pour plus d'efficacité, ce à quoi travail l'Union européenne à travers de nouvelles propositions de réglementations (Chapitre II). La transparence des algorithmes, quand bien même serait-elle réalisée d'un point de vue juridique, puis technique lorsque cela est possible, ne doit pas être un argument de légitimation de recours à des technologies attentatoires aux libertés. En d'autres termes, il conviendrait d'exclure dans certains cas certains usages algorithmiques.

[1565] *Supra*., n° 603 et s.

CHAPITRE I - VERS UN « ECOSYSTEME » JURIDIQUE CONCOURANT A LA TRANSPARENCE DES TRAITEMENTS ALGORITHMIQUES

791. Après avoir évoqué la constitutionnalisation d'un principe de transparence des traitements algorithmiques ainsi que la conciliation de celui-ci avec les autres droits et libertés, puis enfin la nécessaire réforme institutionnelle pour le mettre en œuvre, il convient désormais d'appréhender d'autres mécanismes permettant de concourir en pratique à accomplissement. C'est en cultivant un système global cohérent, c'est-à-dire incluant l'ensemble des techniques juridiques servant le principe étudié, qu'il sera possible d'en garantir l'effectivité.

792. L'Etat et la hiérarchie des normes ne sont pas désuets contrairement à ce qu'affirment certains auteurs[1566]. Le droit étatique cohabite avec le réseau, ce qui a par ailleurs toujours été le cas. La société nourrit le droit, y compris pour résoudre des problèmes complexes. Il convient d'en prendre conscience pour penser l' « écosystème »[1567] juridique le plus à même de participer au principe de transparence dans notre cas d'étude.

793. C'est la raison pour laquelle il est nécessaire de partir de l'existant afin de l'améliorer, car certaines initiatives déjà déployées sont prometteuses et mériteraient d'être renforcées, ou consolidées pour d'autres. Il s'agit de démontrer que la société civile est amenée à concourir à une plus grande transparence des traitements algorithmiques (Section I), ce qu'elle effectue déjà en partie. L'Etat doit en effet offrir un cadre dans lequel cette société pourra s'épanouir en ce sens.

794. Mais la société civile ne peut pas tout, car elle n'est pas un contre-pouvoir institutionnel, seulement une entité dans laquelle s'affronte et se rencontre une pluralité d'acteurs aux intérêts divergents, et qui nécessite parfois la résolution des litiges et des points de vue devant les juridictions. Les acteurs du numérique ne peuvent en revanche s'auto-réguler. Il convient donc de prévoir également une limitation du pouvoir informel de ceux qui développent et déploient les algorithmes. Face aux enjeux complexes du numérique et de sa compréhension, y compris pour son acceptabilité sociale, les acteurs qui conçoivent ces programmes doivent être soumis à une déontologie et non à une simple éthique. Pour reprendre Christian Vigouroux, « *l'éthique*

[1566] BARRAUD B., *Repenser la pyramide des normes à l'ère des réseaux : pour une conception pragmatique du droit, L'Harmattan*, 2012, 394 p.

[1567] Le terme d'écosystème est repris du livre blanc sur l'intelligence artificielle de la Commission européenne. Voir en ce sens, COMMISSION EUROPEENNE, Livre blanc, Intelligence artificielle, Une approche européenne sur l'excellence et la confiance, Bruxelles, p. 3, *Ec.europa.eu* [en ligne]. 19 février 2020. [Consulté le 12 avril 2020]. Disponible à l'adresse : https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf

ou la science de la morale correspond à la recherche d'une manière d'être, à la sagesse dans l'action. L'éthique est personnelle. Elle est d'ordre facultatif, relève de l'autonomie de la volonté, elle exprime une recherche permanente alors que la déontologie est fixée et obligatoire et fait partie de ce que l'on adopte nécessairement en choisissant un métier »[1568] (Section II).

SECTION I – SOCIETE CIVILE ET TRANSPARENCE DES TRAITEMENTS ALGORITHMIQUES

795. La société civile est amenée par son action à jouer un rôle essentiel dans la participation à la transparence des dispositifs numériques, ce qui fait partie intégrante de la démocratie continue[1569].

796. L'objectif est de parvenir à un écosystème encourageant ce principe, notamment car force est de constater que d'une part les institutions relatives à la représentation ne peuvent pas tout, et d'autre part, la société civile participe déjà à la transparence des traitements algorithmiques. Il convient toutefois d'entretenir et d'accélérer ce mouvement.

797. Naturellement ces acteurs n'ont pas et n'auront pas tous le même point de vue sur la nature et le degré de transparence des programmes, mais la rencontre des intérêts, au sein de la société, fait émerger un débat, qui parfois est tranché par les tribunaux ou repris par le pouvoir politique. En ce sens, ils participent à la transparence des algorithmes, et plus largement au numérique. Cette société civile, dont font partie les corps intermédiaires[1570], doit pouvoir s'épanouir dans un cadre juridique établi, ce qui ne l'empêche pas par ailleurs de s'exprimer en faisant peuple par l'intermédiaire de ses représentants[1571].

798. Nous considérons que cette démocratie continue s'exerce au sein de la société civile à la fois de manière institutionnelle (Paragraphe 1) mais aussi non institutionnelle (Paragraphe 2).

[1568] VIGOUROUX C., *Déontologies des fonctions publiques*, *Dalloz*, 2012, p. 11.

[1569] ROUSSEAU D., La démocratie continue : fondements constitutionnels et institutions d'une action continuelle des citoyens, *Confluence des droits_La revue* [en ligne]. Février 2020 [Consulté le 3 avril 2020]. Disponible à l'adresse : https://confluencedesdroits-larevue.com/?p=726

[1570] Nous avons décidé de retenir une acception large de la notion de corps intermédiaire. Voir en ce sens, BOUNEAU C., « Introduction », in *Histoire, économie & société*, 2016/1, 35e année, p. 5 à 13, note 5 [en ligne]. [Consulté le 22 février 2020]. Disponible à l'adresse : https://www.cairn.info/revue-histoire-economie-et-societe-2016-1-page-5.htm#no5 : « *Classiquement, la science politique distingue des catégories fonctionnelles de corps intermédiaires correspondant aux associations, aux organisations politico-sociales et aux organisations professionnelles sectorielles selon la répartition élaborée par Yves Mény dans ses travaux. À ces trois catégories pourraient s'ajouter les médias, qui servent d'intermédiaire entre la société civile et le pouvoir politique, et qui peuvent également être considérés comme des groupes intermédiaires* ».

[1571] *Supra.*, n° 745 et s.

PARAGRAPHE 1 – La société civile non institutionnelle

799. Afin de s'assurer d'une participation active de la société civile au principe de transparence, il convient de prendre en considération le rôle joué par les associations en la matière et la manière dont il est nécessaire de favoriser cette action (A). Remarquons également que parmi la société civile non institutionnelle, le régime juridique du lanceur d'alerte doit évoluer, ne serait-ce car il est démontré qu'il éclaire sur le fonctionnement de ces programmes (B).

A - Les associations et autres initiatives

800. Le rôle des associations est multiple. Elles jouent un rôle d'alerte, y compris en matière de transparence des traitements.

801. Bien que de nombreux acteurs participent dans une démarche individuelle à la justice, certains groupements comme les associations, dont la mission première est la protection des droits et libertés, œuvrent également au principe étudié. Il peut s'agir d'associations généralistes, car les algorithmes ont fait leur immixtion dans leur domaine, ou spécialisées. Ces dernières vont jouer tout à la fois une mission d'alerte et d'effectivité des droits et libertés, y compris dans l'environnement numérique.

802. Elles sont susceptibles d'y participer de différentes manières. Leur mission passe notamment par de nombreuses actions en justice pour contester certaines pratiques ou normes étatiques qui iraient à l'encontre des droits et libertés. Comme nous l'avons évoqué, c'est également devant les prétoires que les interprétations du droit s'entrechoquent. La difficulté réside dans le fait que sans procès, les faits juridiques échappent à la justice, ce qui est particulièrement frappant en matière numérique et a pour conséquence de réduire l'effectivité du principe de transparence. En effet, dans l'immense majorité des cas, la justice est rendue parce qu'à l'origine il y a l'initiative d'un requérant, et que par conséquent, ces acteurs y participent. La justice, en tant que corps constitué, incarne le rôle ternaire de l'Etat pour trancher une situation conflictuelle[1572]. Certaines associations bénéficient d'une importante expertise en matière de numérique, ce qui constitue un contrepouvoir politique et technique, surtout lorsqu'elles agissent en qualité de justiciable.

[1572] SUPIOT A., *La gouvernance par les nombres, op. cit.*

803. Nous pouvons en ce sens citer plusieurs exemples de décisions ayant fait évoluer le régime juridique de la transparence des algorithmes sous l'impulsion d'associations. Tel est le cas de l'Association « *UNEF* » concernant la contestation de la plateforme « *Parcoursup* »[1573], ce qui a notamment abouti à une question prioritaire de constitutionnalité faisant évoluer le régime juridique du droit d'accès à ces algorithmes[1574]. Des entités plus spécialisées comme l'association « *ouvre boîte* » ont également participé à l'obtention du code source de logiciels utilisés par l'Etat en intentant un recours en justice devant le Tribunal administratif, et ce dans l'attente d'un avis CADA après le délai de deux mois[1575]. Plus récemment, elle a par exemple obtenu par ordonnance du Conseil d'Etat que soit enjoint au ministre de la justice l'arrêté prenant « *le soin de fixer " pour chacun des ordres judiciaire et administratif et le cas échéant par niveau d'instance et par type de contentieux, la date à compter de laquelle les décisions de justice sont mises à la disposition du public* »[1576]. Même si nous avons évoqué notre réticence au regard de l'*open data* des décisions de justice[1577], force est de reconnaître qu'il participe au principe de publicité des décisions des justices[1578], et à notre sens, à la potentielle transparence directe des traitements automatisés réutilisant ces données[1579].

804. Dans le cadre de l'urgence sanitaire mise en place lors de la pandémie de la COVID-19, période durant laquelle de nombreux traitements algorithmiques y compris de données à caractère personnel ont été déployés en dehors de tout cadre juridique, des associations, comme « La ligue des droits de l'homme » et « La quadrature du net », sont intervenues afin de mettre fin à certaines violations. Tel a été le cas de la surveillance par drone dans le cadre de missions de police administrative par la Préfecture de police de Paris. En effet, l'instruction a révélé que

> « *les appareils en cause qui sont dotés d'un zoom optique et qui peuvent voler à une distance inférieure à celle fixée par la note du 14 mai 2020 sont susceptibles de collecter des données identifiantes et ne comportent aucun dispositif technique de nature à éviter, dans tous les cas, que les informations collectées puissent conduire, au bénéfice d'un autre usage que celui actuellement pratiqué, à rendre les personnes auxquelles elles se rapportent identifiables. Dans ces conditions, les*

[1573] TA Guadeloupe, 4 février 2019, *UNEF c. Université des Antilles*, req. n° 1801094 et CE, 15 janvier 2020, req. n° 433296.
[1574] CC, décision n° 2020-834 QPC, 3 avril 2020. Pour plus de précisions, *Supra.*, n° 473 et s.
[1575] CADA, avis n° 20180276 du 19 avril 2018.
[1576] CE, 21 janvier 2021, req. n° 429956.
[1577] *Supra*., n° 375 et s.
[1578] PERROUD T., « L'open data des décisions de justice », *Recueil Dalloz*, 2021, p. 344.
[1579] *Supra.*, n° 375 et s. COUR DE CASSATION, Open Justice & L.A.B.E.L. : l'innovation technologique au service de l'anonymisation et de la diffusion de la jurisprudence, *op. cit*.

données susceptibles d'être collectées par le traitement litigieux doivent être regardées comme revêtant un caractère personnel »[1580].

805. C'est au vu des caractéristiques techniques de l'appareil, qu'il a été permis de s'apercevoir qu'un tel usage n'avait pas encore été encadré par voie réglementaire[1581], et donc que le régime juridique applicable était tout autre que celui argué par la Préfecture de Police, puisqu'il s'agissait bien d'une collecte de données personnelles. Ainsi, cette décision a eu pour conséquence d'autoriser uniquement les vols de surveillance non dotés d'un tel zoom ou progressant à plus haute altitude, et ce afin de ne pas identifier les personnes. Au regard de ces éléments, il est possible de considérer qu'au même titre que les journalistes, les associations jouent un rôle de « *chien de garde* » de la démocratie[1582], y compris concernant l'application des droits et libertés à l'environnement numérique.

806. Les associations en droit de la consommation n'interviennent pas que judiciairement[1583] puisqu'elles sont également très actives par l'intermédiaire d'enquêtes ou de débats publics comme sur l'obsolescence programmée, voire logicielle des objets numériques, et ce afin d'informer le consommateur, mais également de militer en faveur d'un régime juridique plus adéquat[1584]. En effet, des objets peuvent être rendus inutilisables à cause d'algorithmes, surtout à la suite de mises à jour altérant la jouissance du produit[1585].

807. En matière de données à caractère personnel, les associations peuvent désormais sous condition[1586] intenter des actions de groupe de plusieurs personnes physiques devant les juridictions civiles et administratives dès lors qu'un dommage émane d'une cause commune à la violation de dispositions du RGPD et de la LIL[1587], et ce dans le but d'en faire cesser le manquement ou d'obtenir réparation, ce qui inclut le respect du principe de transparence prévu par ce régime juridique[1588].

[1580] CE, ordonnance du 18 mai 2020, req. n° 440442 et 440445, § 17.
[1581] *Ibid*., § 18.
[1582] CEDH, Observer et Guardian c. Royaume-Uni, 26 novembre 1991, req. n° 13585/88.
[1583] Voir par exemple en ce sens, TGI de Paris, jugement du 17 décembre 2019, RG 17/06223 sur la loyauté des plateformes numériques par défaut de transparence. *Supra*.
[1584] VAVASSEUR L., CHASSON A., GHESQUIERE Q., Livre blanc, 50 mesures pour une consommation et une production durable, p. 33, *Halte à l'obsolescence programmée.org* [en ligne]. Février 2019 [Consulté le 16 mars 2020]. Disponible à l'adresse : https://www.halteobsolescence.org/wp-content/uploads/2019/03/Livre-Blanc.pdf. 60 millions de consommateur ou UFC que choisir mènent également des actions sur l'obsolescence logicielle en portant également ces thématiques dans le débat public.
[1585] *Supra.*, n° 287 et s.
[1586] Art. 38 de la LIL modifiée.
[1587] Art. 37 de la LIL modifiée.
[1588] *Supra.*, n° 80 et s.

808. L'agrément est au cœur de la participation à la cause de la transparence, car le plus souvent il permet à ces associations de gagner en visibilité et en efficacité. L'agrément octroyé par l'autorité publique à une association est une reconnaissance engendrant certaines incidences juridiques. Il va lui permettre d'obtenir une visibilité et une plus grande confiance vis-à-vis du public. Et surtout, l'intérêt à agir, nécessaire pour entreprendre des actions en justice pour faire respecter les droits et libertés fondamentales, est facilité, puisqu'il n'est plus besoin de le démontrer. Il existe par ailleurs de nombreuses catégories d'agréments[1589] et elles n'emportent pas nécessairement le même régime juridique, raison pour laquelle nous plaidons en faveur d'un agrément qui serait propre à la matière numérique comme cela est aujourd'hui le cas en droit de l'environnement. Cette technique juridique est intéressante. En effet, comme nous l'avons vu, il existe des similitudes entre la matière numérique et environnementale, ne serait-ce que parce qu'elles sont fortement imbriquées. Les associations agréées protection de l'environnement peuvent prendre part aux débats « *dans le cadre des instances consultatives ayant vocation à examiner les politiques d'environnement et de développement durable* »[1590]. Ainsi, cela leur permettrait de siéger dans certains comités décisionnels étatiques, voire de certaines grandes entreprises privées pour les associer à des prises de décision ou *a minima* à des réunions d'information sur les plus grands projets mettant en œuvre des traitements[1591]. La démocratie continue ne devrait pas porter que sur les actions des organismes publics. Elle doit aussi être pensée dans les relations avec les acteurs privés, car certaines activités privées sont de fait d'intérêt général, puisqu'elles exercent une incidence sur la société telle qu'il est légitime que les choix numériques ne soient pas uniquement du ressort de ces entités qui régulent par exemple la liberté d'expression. A titre d'exemple, concernant la Cour suprême Facebook, qui est amenée à statuer sur certaines censures, y compris de nature algorithmique, il est souhaitable que les associations disposant de cet agrément puissent également y siéger. Il en est de même dans l'acception et l'acceptabilité de la transparence à retenir dans ces domaines.

809. De plus, au même titre que certaines associations sont agrées par l'éducation nationale[1592], ce qui leur permet d'intervenir dans les établissements scolaires pour sensibiliser les élèves sur des thématiques précises, l'agrément association numérique pourrait comprendre des missions de sensibilisation à la culture numérique. En effet, l'enjeu n'est pas aujourd'hui de faire de chaque élève un codeur susceptible de comprendre les traitements mis en œuvre à

[1589] DUTHEIL P-H., *Droit des associations et fondations*, *Dalloz*, 1ere édition, 2016.
[1590] Art. L. 141-3 du Code de l'environnement et R. 141-21 et suivant du même code.
[1591] *Infra*., n° 890 et s.
[1592] En vertu de l'art. D. 551-1 du Code de l'éducation.

son encontre, alors même que certains spécialistes peinent déjà à les étudier, mais de transmettre les clés de compréhension sur ces sujets.

810. Se pose toutefois la question de l'autorité compétente pour la délivrance d'un tel agrément. Un agrément numérique pouvant être octroyé par une sorte de pouvoir préservateur civil permettant de sauvegarder l'action civile[1593] afin d'éviter que les Préfets ou les ministères en charge de la délivrance de ces derniers ne les refusent au titre de leur pouvoir discrétionnaire, alors qu'ils bénéficient tout à la fois du pouvoir réglementaire dans ces domaines, actes susceptibles d'être par ailleurs attaqués en justice. A cette fin, il serait intéressant qu'un tel agrément soit délivré, toujours dans la logique de contre-pouvoir que nous soutenons dans ces travaux, par l'organe étatique incarnant cette société civile, soit par le Conseil économique social et environnemental (CESE), qui est tout à fait à même de reconnaître le travail effectué par ces associations.

811. Les syndicats ne sont pas en reste puisqu'ils jouent un rôle significatif, comme cela peut être le cas par exemple lorsque des algorithmes sont susceptibles de modifier les conditions de travail des salariés[1594]. Ces derniers partagent également avec les associations et autres réseaux des initiatives communes comme la mise en place d'un observatoire des libertés numériques[1595] ou encore la rédaction de portes étroites au Conseil constitutionnel[1596] sur ces thématiques[1597].

812. Enfin, notons que la société civile se nourrit d'initiatives transnationales. C'est par exemple le cas de l'organisation « *Algorithm Watch* » qui œuvre pour une plus grande transparence des traitements[1598]. Certaines initiatives sont quant à elles propres à alerter le consommateur sur les pratiques des acteurs du numérique en analysant par exemple la manière

[1593] Il convient effectivement que cet agrément soit octroyé par un pouvoir préservateur extérieur aux institutions exerçant le pouvoir politique. Sur le modèle de Benjamin Constant, l'objectif est que le pouvoir politique ne puisse annihiler par sa force les initiatives de la société civile.

[1594] Voir en ce sens, TGI de Paris, ordonnance de référé du 13 juin 2017, RG 17/51830. Pour plus d'explications, *Supra.*, n° 360 et s.

[1595] OBSERVATOIRE DES LIBERTES ET DU NUMERIQUE, Création de l'Observatoire des Libertés et du Numérique, *IDH France.org* [en ligne]. 28 janvier 2014. [Consulté le 23 février 2020]. Disponible à l'adresse : https://www.ldh-france.org/Creation-de-l-Observatoire-des/

[1596] « *Stricto sensu, la porte étroite est l'intervention adressée au Conseil et reçue par le greffe, qui est ensuite adressée à l'ensemble des membres.* », PERROUD T., « Le Conseil constitutionnel et les portes étroites », *Blog Jus Politicum* [en ligne]. 16 mars 2017. [Consulté le 6 octobre 2020]. Disponible à l'adresse : https://blog.juspoliticum.com/2017/03/16/le-conseil-constitutionnel-et-les-portes-etroites/

[1597] ADELICO, LDH, SAF et al., Contribution extérieure (dite « porte étroite ») auprès du Conseil Constitutionnel sur la saisine n° 2020-800 DC du 9 mai 2020, p. 26 à 27, *Vox public.org* [en ligne], [Consulté le 1er juin 2020]. Disponible à l'adresse : https://www.voxpublic.org/IMG/pdf/contri_ext_loi_prorog_adelico_saf_sm_ldh.pdf

[1598] Site internet de *Algorithm Watch* [en ligne] [Consulté le 25 novembre 2019]. Disponible à l'adresse : https://algorithmwatch.org/en/

dont chaque application mobile est susceptible de collecter des données à caractère personnel[1599].

B - Les lanceurs d'alerte et sources

813. Au-delà du traditionnel rôle d'alerte dévolu à la presse, et à certaines associations[1600], notamment en matière de fonctionnement des algorithmes, les lanceurs d'alerte[1601] participent au maintien de l'Etat de droit en mettant au jour des faits contraire à l'intérêt général. Ils concourent à une plus grande transparence, raison pour laquelle le Conseil de l'Europe est favorable à la protection de ces donneurs d'alertes, et ce depuis un certain temps, particulièrement afin de « *renforcer la responsabilité et la transparence démocratique* »[1602]. Et il s'agit par ailleurs d'un corolaire à la liberté d'expression[1603], ce qui démontre que certaines autres libertés vont également concourir au principe de transparence. Quant à l'Union européenne, elle considère que tout en jouant un rôle significatif dans la prévention des violations du droit de l'Union et de « *préservation du bien-être de la société* », « *les signalements et les divulgations publiques des lanceurs d'alerte constituent une composante en amont de l'application du droit et des politiques de l'Union* »[1604].

814. Concernant spécifiquement le domaine du numérique, les lanceurs d'alerte sont susceptibles de renseigner sur le fonctionnement et les finalités des traitements algorithmiques, ce que rappelait déjà l'étude annuelle du Conseil d'Etat sur les droits fondamentaux et le

---

[1599] Moteur de recherche du site internet de *Exodus* [en ligne] [Consulté le 25 novembre 2019]. Disponible à l'adresse : https://reports.exodus-privacy.eu.org/fr/

[1600] L'association « *Algotransparency* » effectue par exemple un rôle d'alerte au sujet des recommandations algorithmiques de Youtube lors des périodes électorales. Guillaume Chaslot, fondateur, a décidé pour œuvrer à une meilleure compréhension de ces algorithmes, après avoir été employé par plusieurs géants du numérique. Bien qu'il joue un rôle d'alerte, il ne peut pour autant être considéré juridiquement comme un lanceur d'alerte. Site internet de *Algotransparency* [en ligne] [Consulté le 25 novembre 2019]. Disponible à l'adresse : https://www.algotransparency.org/

[1601] Sociologiquement, l'origine de ce terme émane de CHATEAURAYNAUD F., TORNY D., *Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque*, Éditions de l'École des Hautes Études en Sciences Sociales, 1999. Ce terme recoupe plusieurs sens. Le premier sens *« Toute personne, groupe ou institution qui, percevant les signes précurseurs d'un danger ou d'un risque, interpelle une ou plusieurs puissances d'action, dans le but d'éviter un enchaînement catastrophique, avant qu'il ne soit trop tard. »* tandis que le second sens « *de toute personne ou groupe qui rompt le silence pour signaler, dévoiler ou dénoncer des faits, passés, actuels ou à venir, de nature à violer un cadre légal ou réglementaire ou entrant en conflit avec le bien commun ou l'intérêt général* », CHATEAURAYNAUD F., « Lanceur d'alerte », in CASILLO I., BARBIER R., BLONDIAUX L., CHATEAURAYNAUD F., FOURNIAU J-M., LEFEBVRE R., NEVEU C., et SALLES D. (dir.), *Dictionnaire critique et interdisciplinaire de la participation*, Paris, GIS Démocratie et Participation, 2013 [en ligne] [Consulté le 10 janvier 2020]. Disponible à l'adresse : http://www.dicopart.fr/fr/dico/lanceur-dalerte.

[1602] COUNCIL OF EUROPE, *Protection des lanceurs d'alerte, Recommandation CM/Rec(2014)7 et exposé des motifs*, Instruments juridiques, Council of Europe, p. 14 [en ligne]. Octobre 2014. [Consulté le 2 mars 2020]. Disponible à l'adresse : https://rm.coe.int/16807096c8

[1603] En ce sens, voir notamment CEDH, Grande chambre, Guja c. Moldava, 12 février 2008, req n° 14277/04 ; CEDH, Heinisch c. Allemagne, 21 juillet 2011, req. n° 28274/08.

[1604] Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union.

numérique[1605]. Il s'agit d'un complément aux contrôles que peuvent effectuer les régulateurs publics, ne serait-ce car ils ne peuvent assurer en permanence la conformité de tous les systèmes.

815. En France, de nombreux directeurs d'établissement se sont opposés au fichage d'élèves en ne fournissant pas les données statistiques demandées en vue de modifier la carte scolaire par l'intermédiaire du programme « *Base élèves 1er degré* »[1606]. Cette enquête impliquait notamment de renseigner des données à caractère sensibles telles que l'origine ethnique des élèves, ce qui laissait craindre des finalités tout autre que celles déclarées par le ministère de l'Éducation nationale. Le comité des droits de l'enfant s'est par ailleurs dit « *préoccupé par le fait que cette base de données puisse être utilisée à d'autres fins, telles que la détection de la délinquance et des enfants migrants en situation irrégulière, et par l'insuffisance des dispositions légales propres à prévenir son interconnexion avec les bases de données d'autres administrations* »[1607]. Ce mouvement a ensuite abouti à une modification des critères de collecte de ce traitement informatique[1608], confortant cette objection de conscience.

816. Toutefois, tous les lanceurs d'alerte ne bénéficient pas de la même reconnaissance puisque leur action n'est pas toujours jugée éthique. Par exemple l'affaire Philippe Pichon, ce commandant de la police nationale a révélé les dysfonctionnements et les dérives du « *système de traitement des infractions constatées* » (STIC)[1609] en divulguant à la presse les fiches de Johnny Hallyday et Jamel Debbouze afin de démontrer que la durée de conservation des données était extrêmement longue et pouvait porter préjudice aux intéressés, interprétation ensuite confortée par la CNIL[1610]. La communication de ces informations, qui n'a été cependant rendue possible que par l'intermédiaire de son habilitation à accéder à ce fichier, lui a valu d'être mis à la retraite d'office. Le Conseil d'Etat a par ailleurs validé cette sanction disciplinaire au motif qu'il avait recueilli ces informations en violation des règles d'accès au fichier et à ses obligations de réserve et de discrétion professionnelle. De plus, la

[1605] CONSEIL D'ETAT, *Le numérique et les droits fondamentaux*, *op. cit.*, p. 282 à 283.
[1606] MEKHANTAR J., « L'annulation des retenues effectuées sur le traitement d'un directeur d'école ayant refusé de de renseigner une enquête académique », *AJFP,* 2011, p. 89.
[1607] NATIONS UNIES, CRC, Comité des droits de l'enfant, Examen des rapports soumis par les Etats parties en application de l'article 44 de la convention, p. 12, *Tout sur les droits de l'enfant.fr* [en ligne]. 22 juin 2009 [Consulté le 12 octobre 2019] https://www.toutsurlesdroitsdelenfant.fr/documents/cclfinalescomite2009.pdf
[1608] CE, 19 juillet 2010, req. n° 317182 ; CE, 19 juillet 2010, req. n° 334014 ; Annulation arrêté du 20 octobre 2008 portant création d'un traitement automatisé de données à caractère personnel relatif au pilotage et à la gestion des élèves de l'enseignement du premier degré.
[1609] Le fichier STIC a depuis été remplacé par le fichier de Traitement des Antécédents Judiciaires (TAJ).
[1610] CNIL, Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur, *CNIL.fr* [en ligne] [Consulté le 22 mars 2021]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/typo/document/Rapport_controle_des_fichiers_antecedents_judiciaires_juin_2013.pdf (consulté le 22 mars 2021).

communication des fiches à des tiers non habilités à les consulter et à les publier alors que « *ces faits, connus d'un grand nombre de personnes, avaient déjà été portés à la connaissance de sa hiérarchie et du procureur de la République et étaient l'objet d'un contrôle de la commission nationale informatique et libertés* »[1611], ont semé le doute sur l'intérêt public des révélations[1612]. Le Tribunal correctionnel de Paris[1613] l'a par ailleurs reconnu coupable de violation du secret professionnel au titre de l'article L. 226-13 du code pénal tout en considérant que son geste était motivé partiellement par un intérêt public, ce qui lui a finalement valu une peine légère. Mais il est intéressant de noter que « *pour donner du poids à son alerte, il a sciemment enfreint la loi et pris le risque d'être sanctionné* »[1614].

817. Même si naturellement certaines dénonciations sont parfois motivées par une pluralité de motifs, il convient de juger à l'aune des retombées pour l'intérêt général, surtout lorsque l'administration ne poursuit plus cet objectif qui est pourtant au fondement de sa légitimité. La violation des règles du corps, et donc d'obligations statutaires, peuvent avoir une finalité d'intérêt général et de transparence, ce qui justifie à lui seul un régime juridique propre à la protection des lanceurs d'alerte, qu'ils soient fonctionnaires ou salariés, puisque de nombreux systèmes informatiques utilisés sont opaques et illicites.

818. La problématique des lanceurs d'alerte n'est pas que nationale et concerne également le comportement d'Etats tiers, comme cela est le cas en matière de surveillance des données. En divulguant des preuves sur l'espionnage de nombreuses données personnelles de ressortissants du monde entier par la NSA, y compris par l'intermédiaire des GAFAM, Edward Snowden a, comme d'autres, participé à la compréhension du système de surveillance informatisé américain, ce qui a eu des conséquences majeures, en permettant notamment à la CJUE de motiver l'annulation du « *safe harbor* »[1615]. Il a participé à la sensibilisation de la société, y compris de la justice sur ces questions, et le risque de violation des droits fondamentaux lors des transferts de données en dehors de l'Union Européenne. Ces éléments relatifs au fonctionnement ainsi qu'au comportement des Etats-Unis d'Amérique dans le cadre du numérique permet d'appréhender le positionnement et donc le régime juridique qui leur est applicable.

[1611] CE, 31 mars 2017, req. n° 392316.
[1612] Voir en ce sens, FOEGLE J-P., SLAMA S., Refus de transmission d'une QPC sur la protection des fonctionnaires lanceurs d'alerte, *La Revue des droits de l'homme* [en ligne]. 14 mars 2014 [Consulté le 2 mai 2020]. Disponible à l'adresse : https://journals.openedition.org/revdh/628#quotation ; et DE MONTECLER M-C., « Philippe Pichon, lanceur d'alerte ou indiscret », *AJDA*, 2017, p. 709.
[1613] TGI, Paris, 17e chambre, 22 octobre 2013, Ministère public c/ Pichon.
[1614] LOCHAK D., « L'alerte éthique, entre dénonciation et désobéissance », *AJDA*, 2014, p. 2236.
[1615] CJUE, grande chambre, C-362/14, 6 octobre 2015.

819. Concernant la protection des lanceurs d'alerte, jusqu'à récemment il n'y avait pas de régime juridique unifié entre le droit public[1616] et le droit privé. Il a fallu attendre la loi du 9 décembre 2016 pour que le législateur qualifie le lanceur d'alerte, et ce en vue de lui conférer une protection juridique[1617], de « *personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance.* »[1618].

820. La protection du lanceur d'alerte vise à empêcher qu'il ne soit sanctionné par une mesure discriminatoire, ou fasse l'objet d'un licenciement, voire de poursuites pénales pour des faits dont il a pris connaissance dans le cadre de ses fonctions, mais à la condition d'être de bonne foi[1619] . Néanmoins, cette protection juridique ne s'applique que si des conditions restrictives sont réunies.

821. Une récente directive de l'Union européenne[1620] prévoit depuis un nouveau régime juridique permettant une protection des personnes signalant des violations du droit de l'Union, qu'elles travaillent aussi bien dans le secteur public que privé. Bien que les traitements algorithmiques ne constituent pas une catégorie à part entière, le champ d'application de la directive est suffisamment large pour couvrir de nombreux domaines dans lesquels le numérique a fait son immixtion, même si la loi du 9 décembre 2016 évoque de plus la notion de préjudice grave pour l'intérêt général, ce qui nous semble moins restrictif. Le droit de l'Union européenne a par exemple pour ambition de protéger les lanceurs d'alerte dont les révélations porteraient sur les marchés financiers[1621], la sécurité et la conformité des produits[1622], la protection des consommateurs[1623] ou encore « *protection de la vie privée et des*

[1616] SLAMA S., « Le lanceur d'alerte, une nouvelle figure du droit public ? », *AJDA*, 2014, p. 2229.
[1617] Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat.
[1618] Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, art. 6.
[1619] « *Le salarié ne peut être licencié pour ce motif sauf mauvaise < foi >, laquelle ne peut résulter que de la connaissance par le salarié de la fausseté des faits qu'il dénonce et non de la seule circonstance que les faits dénoncés ne sont pas établis.* », voir en ce sens CAGNAT A., LEFEBVRE A., « Bonne fois du lanceur d'alerte : précisions bienvenues de la chambre sociale », *Légipresse*, 2020, p. 557. Commentaire de l'arrêt de la Cour de cassation, chambre sociale, 8 juillet 2020, req. n° 18-13.593.
[1620] Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union.
[1621] *Ibid*., art. 2 § 1 a) ii).
[1622] *Ibid*., art. 2 § 1 a) iii).
[1623] *Ibid*., art. 2 § 1 a) ix).

données à caractère personnel, et sécurité des réseaux et des systèmes d'information »[1624]. Contrairement au droit français en vigueur, la directive prévoit que la protection juridique est effective même s'il s'agit d'un signalement externe auprès d'une autorité compétente[1625], c'est-à-dire dans l'hypothèse où la personne n'a pas prévenu son supérieur hiérarchique[1626]. De plus, elle semble plus protectrice en ce qu'elle n'exige pas que le donneur d'alerte agisse de manière désintéressée et de bonne foi. En effet, nous considérons qu'il est plus opportun de conférer une protection non pas à l'aune d'un élément moral mais parce que la révélation sert l'intérêt public. Qu'il s'agisse du droit national ou de l'Union européenne, cette protection est notamment exclue si les révélations portent sur la défense nationale[1627]. Il est regrettable de constater qu'un lanceur d'alerte dont le profil est celui d'Edward Snowden ne serait donc pas plus protégé au sein de l'Union. L'autorité de contrôle unique[1628] que nous préconisons pourrait recueillir les informations des lanceurs d'alerte sur la défense nationale comme tiers de confiance et leur accorder une protection.

822. Nous sommes par ailleurs favorables, comme le préconise la CNCDH[1629], à ce que la transposition de cette directive prévoie le statut de demandeur d'asile pour les lanceurs d'alerte étrangers, car c'est un signal qui participe à la transparence de ces systèmes, même lorsque cela a lieu à l'étranger. En effet, les révélations concernant de telles pratiques, aussi bien sur les données à caractère personnel que tout autre traitement algorithmique, est un enjeu transnational. Par conséquent, le principe de transparence implique une telle reconnaissance, et ce d'autant plus que ces informations nous servent à découvrir à la fois le positionnement des autres Etats que celui des opérateurs économiques.

PARAGRAPHE 2 - La société civile institutionnelle

823. Il est question que notre commission unique de contrôle des traitements bénéficie d'importants pouvoirs concernant les algorithmes et les jeux de données *a priori* et *a posteriori*. Mais son action ne peut être suffisante seule. La société civile institutionnelle, c'est-à-dire celle directement structurée par l'Etat, œuvre à lever l'opacité des traitements. Nous retrouvons le

[1624] *Ibid*., art. 2 § 1 a) x).
[1625] *Ibid*., art 11.
[1626] *Ibid*., art. 6.
[1627] *Ibid*., « *Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par le présent chapitre* ».
[1628] *Supra.*, n° 717 et s.
[1629] COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME, avis sur la transposition de la directive relative aux lanceurs d'alerte, 4 octobre 2020.

rôle de la recherche, surtout publique, car instituée dans le sens de l'intérêt général (A). Il est également question de traiter des comités consultatifs institutionnels, ceux créés par le pouvoir politique afin de les éclairer sur les enjeux du numérique et en l'occurrence sur la transparence, dans la mesure où les initiatives purement privées de la société civile ont été abordées précédemment[1630] (B).

A - La recherche scientifique

824. Les enseignants-chercheurs et chercheurs publics jouissent d'une « *pleine indépendance et d'une entière liberté d'expression dans l'exercice de leurs fonctions d'enseignement et de leurs activités de recherche* »[1631]. Ces libertés se caractérisent également par l'autonomie de leur démarche scientifique[1632], car ils œuvrent également dans une dimension collective d'intérêt général[1633]. C'est à ce titre qu'ils sont susceptibles de concourir à la transparence des traitements algorithmiques.

825. Les démarches scientifiques individuelles y contribuent également, comme l'économiste Thomas Piketty, qui a obtenu dans le cadre de ses travaux sur la justice du système fiscal français la communication du code source du logiciel utilisé par l'administration pour calculer l'impôt sur le revenu des personnes physiques, et ce afin de le réutiliser. Dans un premier temps, la Direction générale des finances publiques a refusé la communication de ce document administratif, raison pour laquelle il a été contraint de reconstituer les algorithmes du ministère des finances en fonction des informations qu'il avait en sa possession[1634]. Il a toutefois décidé de saisir la CADA. C'est par l'intermédiaire de cette demande que la CADA a entériné sa doctrine selon laquelle *« les fichiers informatiques constituant le code source sollicité, produits par la direction générale des finances publiques dans le cadre de sa mission de service public, revêtent le caractère de documents administratifs, au sens de l'article 1er de la loi du*

[1630] *Supra*., n° 799 et s.

[1631] Art. L. 952-2 du Code de l'éducation ; Voir également en ce sens CC, décision n° 94-345 DC, 29 juillet 1994, pour la liberté d'expression et de communication dans l'enseignement et la recherche, et CC, décision n° 83-165 DC, 20 janvier 1984, pour PFLR du principe de liberté et de l'indépendance des chercheurs.

[1632] Art. L. 411-3 du Code de la recherche.

[1633] Voir en ce sens, FORTIER C., « La liberté du chercheur public », *in* LARRIEU J. (dir.), *Qu'en est-il du droit de la recherche ?, Presses Universitaires Toulouse 1 Capitole*, 2008, p. 113 à 129 [en ligne] [Consulté le 14 février 2021]. Disponible à l'adresse : https://books.openedition.org/putc/2499

[1634] BOUCHOUX C., Rapport d'information n° 589 refonder le droit à l'information publique à l'heure du numérique : un enjeu citoyen, une opportunité stratégique du Sénat, session ordinaire 2013-2014, fait au nom de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques, enregistré à la Présidence du Sénat le 5 juin 2014, p. 130, in *Senat.fr* [en ligne], 5 juin 2014, [Consulté le 12 mars 2021]. Disponible à l'adresse : http://www.senat.fr/rap/r13-589-1/r13-589-1.html : *« l'économiste Thomas Piketty, pour ses travaux sur la justice du système fiscal français, a été forcé de recréer lui-même un outil de simulation fiscale individuelle faute d'avoir pu avoir accès aux algorithmes du ministère des finances.* ».

17 juillet 1978 »[1635]. Le juge administratif a ensuite retenu cette même position dans d'autres affaires, ce qui a participé à la modification du régime juridique relatif à la transparence des traitements algorithmiques publics par l'intermédiaire de la LRN[1636]. Il est intéressant de noter que cette démarche d'étude des algorithmes de l'administration vise à concourir à un contrôle *a posteriori* des algorithmes, c'est-à-dire après leur mise en œuvre, notamment afin de s'assurer dans le cas présent qu'ils sont bien en conformité avec le droit voté par le Parlement.

826. Le régime juridique actuel demeure complexe pour les chercheurs qui souhaiteraient travailler sur les logiciels et les données de l'administration. En ce sens, la mission Bothorel propose de faciliter l'accès aux données aux chercheurs par des procédures simplifiées, y compris aux données non ouvertes, c'est-à-dire non encore considérés comme des documents administratifs communicables[1637] ou en lien avec le secret statistique[1638].

827. D'une part, il est nécessaire qu'ils puissent travailler sur l'étude des algorithmes existants ainsi que sur les données utilisées, et d'autre part, que les chercheurs développent une alternative publique plus compréhensible que leurs homologues fermés, ce qui ne peut s'opérer que grâce à des financements dédiés et massifs aussi bien en sciences humaines et sociales que dans les domaines des sciences dures.

828. Il est également souhaitable que la recherche scientifique ne travaille pas que sur les algorithmes publics, mais aussi privés, et ce par l'intermédiaire de travaux collectifs. Des initiatives existent déjà comme « *Transalgo* »[1639], plateforme collaborative scientifique française, permettant d'étudier le comportement de ces systèmes. Elle est présentée comme un outil de contrôle, de surveillance, y compris par le développement de logiciels visant à opérer cette fonction. Plusieurs acteurs de la recherche publique française portent ce projet comme

---

[1635] CADA, avis n° 20144578 du 8 janvier 2015.

[1636] TA de Paris, 10 mars 2016, M. X, req. n° 1508951. Pour plus de développements, *Supra.*, n° 426 et s.

[1637] BOTHOREL E., COMBES S., VEDEL R., pour une politique publique de la donnée, mission confiée par le Premier ministre, 23 décembre 2020, spec. p. 121 à 124, *Vie publique.fr* [en ligne], 23 décembre 2020. [Consulté le 23 janvier 2021]. Disponible à l'adresse : https://www.vie-publique.fr/rapport/277879-pour-une-politique-publique-de-la-donnee

[1638] *Ibid*., « *Recommandation n° 30 : Améliorer la prise en charge des demandes des chercheurs, en associant les AMDAC et les SSM (délai de réponse obligatoire, création d'un recours, recours à la consultation du comité du secret statistique à titre facultatif)* ».

[1639] CONSEIL GENERAL DE L'ECONOMIE, Modalités de régulation des algorithmes de traitements de contenus, *Vie publique.fr* [en ligne]. 13 mai 2016 [Consulté le 9 septembre 2020]. Disponible à l'adresse : https://www.vie-publique.fr/sites/default/files/rapport/pdf/273514.pdf. L'initiative « transalgo » émane de la recommandation n° 1 contenue dans le rapport intitulé « *Modalités de régulation des algorithmes de traitements de contenus* », remis à la demande d'Axelle Lemaire, ancienne Secrétaire d'Etat chargée du numérique, le 13 mai 2016. En effet, le projet de loi pour une république numérique de 2016 contenait initialement une disposition permettant aux consommateurs des grandes plateformes de signaler le comportement des algorithmes, mais cette dernière fut retirée par le Sénat. C'est notamment la raison pour laquelle en contrepartie une plateforme collaborative scientifique française de compréhension des systèmes algorithmiques a été proposée. Voir en ce sens, le rapport précité, spec. p. 39 à 41.

l'INRIA[1640] et le CNRS par exemple, mais il est également question d'y faire participer des entités privées. Nous ne sommes pas opposés à ce type de démarche dès lors qu'il s'agit d'un dispositif complémentaire aux règles de transparence de nature étatique. Cet exemple illustre parfaitement que les recherches ayant une telle ambition ne peuvent reposer que sur un écosystème de recherche publique française correctement financé pour nourrir la compréhension de ces nouveaux phénomènes.

829. Comme nous l'avions évoqué, les traitements algorithmiques sont parfois difficiles à appréhender, notamment pour les spécialistes, nécessitant des équipes composées de plusieurs chercheurs. L'affaire du *dieselgate* a mis au jour un programme informatique modifié implanté dans un véhicule automobile afin de faire paraître une conformité aux réglementations européennes et américaines lors des essais d'homologation. Le logiciel était capable de déceler lorsque le véhicule se retrouvait en phase d'évaluation de ses émanations Nox[1641], afin qu'il les réduise par rapport à un usage classique. Il a fallu un an à une équipe de chercheurs de l'Université de Stanford pour reconstituer le code source par rétroingénierie[1642]. C'est aussi pour cette raison que des équipes de chercheurs doivent être dédiées à l'étude sur le long terme des traitements algorithmiques. Nous retrouvons également la dimension transnationale de la recherche qui peut aussi bien servir aux autres Etats dans lesquels sont par exemple commercialisés ces véhicules.

830. Quant à la proposition de Règlement européen relatif à un marché intérieur des services numériques, une place serait laissée aux chercheurs universitaires pour qu'ils étudient les données des grandes plateformes en ligne susceptibles d'exercer un risque systémique sur la société, afin qu'ils étudient la conformité de ces dernières aux nouvelles obligations. Cette mission s'effectuerait en accord avec un coordinateur de l'Etat membre, qui pourrait par ailleurs être notre autorité de contrôle technique centralisant l'expertise en matière d'algorithmes. Ces chercheurs devront néanmoins être indépendant « de tous intérêts commerciaux », et bénéficier d'une expertise dans ce domaine. Enfin, ils devront respecter les impératifs de sécurité de ces systèmes d'information, ainsi que les exigences de confidentialité[1643].

[1640] INRIA, TransAlgo : évaluer la responsabilité et la transparence des systèmes algorithmiques, *INRIA.fr* [en ligne], 4 avril 2018 [Consulté le 19 mars 2020]. Disponible à l'adresse : https://www.inria.fr/fr/transalgo-evaluer-la-responsabilite-et-la-transparence-des-systemes-algorithmiques

[1641] MANDARD S., Cinq ans après le « Dieselgate », les constructeurs bénéficient toujours d'une « clause de confidentialité », *op. cit.*

[1642] CONTAG, M. *et al*., « How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles », *op. cit*., UC SAN DIEGO, Researchers find Computer Code that Volkswagen Used to Cheat Emissions Tests, *op. cit.*

[1643] 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 2000/31CE, art. 31 § 4.

831. Nous proposons de plus une modification du régime juridique pour que les chercheurs bénéficient de causes exonératoires de responsabilité, y compris en matière pénale, lorsqu'ils travaillent sur ces systèmes, justement parce qu'ils remplissent une mission d'intérêt général par la voie du service public de la recherche. Il est essentiel qu'ils puissent jouer un rôle d'alerte. A la différence des lanceurs d'alerte, il est important qu'ils soient présumés de bonne foi dans leur action. C'est effectivement toute la différence entre le hackeur qui agit en dehors de tout cadre et le chercheur qui œuvre dans le cadre d'un projet de recherche. A cet égard, nous souhaitons mettre l'accent sur deux régimes juridiques, à savoir celui de l'introduction dans des systèmes automatisés de données et la décompilation des logiciels.

832. Bien que les pirates informatiques éclairent le numérique sur ses usages et participent parfois à rendre l'environnement plus sûr[1644], leur action doit être strictement encadrée, car il existe également des pratiques malveillantes. C'est la raison pour laquelle ils ne peuvent être qualifiés juridiquement de lanceur d'alerte[1645], même s'ils jouent parfois ce rôle, et que dans le respect du droit leur action est cantonnée au consentement des responsables de traitement pour trouver les failles ou biais des algorithmes lors de certaines opérations[1646]. A titre d'exemple, Serge Humpich a été condamné par le Tribunal correctionnel de Paris[1647] pour contrefaçon de carte bancaire et décompilation du logiciel d'identification d'un terminal de paiement électronique afin de comprendre l'algorithme de chiffrement du système, alors que ses découvertes ont ensuite permis de combler ces vulnérabilités techniques. Il avait en effet démontré qu'il était possible d'effectuer des paiements avec des cartes vierges reprogrammées dans certains terminaux de paiement qui n'interrogeaient pas l'existence des cartes par l'intermédiaire d'un serveur, comme les distributeurs de tickets RATP à l'époque. Même si les juges peuvent reconnaître un intérêt public à ces démarches[1648], ce qui a pour conséquence

[1644] A titre d'exemple, l'article L. 2321-4 du Code de la défense nationale considère que l'obligation prévue à l'article 40 du Code de procédure pénale ne s'applique pas à l'encontre d'une personne de bonne foi qui informe l'ANSII d'une vulnérabilité de sécurité dans un système de traitement automatisé de données. Néanmoins, dans cette hypothèse, l'explication demeure confidentielle. Nous préconisons qu'elle soit transmise à l'autorité de contrôle des algorithmes et non seulement à l'ANSSI, qui décidera le cas échéant, après correction si la vulnérabilité mérite d'être communiquée au public et/ou aux chercheurs. En effet, la publicité est également une manière que les autres acteurs sécurisent leurs systèmes.

[1645] *Supra.*, n° 813 et s.

[1646] Tel est par exemple le cas des événements organisés par les responsables de traitement, dits « prime aux bogues » pour découvrir les failles dans leur système.

[1647] Tribunal correctionnel de Paris, 25 février 2000, Serge H. c/ GIE cartes bancaires.

[1648] Comme l'indique Xavier Delpech, « *On relèvera, en outre, que, dès lors que la démarche se présentait comme scientifique, et était ainsi susceptible de servir l'intérêt général, elle pouvait légitimement être considérée comme un fait justificatif, excluant la responsabilité pénale du prévenu. Pour qu'il en soit ainsi, le trouble social occasionné par le comportement du prévenu, doit avoir une valeur égale, voire moindre, au bénéfice que la société retirerait de cette découverte. La reconnaissance d'un fait justificatif est, en tout état de cause, abandonnée à l'appréciation subjective du juge, chargé en quelques sortes, de mesurer la « balance des intérêts » en présence. En l'occurrence, les magistrats parisiens n'ont reconnu aucun effet bénéfique à la recherche menée, et ont, au contraire, considéré que « cette fraude informatique, par la menace qu'elle fera courir sur l'ensemble des transactions bancaires, a troublé gravement l'ordre public », position, qui, on l'a vu, est loin de faire l'unanimité.* » DELPECH X., « Fraude à la carte bancaire : aspects juridiques », *Recueil Dalloz*, 2000, p. 219.

d'aboutir à une réduction de la peine, il convient de considérer que les chercheurs pourraient bénéficier d'exonérations de responsabilité s'ils développaient des recherches dans ces domaines. Ainsi, nous pourrions imaginer que les infractions pénales prévues aujourd'hui[1649], comme « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* »[1650], ne soient pas sanctionnables pour cette catégorie de personne. Naturellement, cela se ferait sous réserve de certaines garanties comme la non-divulgation de données personnelles dans le cadre de leur étude au même titre qu'actuellement pour les agents des services de l'Etat agissant dans le cadre d'une mission de renseignement extérieure[1651]. De la même manière, le délit de contrefaçon[1652], dès lors qu'il sert l'étude réalisée, c'est-à-dire excluant la revente, ne serait pas applicable. Il serait préférable que la décompilation[1653], qui permet d'accéder au code source d'une application, puisse être ouverte aux universitaires, et ce même lorsqu'ils ne sont pas considérés comme utilisateur du logiciel, ce qui n'empêchera pas le cas échéant les procédures pour parasitisme[1654] si jamais certains chercheurs étaient amenés à se servir ensuite de cette connaissance pour concurrencer d'autres acteurs. La reproduction du code source au-delà de l'exception d'interopérabilité[1655] qu'à des fins de recherche scientifique non lucrative est donc à privilégier. Cette connaissance pourrait ensuite être transmise à notre autorité en charge de la surveillance des traitements algorithmiques.

[1649] Livre III, titre II, chapitre III « des atteintes aux systèmes de traitement automatisé de données » du Code pénal.
[1650] Art. 323-1 du Code pénal.
[1651] Art. 323-8 du Code pénal.
[1652] Voir en ce sens art. L. 335-3 du Code pénal.
[1653] « *La personne ayant le droit d'utiliser le logiciel peut sans l'autorisation de l'auteur observer, étudier ou tester le fonctionnement ou la sécurité de ce logiciel afin de déterminer les idées et principes qui sont à la base de n'importe quel élément du logiciel lorsqu'elle effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du logiciel qu'elle est en droit d'effectuer.* », Art. L. 122-6-1 III du Code de la propriété intellectuelle.
[1654] « *Toutefois, l'ingénierie inverse est soumise à de très nombreuses restrictions, énumérées par la loi. Cela laisse entendre implicitement qu'elle est a priori illicite comme acte de « parasitisme », car elle entraîne la reprise par un tiers des connaissances appliquées d'autrui, voire la création de « logiciels » concurrents* », LE TOURNEAU P., *Contrats du numérique Informatiques et Electroniques 2021/2022*, *Dalloz*, 2020, p. 349.
[1655] La décompilation d'un code source en vue de sa modification à des fins d'interopérabilité est par exemple licite, mais pas pour les autres usages. Voir en ce sens, art. L. 122-6-1 IV du Code de propriété intellectuelle : « *La reproduction du code du logiciel ou la traduction de la forme de ce code n'est pas soumise à l'autorisation de l'auteur lorsque la reproduction ou la traduction au sens du 1° ou du 2° de l'article L. 122-6 est indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels, sous réserve que soient réunies les conditions suivantes :*
1° Ces actes sont accomplis par la personne ayant le droit d'utiliser un exemplaire du logiciel ou pour son compte par une personne habilitée à cette fin ;
2° Les informations nécessaires à l'interopérabilité n'ont pas déjà été rendues facilement et rapidement accessibles aux personnes mentionnées au 1° ci-dessus ;
3° Et ces actes sont limités aux parties du logiciel d'origine nécessaires à cette interopérabilité.
Les informations ainsi obtenues ne peuvent être :
1° Ni utilisées à des fins autres que la réalisation de l'interopérabilité du logiciel créé de façon indépendante ;
2° Ni communiquées à des tiers sauf si cela est nécessaire à l'interopérabilité du logiciel créé de façon indépendante ;
3° Ni utilisées pour la mise au point, la production ou la commercialisation d'un logiciel dont l'expression est substantiellement similaire ou pour tout autre acte portant atteinte au droit d'auteur. »

833. Certaines techniques jugées plus douces comme le « *testing* » peuvent être encouragées[1656] afin de vérifier si les traitements algorithmiques utilisés dans le cadre de procédures du recrutement sont discriminatoires.

834. Les chercheurs jouent également un rôle par la voie de pétitions lorsqu'ils prennent position sur une réforme[1657] ou lorsqu'ils intègrent des groupements aussi bien publics[1658] que privés, parfois pluridisciplinaires et transnationaux, dans lesquels ils vont pouvoir partager leur expertise.

835. Toutes ces initiatives visent à enrichir la connaissance scientifique, mais aussi celle de la société, et ce en vue de débattre aussi bien politiquement que techniquement sur ces thématiques.

B - Les organes consultatifs institutionnels concourant à la transparence

836. Les organes consultatifs ont une origine plurale en la matière puisqu'ils sont parfois l'émanation du pouvoir politique pour mener des réflexions sur certaines thématiques, tandis que dans d'autres hypothèses, ils ont été créés dans le cadre d'une pure initiative privée ou de recherche, ce qui n'exclut pas pour autant une participation à l'intérêt général.

837. Au même titre que la France s'était dotée de nombreuses AAI, dont plusieurs concourent à la transparence des algorithmes[1659], il en est de même pour les comités. Nous ne pourrons donc tous pas les aborder. Le rapport Tricot notait déjà en 1975[1660] que les organes consultatifs pouvaient jouer un rôle de conseil dans des domaines très spécifiques auprès de la future CNIL[1661].

838. Alors même qu'ils ne sont pas considérés comme des régulateurs, certains comités consultatifs ont toutefois le statut d'AAI ou assimilée. Ils se caractérisent par le fait qu'ils ont

[1656] AMER-YAHIA S., MULHEM P., Le testing algorithmique de la discrimination à l'embauche (2), *Binaire*, *Le Monde.fr* [en ligne]. 10 janvier 2020 [Consulté le 5 novembre 2020]. Disponible à l'adresse : https://www.lemonde.fr/blog/binaire/2020/01/10/le-testing-algorithmique-de-la-discrimination-a-lembauche-2/
[1657] Contre la résolution du Parlement européen sur la responsabilité en matière de robotique civile, voir : MULTIPLE, Open Letter to the European Commission Artificial Intelligence and Robotics, *Robotics-Openletter.eu* [en ligne]. [Consulté le 2 mai 2021]. Disponible à l'adresse : http://www.robotics-openletter.eu/
[1658] Le Centre Internet et Société est par un exemple un centre de recherche initié par le CNRS composé majoritairement de chercheurs, mais il également est ouvert à la société civile. Site internet du *Centre Internet et Société* [en ligne] [Consulté le 2 mars 2021]. Disponible à l'adresse : https://cis.cnrs.fr/about/
[1659] *Supra*., n° 703 et s.
[1660] Rapport de la commission informatique et libertés, *La Documentation française*, 1975.
[1661] *Ibid*., p. 75.

été créés dans le but de conseiller le pouvoir politique et la société par leur rôle d'alerte, notamment par l'intermédiaire d'avis. En tant qu'institutions collégiales, elles sont d'ailleurs le plus souvent composées aussi bien de chercheurs que de représentant de la société civile.

839. La CNCDH[1662] *« assure, auprès du Gouvernement, un rôle de conseil et de proposition dans le domaine des droits de l'homme, du droit international humanitaire et de l'action humanitaire.* », et ce en toute indépendance[1663]. C'est donc par l'intermédiaire de son rôle généraliste en matière de droits humains que cette commission est de plus en plus amenée à connaître des enjeux relatifs au numérique, ce qui lui a permis de se prononcer sur la question de la transparence des outils numériques. A titre d'exemple, elle a constaté dans l'un de ses avis relatifs à la proposition de loi visant à lutter contre la haine en ligne que « *c'est au juge, et à lui seul, d'apprécier le caractère abusif de l'exercice de la liberté d'expression* »[1664]. En effet, elle a évoqué sa crainte de voir confier à des acteurs privés, par la voie de traitements algorithmiques la censure de propos tenus sur les réseaux sociaux, tout en précisant que

> « *les opérateurs devraient être en mesure de fournir au régulateur leur mode de fonctionnement et d'en expliquer les « choix » a posteriori. Cette exigence d'explicabilité et d'intelligibilité impliquerait d'étendre également les pouvoirs du régulateur à la possibilité de procéder aux audits des algorithmes utilisés par les plateformes en ligne et d'apprécier les moyens humains mis en œuvre par le régulateur pour contrôler le traitement réservé aux résultats issus des systèmes algorithmiques.* ».

840. Des institutions plus spécialisées ont également été créées par le pouvoir politique afin de faire bénéficier de leur expertise. Tel est par exemple le cas du Comité Consultatif National d'Ethique pour les sciences de la vie et de la santé[1665] (CCNE) qui a pour « *mission de donner des avis sur les problèmes éthiques et les questions de société soulevés par les progrès de la connaissance dans les domaines de la biologie, de la médecine et de la santé.* »[1666]. En tant

[1662] Loi n° 2007-292 du 5 mars 2007 relative à la Commission nationale consultative des droits de l'homme, modifiée.
[1663] *Ibid., art. 1, « Elle est composée de représentants des organisations non gouvernementales spécialisées dans le domaine des droits de l'homme, du droit international humanitaire ou de l'action humanitaire, d'experts siégeant dans les organisations internationales compétentes dans ce même domaine, de personnalités qualifiées, de représentants des principales confédérations syndicales, du Défenseur des droits, ainsi que d'un député, d'un sénateur et d'un membre du Conseil économique, social et environnemental désignés par leurs assemblées respectives.* ».
[1664] CNCDH, Avis relatif à la proposition de loi visant à lutter contre la haine sur internet, 9 juillet 2019.
[1665] Décret n° 83-132 du 23 février 1983 portant création d'un Comité consultatif national d'éthique pour les sciences de la vie et de la santé, depuis abrogé.
[1666] Art. L. 1412-1 du Code de la santé publique.

qu'organe collégial[1667], il est aussi bien composé de personnalités issues du secteur de la recherche que de personnalités qualifiées pour leur « *compétence et de leur intérêt pour les problèmes d'éthique* » ainsi que « *appartenant aux principales familles philosophiques et spirituelles* »[1668]. C'est donc par le truchement du droit de la santé qu'il connait de la transparence des traitements algorithmiques, dans la mesure où les technologies de pointes font leur immixtion dans le domaine médical. Toutefois, depuis sa création, il n'a été amené à se prononcer que cinq fois sur des thématiques spécifiques au numérique, parmi lesquels un rapport[1669] et quatre avis[1670]. Dès 2006, un avis du CCNE évoque l'expérimentation d'outils d'aide à la prise de décision concernant les prescriptions médicales et ses difficultés éthiques, notamment vis-à-vis du patient, nécessitant de fait une exigence de transparence[1671]. Puis, en 2018, lorsque le comité a effectué des propositions concernant la modification de la loi relative à la bioéthique, il a soulevé les nouvelles vulnérabilités induites par le recours aux traitements algorithmiques, dont les techniques d'IA, raison pour laquelle il a proposé, sur le modèle de la LIL, un principe d'information préalable du recours à un traitement par un médecin auprès du patient ou de son représentant légal[1672] afin de recueillir un consentement libre et éclairé[1673]. C'est par un autre avis rendu en 2019 que le CCNE évoquera que l'autonomie de la personne est au fondement des choix individuels, et que « *cette logique exige une loyauté de comportement des responsables du traitement, une transparence de leurs processus, et la possibilité de contrôler leurs possibilités d'accès aux données et leur démarche déontologique* »[1674]. Ainsi, l'avis aboutit sur plusieurs recommandations portant sur l'enjeu des algorithmes telles que le droit à une information compréhensible, précise et loyale[1675] et que les décisions médicales prises sur le fondement d'un traitement algorithmique doivent « *être évalués et validés que par une garantie humaine, condition d'une responsabilisation des*

[1667] Art. L. 1412-2 II du Code de la santé publique. Ses membres sont désignés par le pouvoir politique. A l'exception de son Président, nommé pour une durée de deux ans renouvelables, leur mandat étant de quatre ans renouvelables.
[1668] Art. L. 1412-2 I du Code de la santé publique.
[1669] CCNE, Rapport du groupe de travail commandé par le comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE) avec le concours de la commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene (CERNA), CCNE-ethique.fr [en ligne]. 19 novembre 2018 [Consulté le 1er mars 2019]. Disponible à l'adresse : https://www.ccne-ethique.fr/fr/publications/numerique-sante-quels-enjeux-ethiques-pour-quelles-regulations
[1670] Voir en ce sens, avis 91, 104, 129 et 130.
[1671] CCNE, Avis 91 sur les problèmes éthiques posés par l'informatisation de la prescription hospitalière et du dossier du patient, p. 7, CCNE-ethique.fr [en ligne] [Consulté le 18 avril 2021]. Disponible à l'adresse : https://www.ccne-ethique.fr/sites/default/files/publications/avis091.pdf
[1672] CCNE, Avis 129. Contribution du comité consultatif national d'éthique à la révision de la loi de bioéthique, p. 103, CCNE-ethique.fr [en ligne], 2018 [Consulté le 18 avril 2021]. Disponible à l'adresse : https://www.ccne-ethique.fr/sites/default/files/avis_129_vf.pdf
[1673] Pour plus de précisions au sujet de la loi bioéthique, *Supra.*, n° 381 et s.
[1674] CCNE, Avis 130. Données massives et santé : une nouvelle approche des enjeux éthiques, p. 7, *CCNE-ethique.fr* [en ligne]. 29 mai 2019 [Consulté le 3 avril 2021]. Disponible à l'adresse : https://www.ccne-ethique.fr/sites/default/files/publications/avis_130.pdf
[1675] *Ibid*., Recommandation 1.

acteurs », et que cette mission doit être opérée par une instance de contrôle[1676], ce qui nourrira les débats relatifs à l'article 11 du projet de loi bioéthique[1677]. Toutefois, de nombreux commentateurs considèrent que la production scientifique de cette instance est insuffisante au regard des nouveaux enjeux, dont fait partie prenante le numérique, notamment car son champ de compétence, qui a été établi par le législateur, est considéré comme trop restreint pour qu'il s'approprie ces thématiques[1678]. Sa production a par ailleurs été jugée inférieure à celle de l'Office parlementaire d'évaluation des choix scientifiques et technologiques[1679], qui n'a pourtant pas le même rôle institutionnel et n'est pas composé d'experts, mais de parlementaires. Sous l'impulsion du rapport Villani[1680], le CCNE a repris l'idée en se proposant « *de jouer un rôle d'aide à la constitution d'un futur comité d'éthique du numérique, spécialiste des enjeux numériques dans leur globalité* »[1681], ce qui fut ensuite accepté par le Premier Ministre[1682]. Cette instance n'est pour l'heure qu'un comité national pilote d'éthique du numérique (CNPEN)[1683] et n'a pas encore assuré sa pérennité puisqu'il est d'abord question qu'il rende des travaux sur certaines thématiques comme les voitures autonomes, les agents conversationnels et le diagnostic médical mené par l'IA courant 2021. Il publie toutefois des contributions comme lorsqu'il a été amené à collaborer sur le livre blanc de l'IA de la Commission européenne dans lequel il s'est prononcé en faveur d'une plus grande explicabilité et transparence de ces technologies[1684].

841. Pourtant, en 2011, un Conseil National du Numérique (CNN) [1685] avait été institué pour conseiller le gouvernement « *sur tout projet de disposition législative ou réglementaire susceptible d'avoir un impact sur l'économie numérique* »[1686]. Il était également question qu'il

[1676] *Ibid*., Recommandation 4.
[1677] ASSEMBLEE NATIONALE, Projet de loi n° 3833, modifié par le Sénat, en deuxième lecture, relatif à la bioéthique, art. 11, *Assemblée nationale.fr* [en ligne], [Consulté le 3 avril 2021]. Disponible à l'adresse : https://www.assemblee-nationale.fr/dyn/15/textes/l15b3833_projet-loi#D_Article_11
[1678] BEVIERE-BOYER B., « Révolution technoscientifique d'amélioration : quelle éthique pour quelle humanité ? », *in* MARTINENT E., STANTON J., MAMZER M-F. (dir.), *Réflexion et recherche en éthique, Mélange en honneur du professeur Christian Hervé*, *Dalloz*, 2018, p. 304.
[1679] Loi n°83-609 du 8 juillet 1983 portant création d'une délégation parlementaire dénommée office parlementaire d'évaluation des choix scientifiques et technologiques.
[1680] VILLIANI C., SCHOENAUER M., BONNET Y., et *al.*, Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne, *op. cit.*
[1681] CCNE, Avis 129. Contribution du comité consultatif national d'éthique à la révision de la loi de bioéthique, *op. cit.*, p. 158.
[1682] CCNE, Création du comité pilote d'éthique du numérique, *CCNE-éthique.fr* [en ligne]. 2 décembre 2019 [Consulté le 16 juin 2020]. Disponible à l'adresse : https://www.ccne-ethique.fr/sites/default/files/communique_lancement_comite_numerique.pdf
[1683] Ce comité est composé de plusieurs spécialistes du numérique dans une approche disciplinaire ainsi que des membres de la société civile.
[1684] CCNE, Consultation sur le Livre blanc sur l'intelligence artificielle. Une approche européenne, *CCNE-éthique.fr* [en ligne] [Consulté le 19 mars 2021]. Disponible à l'adresse : https://www.ccne-ethique.fr/sites/default/files/publications/cpen-contribution-consultation-ia4eu-2020-06-14.pdf
[1685] Décret n° 2011-476 du 29 avril 2011 portant création du Conseil national du numérique.
[1686] *Ibid.*, art. 1.

formule des recommandations en faveur du développement économique de la France dans le secteur du numérique[1687]. Il remplissait donc une mission purement en lien avec l'économie. Malgré un élargissement de son champ d'intervention[1688], la dimension relative aux droits des libertés demeure toujours en retrait par rapport à la dimension économique[1689], ce qui est par ailleurs une tendance actuelle puisque le Premier Ministre a préféré réduire les enjeux du numérique à cette question en instituant un secrétariat d'Etat chargé de la transition numérique et des communications électroniques rattaché au Ministre de l'économie[1690], laissant présager une difficile place pour penser le droit des libertés dans l'environnement numérique. Le CNN est désormais composé de deux députés et sénateurs désignés par les assemblées[1691], en plus des dix-sept personnalités de la société civile nommées par le Premier Ministre sur proposition du ministre chargé du numérique pour leur action et leurs compétences dans le domaine du numérique[1692]. Il convient toutefois de noter que ce conseil a proposé en 2016 un projet d'agence de notation des plateformes numériques, notamment dans le but d'étudier le comportement des algorithmes[1693]. Ainsi, ce dispositif est considéré comme « *une approche pragmatique et complémentaire des dispositifs existants* »[1694]. Cette proposition d'agence fait suite à ses recommandations en matière de transparence des plateformes numériques ayant précédé la LRN de 2016[1695].

842. Dans le cadre de l'urgence sanitaire, il a évoqué la thématique de la transparence des systèmes d'information puisqu'il a été saisi par le secrétaire d'Etat chargé du numérique[1696] sur la mise en œuvre et le fonctionnement de l'application « *StopCovid* » le 17 avril 2020[1697]. Il est par ailleurs regrettable que la CNIL n'ait été saisie que le 20 avril 2020, ce qui laisse à penser

---

[1687] *Ibid*.
[1688] Décret n° 2017-1677 du 8 décembre 2017 relatif au Conseil national du numérique.
[1689] « *Le Conseil national du numérique est chargé d'étudier les questions relatives au numérique, en particulier les enjeux et les perspectives de la transition numérique de la société, de l'économie, des organisations, de l'action publique et des territoires* », Décret n° 2017-1677 du 8 décembre 2017 relatif au Conseil national du numérique modifiée par le décret n° 2021-154 du 13 février 2021, art. 1.
[1690] Décret n° 2020-1045 du 14 août 2020 relatif aux attributions du secrétaire d'État auprès du ministre de l'économie, des finances et de la relance et de la ministre de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques.
[1691] *Ibid*., art. 2.
[1692] *Ibid*., art. 3.
[1693] LEMAIRE A., Lettre de mission CNNum au Président du Conseil national du numérique, *Economie.gouv.fr* [en ligne] 8 décembre 2016 [Consulté le 26 janvier 2021]. Disponible à l'adresse : https://www.economie.gouv.fr/files/files/PDF/Lettre_de_mission_CNNum.pdf
[1694] *Ibid.*, p. 3.
[1695] CONSEIL NATIONAL DU NUMERIQUE, Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouverte et soutenable, *CNNumérique.fr* [en ligne]. Mai 2014 [Consulté le 10 juin 2020]. Disponible à l'adresse : https://cnnumerique.fr/files/2017-09/CNNum_Rapport_Neutralite_des_plateformes.pdf
[1696] Dénomination qui précède le remaniement de l'été 2020.
[1697] CONSEIL NATIONAL DU NUMERIQUE, *Avis relatif à l'application Stopcovid en date du 24 avril 2020 après saisine du 14 avril 2020* [en ligne] [Consulté le 10 juin 2020]. Disponible à l'adresse : https://cnnumerique.fr/files/uploads/2020/2020.04.17_Saisine_Stop_Covid.pdf

que le régulateur historique a été rétrogradé par rapport au CNN. Ce dernier s'est prononcé en faveur d'une transparence de l'application tels que la publication du « *code source de l'application et des systèmes associés ainsi que leur documentation sous des licences libres et des éléments de vulgarisation* »[1698] et l'explicabilité « *du processus déterminant lorsqu'un contact est à risque* »[1699]. Mais cela ne peut être suffisant, et la transparence ne saurait justifier tous les usages. Contrairement au CNN, la CNIL a demandé une analyse d'impact relative à la protection des données. Concernant le CNCDH, elle s'est finalement auto-saisie « *pour alerter les pouvoirs publics sur les dangers pour les droits fondamentaux de toute application de suivi de personnes et des contacts, en particulier sur le droit à la vie privée* », notamment car elle y voit un risque d'effet cliquet[1700]. Le CCNE n'a quant à lui rendu qu'un avis le 13 mars 2020 après saisine du ministre de la Santé, soit avant l'adoption de l'urgence sanitaire, mais il n'existait pas encore à cette date de volonté politique de mettre en œuvre des dispositifs sanitaires numériques. C'est ensuite le Conseil scientifique[1701] et le CNPEN[1702] qui se sont essentiellement substitués à lui sur ces questions.

843. Même si les comités consultatifs semblent en apparence constituer une richesse, aussi bien par leur qualité technique que par l'organisation de débats publics[1703], ils nourrissent tout au plus la société civile. En effet, les incidences de cette *soft law* sur l'exercice du pouvoir politique est en revanche à nuancer. En effet, au même titre qu'il existe aujourd'hui une pluralité de régulateurs entrant dans le champ d'application des traitements algorithmiques, et donc de

[1698] *Ibid*., recommandation 5.
[1699] *Ibid*., recommandation 6.
[1700] COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME, Avis sur le suivi numérique des personnes, *CNCDE.fr* [en ligne], 28 avril 2020 [Consulté le 2 novembre 2020]. Disponible à l'adresse : https://www.cncdh.fr/fr/actualite/avis-sur-le-suivi-numerique-des-personnes ; COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME, La CNCDH souligne les dangers de l'application *StopCovid*, in *CNCDE.fr* [en ligne]. 26 mai 2020 [Consulté le 2 novembre 2020]. Disponible à l'adresse : https://www.cncdh.fr/fr/publications/la-cncdh-souligne-les-dangers-de-lapplication-stopcovid
[1701] Loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, art. 2.
[1702] Le CNPEN a cependant rendu plusieurs avis sous forme de veille lors de la pandémie de la covid-19. L'un porte sur l'utilisation des outils numériques lors du confinement, tandis que l'autre aborde le recours à ces outils en période de déconfinement. Les deux réflexions font état de la nécessité de transparence de ces outils sans pour autant les remettre en cause. Voir en ce sens, CCNE, Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë, *CCNE-éthique.fr* [en ligne]. 7 avril 2020 [Consulté le 22 janvier 2020]. Disponible à l'adresse : https://www.ccne-ethique.fr/sites/default/files/publications/bulletin-1-ethique-du-numerique-covid19-2020-04-07.pdf ; CCNE, CNPEN Enjeux d'éthique concernant des outils numériques pour le déconfinement, *CCNE-éthique.fr* [en ligne]. 14 mai 2020 [Consulté le 22 janvier 2021]. Disponible à l'adresse : https://www.ccne-ethique.fr/fr/actualites/cnpen-enjeux-dethique-concernant-des-outils-numeriques-pour-le-deconfinement. Ce comité a également évoqué la transparence des traitements algorithmiques dans les recommandations relatives aux fausses informations dans le cadre de la crise sanitaire : CCNE, Enjeux d'éthique dans la lutte contre la désinformation et la mésinformation, in *CCNE-éthique.fr* [en ligne]. 21 juillet 2020 [Consulté le 22 janvier 2021]. Disponible à l'adresse : https://www.ccne-ethique.fr/sites/default/files/cnpen-desinformation-v2020-10-01.pdf. La dernière veille en date évoque une vigilance particulière quant à la transparence des outils d'aide au diagnostic utilisé dans le cadre de la médecine et du télésoin utilisé lors de la pandémie : CCNE, Enjeux d'éthique liés aux outils numériques en télémédecine et télésoin dans le contexte de la COVID-19, *CCNE-éthique.fr* [en ligne]. 21 juillet 2020 [Consulté le 22 janvier 2021]. Disponible à l'adresse : https://www.ccne-ethique.fr/sites/default/files/cnpen-bulletin-telemedecine-2021-01-04.pdf
[1703] Au-delà de leur rôle de conseil auprès des gouvernants, ils organisent également des débats publics. Voir en ce sens, L. 1412-6 du Code de la santé publique pour le CCNE.

leur transparence, ces comités institutionnels collégiaux perdent également en visibilité. Pire, le pouvoir politique les confronte entre eux, voire parfois à des régulateurs historiques comme ce fut le cas dans le cadre de l'urgence sanitaire. En sollicitant une pluralité d'avis auprès d'instance de personnalités présupposées qualifiées, il finit forcément par y trouver les arguments pour légitimer ses décisions politiques. Il ne peut donc s'agir d'un véritable contre-pouvoir de la société civile, raison pour laquelle il conviendra d'évoquer plus tardivement un principe de participation en matière de recours aux algorithmes[1704].

SECTION II - LE RENFORCEMENT DU CADRE ETHIQUE ET DEONTOLOGIQUE DES PROFESSIONNELS

844. Comme nous l'avons vu, le rôle des corps intermédiaires et des comités institutionnels est à encourager. Mais pour s'assurer de l'effectivité du principe de transparence, il convient d'agir au plus près des acteurs concevant et mettant en œuvre ces traitements algorithmiques. Certes, il serait déraisonnable de considérer qu'aucun effort n'a été entrepris par ces derniers dans la mesure où certaines initiatives ont démontré une volonté de penser l'éthique afin d'éclairer sur leur fonctionnement.

845. L'éthique est soumise à des aléas du point de vue de son contenu et ne demeure qu'un outil informel de régulation ou d'autorégulation lorsqu'elle est pensée en dehors de tout cadre juridique. Elle ne peut donc être considérée comme une garantie juridique à la différence de la déontologie (Paragraphe 1). En effet, il n'est pas concevable que le respect d'une prétendue éthique exonérerait du droit. Il est donc impératif que l'éthique se mue en déontologie, c'est-à-dire en obligation pour les professionnels. Mais les acteurs participant à la conception de ces programmes peuvent être si nombreux, et aux provenances diverses, qu'il est difficile d'obtenir d'eux l'application de règles déontologiques précises. C'est la raison pour laquelle, tout en nous prononçant en faveur d'une extension des missions du DPD, une nouvelle profession soumise à des règles déontologiques particulières, dont le rôle portera notamment sur la transparence est souhaitée (Paragraphe 2).

[1704] *Infra*., n° 986 et s.

PARAGRAPHE 1 – DE L'ETHIQUE A LA DEONTOLOGIE DES ACTEURS DES TRAITEMENTS ALGORITHMIQUES

846. La difficulté de mise en œuvre d'un principe de transparence, lorsque la réglementation le prévoit déjà, repose essentiellement par l'adoption d'un droit souple dépourvu d'effets contraignants. L'éthique s'est imposée ces dernières années comme un instrument aussi bien d'autorégulation que de corégulation. Il n'est toutefois pas suffisant et s'est souvent substitué au droit dur, marquant l'échec de la régulation par la norme informelle (A). Enfin, afin de pallier cette insuffisance, le principe de transparence implique un recours à la déontologie (B).

A - L'éthique des algorithmes : l'échec de la régulation par la norme informelle

847. La question éthique des nouvelles technologies n'est pas une thématique nouvelle tant de nombreux philosophes y ont consacré leurs travaux[1705]. Les enjeux spécifiques du numérique ont émergé dès l'après Seconde Guerre mondiale lors de l'avènement de l'ordinateur lorsqu'il est aussi bien apparu comme vecteur de progrès que d'inquiétude[1706], posant nécessairement la question de l'éthique des chercheurs et ingénieurs développant et mettent en œuvre ces nouveaux outils. La problématique éthique est de plus en plus posée à une époque où les algorithmes auto-apprenants font leur immixtion dans de nombreux domaines comme en matière de robotique avec les robots létaux autonomes[1707], ou encore de décisions ayant des conséquences juridiques sur les personnes et la société, et dont l'explication de leur fonctionnement échappe en partie à leur créateur, rendant par ailleurs difficile leur acceptabilité.

848. Mais il convient de lever dès à présent la distinction entre l'éthique et la déontologie. Ainsi, « *l'éthique ou la science de la morale correspond à la recherche d'une manière d'être, à la sagesse dans l'action. L'éthique est personnelle. Elle est d'ordre facultatif, relève de l'autonomie de la volonté, elle exprime une recherche permanente alors que la déontologie est fixée et obligatoire et fait partie de ce que l'on adopte nécessairement en choisissant un métier* »[1708].

849. Dès lors, il est important de noter que la déontologie, à la différence de l'éthique, est une technique juridique permettant dans un cas précis d'obtenir une réponse déterminée de la

[1705] Voir par exemple, POMMIER E., « Ethique et politique chez Hans Jonas et Hannah Arendt », *Revue de métaphysique et de morale*, 2013/2, n° 78, p. 271 à 286.
[1706] Voir en ce sens, WIENER N., *La cybernétique, information et régulation dans le vivant et la machine, op. cit*.
[1707] NEVEJANS N., « La légalité des robots de guerre dans les conflits internationaux », *Recueil Dalloz.* 2016, p. 1273.
[1708] VIGOUROUX C., *Déontologies des fonctions publiques*, *op. cit.*, p. 11.

part d'un professionnel. A défaut, tout comportement inverse à cette situation pourrait être sanctionné. Mais faut-il encore que cette situation ait été anticipée, discutée, adoptée, puis intégrée dans une norme.

850. L'éthique peut toutefois être considérée comme l'« antichambre » de la déontologie. Ainsi, la nature et le degré de la transparence ne peuvent qu'être variables. L'éthique est toutefois un élément qui permet de penser les enjeux. Cantonner la régulation du numérique à la question éthique emporte selon nous deux conséquences. D'une part, cela consisterait à reconnaître que le numérique pourrait être régulé autrement que par du droit dur, et d'autre part, il s'agirait d'alimenter le mythe selon lequel l'éthique serait universaliste, c'est-à-dire qu'elle serait identique d'une entreprise à l'autre, voire d'un Etat à l'autre, ce qui n'est guère le cas. En effet, l'éthique a cette particularité d'être fluctuante. Il est évident que l'éthique est moins présente au cœur de la *Silicon Valley*[1709] où l'intérêt économique et les expérimentations priment sur un éventuel principe de précaution, et sur les exigences d'explicabilité auprès des utilisateurs, ne serait-ce car cela pourrait remettre en cause le secret industriel de ces algorithmes ainsi que leur politique commerciale. Par ailleurs, la concurrence, dans un domaine aussi compétitif, ne plaide pas en faveur de l'émergence d'une éthique uniforme.

851. Qu'elle soit d'origine étatique ou privée, il existe pourtant des tentatives d'instauration d'une éthique, mais ces textes n'ont aucune valeur contraignante. En l'occurrence, cela concerne surtout l'IA, c'est-à-dire les algorithmes auto-apprenants, dans le cadre duquel les organismes privés ont élaboré des chartes éthiques, à des fins d'autorégulation. Ces algorithmes sont réputés opaques et offrent également des possibilités bien supérieures aux algorithmes déterministes.

852. Ainsi, de nombreux acteurs privés du numérique ont adopté une telle charte contenant notamment un principe de transparence de l'IA. Concernant les GAFAM[1710], tel est par exemple le cas de Microsoft[1711]. Les BATX[1712] ne sont pas en reste comme le montre l'initiative de

[1709] SADIN E., *La Silicolonisation du monde, l'irrésistible expansion du libéralisme*, *L'échappée*, 2016, 291 p.
[1710] GAFAM est le sigle des géants du numérique ayant été créés aux Etats-Unis d'Amérique. Il s'agit en l'occurrence de Google, Amazon, Facebook, Apple et Microsoft.
[1711] Selon Microsoft, les systèmes d'IA doivent être transparents, c'est-à-dire compréhensibles. C'est la raison pour laquelle l'entreprise s'engage à appliquer ces principes à travers le « Bureau de l'IA responsable (ORA) et du comité AETHER (IA et éthique de l'ingénierie et de la recherche) ». MICROSOFT, IA responsable, *Microsoft.com* [en ligne] [Consulté le 12 mars 2021]. Disponible à l'adresse : https://www.microsoft.com/fr-fr/ai/responsible-ai?activetab=pivot1:primaryr6
[1712] Par juxtaposition avec les géants américains, le sigle BATX évoque les géants du numérique Chinois. Il s'agit de Baidu, Alibaba, Tencent et Xiaomi.

Tencent[1713]. Il existe un relatif consensus sur le principe de transparence bien que le degré et la nature de celui-ci diffèrent en fonction de l'entité[1714]. D'autres acteurs, comme Orange, travaillent actuellement à l'élaboration d'une telle charte afin d'appliquer les principes déjà retenus par des groupes de travail[1715], sans doute pour répandre l'idée d'une traçabilité de l'IA, figurant déjà dans leurs engagements précédents[1716]. Toutefois, ces initiatives intéressantes ne doivent pas laisser penser que l'éthique se suffirait à elle-même, et ne nécessiterait pas un cadre juridique pour réguler ces acteurs. En effet, il est parfois difficile de s'assurer que les acteurs ayant édictés ces principes les appliquent en pratique et qu'il ne s'agit pas d'une méthode de communication, et en l'occurrence de « *transparency-washing* »[1717]. C'est d'ailleurs la raison pour laquelle, à la suite d'un livre blanc sur les enjeux de l'IA[1718], la Commission européenne envisage désormais une réglementation générale sur ces sujets dans un but de protection des droits fondamentaux et non plus par le truchement des données personnelles uniquement,

[1713] TENCENT RESEARCH INSTITUTE, « ARCC » : An Ethical Framework for Artificial Intelligence, principe n° 3, *Tisi.org* [en ligne]. 09 avril 2020 [Consulté le 16 avril 2021]. Disponible à l'adresse : https://www.tisi.org/13747 : « **Principle III: AI should be comprehensible. "Black-box" technology :** Promote algorithmic transparency and algorithmic audit, to achieve understandable and explainable AI systems. **Differential transparency** : Different entity needs different transparency and information, and intellectual property, technical feature, and technical literacy should also be considered**. Explanation rather than technological transparency** :Provide explanation in respect of decisions assisted/made by AI systems where appropriate**. Public engagement and exercise of individuals' rights**: Various ways of engagement: user feedback, user choice, user control, etc.; use the capabilities of AI systems to foster an equal empowerment and enhance public engagement**.** Respect individuals' rights, such as data privacy, expression and information freedom, non-discrimination, etc.; challenge decisions assisted/made by AI systems; provide relief for victims in respect of AI-caused harms**. Informational self-determination** : Ensure individuals' right to know, and provide users with sufficient information concerning AI system's purpose, function, limitation, and impact ». Nous traduisons « **Principe III : l'IA doit être compréhensible**. **Technologie boîte noire** : promouvoir la transparence algorithmique et l'audit algorithmique pour obtenir des systèmes d'IA compréhensibles et explicables. **Transparence différentielle** : chaque entité a besoin d'une transparence et d'informations différentes. La propriété intellectuelle, les caractéristiques techniques et les connaissances techniques doivent également être prises en compte. **Explication plutôt que transparence technologique** : fournir des explications sur les décisions fondées ou automatisées par un système d'IA le cas échéant. **Engagements publics et exercice des droits des personnes** : diverses formes d'engagement telles qu'un retour d'information utilisateur, choix de l'utilisateur, contrôle de l'utilisateur notamment ; recourir aux systèmes d'IA pour favoriser une responsabilisation égale et renforcer l'engagement du public. Respecter les droits des personnes tels que la confidentialité des données, la liberté d'expression et d'information, la non-discrimination etc ; Contester les décisions prises fondées sur un d'outil d'aide à la prise de décision ; accorder une aide aux victimes de préjudices causés par l'IA. **Autodétermination informationnelle** : garantir le droit des individus de savoir et fournir aux utilisateurs des informations suffisantes concernant la finalité, la fonction, les limites et l'impact des systèmes d'IA ».

[1714] FJELD J, ACHTEN N, HILLIGOSS H, NAGY A, SRIKUMAR M., *Principled Artifical Intelligence : Mapping Consensus in Ethical and Rights-Based Approches to Principles for AI*, *op. cit.* ; DECLARATION DE MONTREAL IA RESPONSABLE, La déclaration de Montréal pour un développement responsable de l'intelligence artificielle, *Declaration Montreal IA Responsable.com* [en ligne] [Consulté le 12 décembre 2020]. Disponible à l'adresse : https://www.declarationmontreal-iaresponsable.com/la-declaration

[1715] ORANGE, Orange crée un Conseil d'éthique de la Data et de l'IA, *Orange.com* [en ligne]. 23 mars 2021 [Consulté le 3 avril 2021]. Disponible à l'adresse : https://www.orange.com/fr/newsroom/communiques/2021/orange-cree-un-conseil-dethique-de-la-data-et-de-lia

[1716] ARBORUS, ORANGE, Charte internationale pour une I.A inclusive, *Charteia.arborus.org* [en ligne] [Consulté le 3 avril 2021]. Disponible à l'adresse : https://charteia.arborus.org/

[1717] Voir en ce sens, ZALNIERIUTE M., « « Transparency-Washing » In The Digital Age : A Corporate Agenda of Procedural Fetishism », *Critical Analysis of Law*, UNSW Law Research Paper, 8(1), 2021, p. 21 à 33. Selon l'auteure, les initiatives éthiques des géants du numérique en matière de transparence n'ont pas d'autres missions que d'empêcher l'adoption d'une réglementation par les régulateurs et/ou les Etats.

[1718] COMMISSION EUROPEENNE, Livre blanc. Intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance, *op. cit.* ; COMMISSION EUROPEENNE, Ethics guidelines for trustworthy AI, *Digital-strategy.ec.europe.eu* [en ligne]. 8 mars 2021 [Consulté le 15 avril 2021]. Disponible à l'adresse : https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Ce livre blanc fait suite à des lignes directrices « *en matière d'éthique pour une IA digne de confiance* » émanant d'un groupe d'experts constitué par la Commission, en date du 8 novembre 2019.

notamment afin de promouvoir une IA plus transparente[1719]. Les réflexions éthiques mènent donc à des régimes juridiques, ce qui est par ailleurs tout à fait logique et habituel pour répondre à un nouveau fait juridique.

853. Les Etats et les organisations internationales ont également une part de responsabilité dans l'échec de la corégulation par la norme informelle. Le plus souvent, lorsque l'Etat tente de s'immiscer dans ce domaine, il le fait par la voie de l'incitation comme c'est par exemple le cas en Australie. Le gouvernement australien, dans cette approche incitative, a publié une charte éthique à destination des industriels en matière d'IA, comprenant des dispositions relatives à un principe de « *transparence et à l'explicabilité* » des traitements[1720]. Toutefois, il est précisé qu'il ne s'agit que de principes volontaires[1721]. Il en est de même lorsque le Conseil de l'Europe adopte, à destination des concepteurs et des Etats, sa première charte éthique relative à l'utilisation de l'IA dans le domaine judiciaire[1722].

854. Ces initiatives ne sont pas à rejeter, car elles ont tout de même pour ambition de penser et poser les jalons d'un droit nouveau, mais force est de constater que ce droit non contraignant ne participe que très marginalement à l'effectivité du principe de transparence. Ainsi, « *le recours à l'éthique est privilégié ainsi que la responsabilité sociétale des entreprises, mais cette « soft law » n'exclut pas le recours au droit dur* » comme le note certains auteurs[1723]. La multiplication de ces chartes laisse d'ailleurs à penser que les acteurs ne souhaitent pas s'engager dans une démarche plus performative, insinuant dans le reste de la société que l'éthique est la seule solution aux problématiques de numérique et de transparence[1724].

[1719] Proposition n° 2021/0106 (COD) 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, du 21 avril 2021.

[1720] AUSTRALIAN GOVERNMENT, DEPARTMENT OF INDUSTRY, SCIENCE, ENERGY AND RESOURCES, Al Ethics Principles, *Industry.gov.au* [en ligne] [Consulté le 22 mars 2021]. Disponible à l'adresse : https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles

[1721] *Ibid.*

[1722] COMMISSION EUROPEENNE, Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, *RM.Coe.int* [en ligne]. Décembre 2018 [Consulté le 22 mars 2021]. Disponible à l'adresse : https://rm.coe.int/charte-ethique-fr-pour-publication-4-decembre-2018/16808f699b : « *Principe de transparence, de neutralité et d'intégrité intellectuelle : rendre accessibles et compréhensibles les méthodologies de traitement des données, autoriser les audits externes* », et cela sans indiquer par ailleurs la nature et le degré de la conciliation souhaité avec d'autres droits et libertés comme le secret industriel, p. 11.

[1723] BLIN-FRANCHOMME M-P., « Le défi d'une IA inclusive et responsable », *Droit social*, 2021, p. 100.

[1724] « *Sans attendre ces potentielles évolutions juridiques, les médias, mais aussi les décideurs publics, ne devraient donc pas se laisser distraire par « ces éthiques » et croire qu'elles apportent des réponses suffisantes aux effets systémiques et invasifs de l'IA sur notre société* », MENECEUR Y., « Les enseignements des éthiques européennes de l'intelligence artificielle », *La semaine juridique*, n° 12, 25 mars 2019, spec. p. 558 ; Voir également MENECEUR Y., L'éthique, insuffisante à réguler seule les technologies numérique et l'intelligence artificielle, *Blog Le temps électrique* [en ligne]. 7 mai 2020 [Consulté le 2 mars 2021]. Disponible à l'adresse : https://lestempselectriques.net/index.php/2020/05/07/linsuffisance-de-lethique-a-reguler-lintelligence-artificielle/

855. La contractualisation entre ces différents acteurs, voire par l'intermédiaire des conditions générales d'utilisation avec le consommateur, pourraient être un outil intéressant pour intégrer des principes éthiques qui n'ont pas valeur de loi, ce qui permettrait de leur faire revêtir une force contraignante. Néanmoins, elle doit s'inscrire dans la conformité avec le droit, et ne peut pas être une occasion supplémentaire de faire entrer dans le droit contractuel tout autre principe alternatif à l'intérêt général public[1725].

856. Mais il convient de considérer que les acteurs concernés par ces obligations de transparence n'ont qu'un intérêt limité à les appliquer tant il existe une culture économique du secret. C'est la raison pour laquelle nous souhaitons l'adoption d'un droit dur dans ce domaine, surtout que l'exigence de transparence des traitements algorithmiques semble bien moins fluctuante qu'on pourrait le supposer[1726], et il nous semble suffisamment mature pour intégrer une déontologie, et ce même si c'est sa mise en œuvre en informatique est encore à l'étude concernant certaines techniques informatiques.

B - Vers une institutionnalisation de l'éthique en vue de son uniformisation pour réglementer les acteurs

857. A la différence des comités institutionnels ayant été créés pour conseiller le gouvernement ou le législateur[1727], il s'agit ici d'étudier les structures mises en place pour penser l'éthique avec les acteurs en vue d'aboutir à une véritable déontologie.

858. Dès 1975, le rapport Tricot[1728] s'interrogeait sur l'instauration d'un code et d'un ordre pour les informaticiens. Il n'a toutefois pas fait le choix de retenir cette piste. Il a en effet considéré que d'une part les contours de la profession d'informaticien n'étaient pas suffisamment précis, et il convient de reconnaître que l'informatique constitue une catégorie très large de métiers[1729], et que d'autre part ils sont plus souvent des salariés que des indépendants. Pour pallier ce dernier point, le rapport a envisagé l'insertion dans les statuts, tels

[1725] Twitter effectue par exemple des consultations dans le but de définir ce qu'est un intérêt public sur sa plateforme. Voir en ce sens, TWITTERSAFETY, Calling for public input on our approach to world leaders, *Blog.Twitter.com* [en ligne]. 18 mars 2021 [Consulté le 12 avril 2021]. Disponible à l'adresse : https://blog.twitter.com/en_us/topics/company/2021/calling-for-public-input-on-our-approach-to-world-leaders.html

[1726] FJELD J, ACHTEN N, HILLIGOSS H, NAGY A, SRIKUMAR M., Principled *Artifical Intelligence : Mapping Consensus in Ethical and Rights-Based Approches to Principles for AI, op. cit.* ; DECLARATION DE MONTREAL IA RESPONSABLE, La déclaration de Montréal pour un développement responsable de l'intelligence artificielle, *op. cit.*

[1727] *Supra*., n° 836 et s.

[1728] Rapport de la commission informatique et libertés, *La Documentation française*, 1975, p. 66.

[1729] *Ibid.*, Les rapporteurs avaient noté que l'informatique implique par ailleurs de nombreuses autres activités humaines existantes telles que le personnel soignant ou encore les juristes. De plus, cette matière est qualifiée de mouvante par ces derniers.

que les contrats de travail, l'ajout d'une clause de conscience afin que « *que dans les cas douteux, notamment ceux qui peuvent se situer à la frange du droit et de la morale, l'employé ou l'employeur ou encore, le cas échéant, la juridiction saisie, puissent demander l'avis de l'instance de contrôle* »[1730].

859. Il est vrai qu'aujourd'hui le numérique est aussi saisi par le truchement de la déontologie médicale. En effet, faut-il qu'un médecin comprenne le cheminement algorithmique ayant mené à la recommandation de la prescription d'un traitement par un logiciel ?[1731] Auquel cas, quel est l'intérêt de l'automatisation s'il s'agit de revérifier la cohérence de chaque traitement ? Nos réflexions n'ont jamais mené à exclure le recours à l'informatique dans tous les usages, mais il convient également de prendre en considération que, sans la transparence, nécessaire à l'explicabilité de ces technologies surtout pour le professionnel de santé il demeure un risque d'erreurs, voire de mauvaises recommandations, pouvant aboutir à des incidences sur l'intégrité physique et morale des patients, et ce de manière potentiellement systémique[1732]. Certes, lorsque les algorithmes sont contenus dans des dispositifs de santé, et qu'ils s'apparentent défectueux, ce n'est pas le professionnel de santé qui engage sa responsabilité, mais le fabricant[1733]. Toutefois, dans les hypothèses où le dispositif médical serait parfaitement fonctionnel, son usage pourrait être caractérisé comme une faute du professionnel de santé s'il y a manquement à la déontologie prévue par le Code de la santé publique[1734]. Ainsi, comme nous l'avons abordé en détail[1735], la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique prévoit en son titre III intitulé « *appuyer la diffusion des progrès scientifiques et technologiques dans le respect des principes éthiques* »[1736] que le professionnel de santé qui recourt à des traitements algorithmiques auto-apprenants utilisés à des fins de visée préventive, thérapeutique ou de diagnostic doit garder la main sur ce processus et en avertir le patient de son utilisation et de son résultat[1737].

860. De la même manière, lorsque les traitements algorithmiques font leur immixtion dans le droit, notamment pour analyser des décisions de justice, ouvrant potentiellement la voie à une

[1730] *Ibid*., p. 67.
[1731] NEVEJANS N., « L'influence des logiciels d'aide à la décision sur le processus décisionnel médical à la lumière du droit et de l'éthique », *op. cit*., p. 120 et ss.
[1732] En effet, il existe quelques grands éditeurs de logiciel. Si une erreur importante de traitement intervenait, la patientèle des médecins recourant au logiciel défectueux pourraient être affectées.
[1733] Art. L. 1142-1 du Code de la santé publique.
[1734] Art. R. 4127-1 à R. 4127-112 du Code de la santé publique.
[1735] *Supra*., n° 381 et s.
[1736] Loi n° 2021-1017 du 2 août 2021 relative à la bioéthique.
[1737] Art. L. 4001-3 du Code de la santé publique crée par l'art. 17 de la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique.

justice augmentée, il est possible de les réglementer[1738], et on envisage assez facilement la possibilité d'encadrer leur conception par l'intermédiaire de la déontologie comme le prévoyait le Rapport Tricot[1739].

861. Cela étant, notre réflexion nous pousse à aller plus loin dans la mesure où l'objectif est d'envisager une déontologie des professions informatiques afin d'y inclure des exigences relatives à la transparence des systèmes qu'ils créent, et ce de différentes manières, à travers la traçabilité des processus du système, la notification à l'utilisateur qu'un système est intervenu, voire l'explicabilité, et ce dès la conception du système. C'est-à-dire imposer que ces systèmes soient conçus dès le départ pour respecter le principe de transparence. Mais pour cela, puisque nous ne pouvons nous satisfaire des initiatives de « *soft law* », l'Etat, pour la raison que nous avons déjà abordée[1740], bénéficie de la légitimité à imposer un cadre dans lequel des réflexions pourront avoir lieu sur ces thématiques, de façon à ce que, le cas échéant, cette éthique intègre ensuite notre droit. Certes, les nouvelles technologies imposent un suivi et une rigueur, mais le droit a toujours été produit en réaction à des nouveaux faits juridiques. La problématique est donc plutôt de permettre l'adaptabilité rapide du droit, du moins dans certains cas de figure, c'est-à-dire dans les cas où la règle est purement technique, et surtout une fois adoptée de la faire respecter.

862. Il manque toutefois une structure pour élaborer cette déontologie. Force est de constater qu'il n'a jamais été question que le CNPEN rattaché au CCNE proposé dès 2017 par la CNIL[1741] à la suite de la LRN[1742], puis en 2018, par le rapport Villani[1743], n'ait eu pour objectif d'adopter une déontologie, mais de conseiller les gouvernants, voire d'aboutir à une simple éthique.

863. Pourtant, selon la CNIL, « *l'éthique apparaît comme une éclaireuse du droit, la norme éthique une préfiguration de la norme juridique* »[1744] et il apparait nécessaire de former les

[1738] Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice (1). Pour plus de précisions, *Supra.*, n° 373 et s.
[1739] *Supra*., n° 858.
[1740] *Supra*., n° 624 et s.
[1741] CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *CNIL.fr* [en ligne]. Décembre 2017 [Consulté le 22 avril 2021]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
[1742] Le législateur a également donné compétence à la CNIL, par l'intermédiaire de la loi pour une république numérique de 2016, de conduite « une réflexion sur les problèmes éthiques et les questions de société soulevées par l'évolution des technologies numériques ; », loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, art. 59.
[1743] VILLIANI C., Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne, p. 22, *Vie-publique.fr* [en ligne]. Mars 2018 [Consulté le 16 avril 2020]. Disponible à l'adresse : https://www.vie-publique.fr/sites/default/files/rapport/pdf/184000159.pdf
[1744] CNIL, Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, *op. cit.*, p. 24.

maillons de la « *chaîne algorithmique* », c'est-à-dire à la fois les concepteurs et les professionnels[1745]. La CNIL, dans la première recommandation de son rapport[1746], évoquait que parmi les contributions qu'elle a pu analyser, un renforcement de l'éthique était souhaitable pour les professions ayant trait à l'informatique, parmi lesquels il existait également un enthousiasme chez les personnes interrogées au sujet d'un principe de transparence. Les groupes de travail ont par exemple souligné « *la nécessité de disposer de droits renforcés en matière d'information, de transparence et d'explication quant à la logique de fonctionnement de l'algorithme* ». Tous les participants n'étaient cependant pas en accord avec ce principe, et ne considéraient pas que la transparence pouvait régler à elle seule l'enjeu du numérique. La CNIL insiste toutefois énormément sur l'ouverture des enjeux éthiques dès l'enseignement de ces matières, et incite à la féminisation de ces professions ou encore à une plus grande ouverture, y compris aux sciences humaines et sociales. Nous pensons que c'est effectivement une chose essentielle, mais cela ne peut être suffisant. Et pour enseigner l'éthique, et espérer les effets d'un éventuel droit souple, faut-il encore connaître le contenu de ce dernier, ce qui implique une certaine uniformisation de l'enseignement pour ces professions. Cela renvoie également à l'instance qui sera amenée à établir ces réflexions, puisqu'à défaut, d'une école à l'autre, d'une entreprise à l'autre, les règles éthiques ne pourront être que disparates[1747], et les effets bénéfiques sur la société et les individus, ne pourraient s'en faire ressentir. Le rapport Villani note toutefois à raison que « *L'enseignement de l'éthique vise plutôt à transmettre aux futurs architectes de la société numérique les outils conceptuels pour identifier et confronter de manière responsable les problèmes éthiques et moraux rencontrés dans le cadre de leur activité professionnelle* »[1748]. Nous pensons qu'il ne peut s'agir, tout au plus que d'une simple initiation tant que l'éthique ne s'est pas mue en déontologie. Elle ne saurait donc pallier l'absence de réglementation.

864. C'est un cadre que l'Etat doit mettre en œuvre, car il est assez peu probable que l'initiative privée se structure de manière unanime à cette fin, raison pour laquelle il est voué à jouer un rôle ternaire, c'est-à-dire d'arbitre entre les différentes initiatives des acteurs privés, ne serait-ce car il en a la légitimité. Naturellement, lorsque l'acteur est confronté à une nouvelle situation non encore appréhendée par le droit, sa formation doit lui permettre de faire le meilleur

[1745] *Ibid*., p. 6.
[1746] *Ibid*., p. 54.
[1747] *Supra*., n° 847 et s.
[1748] VILLIANI C., SCHOENAUER M., BONNET Y., et *al.*, Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne, *op. cit*., p. 147.

choix, voire le cas échéant, comme le soulignait le rapport Tricot[1749], de solliciter une instance éthique sur cette question pour apporter une réponse concrète dans le cadre du développement d'une application, doctrine qui revêtirait ensuite un caractère obligatoire.

865. L'objectif étant d'éviter une certaine lenteur dans la remise des travaux de cette instance et un déploiement pratique et rapide pour être le plus respectueux possible du principe de transparence ; principe qui, rappelons-le, serait constitutionnellement protégé dans notre paradigme, et nécessiterait une application concrète, même si le législateur n'a pas encore jugé utile de venir préciser la mise en œuvre d'un usage.

866. La CNIL notait par ailleurs que *« l'intervention du législateur est également vivement souhaitée (94%) afin de mieux intégrer l'éthique dans les lois « à travers des chartes et des règles déontologiques, des formations, des concertations »*[1750]. A notre sens, la déontologie doit nécessairement s'imposer, surtout lorsque les pratiques des acteurs sont trop divergentes, ce qui est actuellement le cas. En effet, comme nous l'avons vu, bien qu'il y ait consensus sur le principe de transparence, il n'y en a aucun sur sa nature et son degré. Ainsi, certaines initiatives en matière de déontologie de l'informatique existent, mais n'ont jamais été reprises, voire complétées[1751].

867. Qu'il s'agisse de l'effectivité des droits et libertés, ou de l'ordre juridique en général, ce à quoi concourt le principe de transparence des traitements algorithmiques, il est désormais nécessaire qu'un droit étatique dur intervienne pour réglementer les pratiques des concepteurs de ces systèmes par la déontologie. Nous nous prononçons donc en faveur de la création d'une assemblée dédiée, ce qui n'empêchera nullement l'adoption, comme c'est déjà le cas en médecine, de règles professionnelles sectorielles. Cette assemblée, à l'initiative des règles déontologiques par l'éthique, en collaboration avec l'Etat, pourrait également faire l'objet de participation d'acteurs extérieurs comme des représentants de la société civile. Elle réunirait par ailleurs les ordres professionnels existants sur ces questions. A cette fin, il pourrait s'agir d'une chambre du CESE, de façon à ce qu'ensuite l'éthique puisse se muer en déontologie.

[1749] *Supra*., n° 858.
[1750] CNIL, Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, *op. cit.*, p. 54 à 55.
[1751] CIGREF, Déontologie des usages des Systèmes d'Information, Principes fondamentaux », *Cigref.fr* [en ligne] [Consulté le 2 mars 2020]. Disponible à l'adresse : https://www.cigref.fr/cigref_publications/RapportsContainer/Parus2006/2006_-_Deontologie_des_usages_des_SI_CIGREF_-_CEA-CED_Rapport_Web.pdf

868. Certains chercheurs, comme Céline Castets-Renard, ont déjà relevé que parmi le contenu de ces règles, « *de bonnes pratiques déontologiques à l'adresse des développeurs d'IA pourrait, par exemple, être pertinent, tel le choix des méthodes statistiques dans la constitution d'un échantillon de données d'apprentissage* »[1752].

869. Au-delà d'une telle institution, il apparaît de plus en plus nécessaire de créer une profession dédiée aux algorithmes manipulant ou non des données personnelles. Cette profession ferait le pont entre l'informatique, la sociologie et le juridique.

PARAGRAPHE 2 – VERS DES INSTITUTIONS PROFESSIONNELLES REGLEMENTEES CONCOURANT A LA TRANSPARENCE

870. Il semble difficile d'obtenir une conformité des professionnels qui développent ou mettent en œuvre les systèmes automatisés sans en penser les mécanismes juridiquement.

871. Le correspondant « informatique et libertés » (CIL), ayant fait l'apparition dans notre droit national dès 2004, était un outil juridique intéressant participant à une meilleure effectivité de la réglementation, notamment en matière de transparence, tout en jouant le rôle d'intermédiaire avec le régulateur qu'est la CNIL. Cette institution[1753], devenue DPD, a été consolidée par le RGPD, mais ce régime juridique dispose encore de nombreuses carences (A).

872. Afin de pallier ces imperfections nous proposons son extension aux traitements de données non seulement personnelles et le renforcement du statut du DPD amené à intervenir surtout dans la phase de mise en œuvre du traitement, c'est-à-dire de son fonctionnement. Quant à l'élaboration des traitements susceptibles d'entraîner des conséquences juridiques systémiques sur les individus et la société, il s'agirait donc de créer une profession réglementée dont l'objectif portera sur la maîtrise d'œuvre de ces systèmes (B).

[1752] CASTETS-RENARD C., « Comment construire une intelligence artificielle responsable et inclusive ? », *Recueil Dalloz*, 2020, p. 225.
[1753] Le Rapport Braibant qualifie cette profession d'institution, raison pour laquelle nous reprenons cette dénomination. Voir en ce sens, BRAIBANT G., Rapport public données personnelles et société de l'information Premier ministre sur la transposition en droit français de la directive n° 95-46, 1998.

A - Du correspondant « informatique et libertés » au délégué à la protection des données : les carences du régime juridique d'une institution

873. Il convient de remonter aux prémices des législations relatives aux données à caractère personnel pour resituer ce débat sur l'utilité d'une telle profession qui pourrait être étendue aux traitements algorithmiques en général, et ce afin de penser et faire respecter les obligations relatives au principe de transparence. Dès 1970, en Allemagne[1754], en l'occurrence dans le Land de Hesse, nous retrouvons les premières traces du CIL en vue d'assurer la conformité des responsables de traitement, et ce avant l'adoption de la réglementation fédérale de 1977 qui généralisa ce dispositif.

874. En France, les discussions relatives à ce délégué n'ont eu lieu que lors de la transposition de la directive 95/46/CE[1755], puisqu'elle comportait à la demande de l'Etat Allemand[1756], la création d'un *« détaché à la protection des données* »[1757]. Mais le rapport Braibant accueillera avec scepticisme cette institution. Selon lui, la France, contrairement à l'Allemagne, ne se situerait pas dans la culture de la cogestion et son indépendance ne pourrait être garantie sans la mise en œuvre d'un ordre et d'un code de déontologie[1758]. Pourtant, dès 1993, une circulaire[1759] prévoyait la mise en œuvre d'un *« correspondant du commissaire du Gouvernement auprès la CNIL* ». La mission de ces délégués, désignés dans chaque département ministériel, est de s'assurer de la conformité de l'administration à la LIL, et ce en lien avec le commissaire du gouvernement auprès de la CNIL. A l'instar du correspondant proposé par l'Allemagne au niveau de l'Union européenne en 1995, mais qui s'applique aussi bien aux organismes privés que publics, le correspondant du commissaire est une prémisse du CIL en France.

875. Malgré ce rapport très critique, le CIL, appelé « *correspondant à la protection des données à caractère personnel »* par le législateur, est adopté par les parlementaires et figure dans la loi de 2004[1760]. Il est chargé « *d'assurer, d'une manière indépendante, le respect des*

[1754] CNIL, *Guide du correspondant informatique et libertés*, édition 2011, p. 46.
[1755] BRAIBANT G., Rapport public données personnelles, *op. cit*.
[1756] *Ibid*., p. 72.
[1757] 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.
[1758] BRAIBANT G., Rapport public données personnelles, *op. cit*., p. 72 à 73.
[1759] Circulaire du 12 mars 1993 relative à la protection de la vie privée en matière de traitements automatisés : application aux administrations et à l'ensemble du secteur public de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; rôle des ministères et coordination par le commissaire du Gouvernement auprès de la Commission nationale de l'informatique et des libertés.
[1760] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

obligations prévues dans la présente loi »[1761], ce qui implique la conformité au principe de transparence déjà prévu par la directive[1762], ainsi que les obligations relatives au droit d'accès à ses données à caractère personnel depuis 1978[1763]. Afin d'inciter le plus possible les acteurs à recourir à un tel délégué, car sa désignation n'est que facultative, elle conditionne l'exonération pour le responsable de traitement de certaines modalités comme les formalités préalables auprès de la CNIL[1764]. Il s'agit donc d'un mécanisme de corégulation pragmatique partant du postulat que le régulateur ne peut pas contrôler en permanence tous les acteurs, et qu'il conviendrait mieux d'associer ces professionnels à leur mise en conformité, et ce par l'intermédiaire de cette institution, n'empêchant pas par ailleurs des contrôles opérés par la CNIL[1765].

876. Le CIL est aussi un atout pour les petites structures, comme les collectivités territoriales, qui ne disposent pas toujours des services suffisants pour répondre aux nouvelles exigences réglementaires[1766]. Cette institution joue de plus le rôle d'interface avec le régulateur historique en tant qu'outil essentiel au dialogue, y compris pour favoriser le travail de l'instance de contrôle. A ce titre, la désignation d'un CIL fait l'objet d'une notification à la CNIL. Le correspondant pouvait également « *saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions.* »[1767]. Il s'agissait donc de l'instituer en tant que collaborateur de l'instance de régulation.

877. C'est sous la dénomination de « *délégué à la protection des données* » que cette logique a finalement a été reprise par le RGPD, mais en la rendant cette fois-ci obligatoire pour certains organismes[1768]. Toutefois, il convient de reconnaître que considérant la qualification du DPD, comme autrefois avec le CIL, il ne s'agit toujours pas d'une profession réglementée, et le niveau de qualification de celui-ci est variable. Le RGPD indique que « *Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses*

[1761] *Ibid*., art 22 III.
[1762] *Supra*., n° 80 et s.
[1763] *Ibid.*
[1764] « *des possibilités de déclaration simplifiée, voire d'exonération totale de déclaration » (…) « En contrepartie, les entreprises bénéficieront d'une exemption de déclaration de leurs traitements sous réserve de la tenue d'un registre* », TURK A., Rapport public n°218, *op. cit*., p. 43. La loi adoptée a ensuite comporté qu'en contrepartie de la désignation d'un correspondant « le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non-membre de la Communauté européenne est envisagé. », art. 22 de la LIL de 1978 modifiée par la loi de 2004.
[1765] « *Leur mise en place doit permettre à la CNIL de disposer d'un réseau de correspondants, ainsi que cela existe déjà dans le secteur public. En effet, une seule autorité de contrôle ne peut pas tout assurer*. » *Ibid*., p. 95.
[1766] **«** *Cette possibilité pourrait d'ailleurs s'avérer particulièrement utile pour les collectivités territoriales, qui souffrent parfois d'un manque d'expertise pour les plus petites d'entre elles*. TURK A., Rapport public n°218, *op. cit.*, p. 96.
[1767] Art. 22 III de la LIL de 1978 modifiée par la loi de 2004.
[1768] Art. 37 et suivants du RGPD. *Supra.*, n° 237 et s.

connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39. »[1769], c'est-à-dire de ses missions prévues par le texte[1770]. Les compétences exigées sont donc évasives[1771], et s'apprécient à l'aune de ses missions pour apprécier sa compétence[1772], comme opérer ou faciliter les audits internes, voire externes des traitements[1773]. C'est donc au responsable du traitement ou à son sous-traitant de s'assurer des compétences de ce dernier, ce qui est dans son intérêt pour être en conformité et se prémunir des éventuelles violations du RGPD, et donc notamment des sanctions de l'autorité de contrôle.

878. Mais force est de reconnaître que l'employeur n'est pas toujours apte à évaluer ses compétences tant elles sont transdisciplinaires, allant de l'informatique à une bonne connaissance du régime juridique applicable. Afin de faire gagner en visibilité, la CNIL peut procéder à la certification des compétences du DPD selon deux référentiels qu'elle a établi. Le premier permet à la CNIL d'évaluer le délégué lui-même[1774], tandis que l'autre certifie par l'obtention d'un agrément les organismes habilités à certifier les DPD[1775]. Toutefois, cette certification n'est pas obligatoire pour exercer cette fonction.

879. Néanmoins, et nous abordions déjà cette problématique précédemment[1776], dans la grande majorité des cas, le DPD est un délégué interne à l'organisme, c'est-à-dire salarié[1777]. Bien qu'il soit soumis à un lien de subordination juridique, il ne peut en théorie « *être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions* »[1778] ou bien recevoir des instructions[1779]. De plus, parce qu'il exerce ses missions au cœur de ce qui constitue la valeur ajoutée de l'organisme, et ce en ayant accès aussi bien aux données à caractère personnel qu'aux opérations de traitement[1780], il est soumis au secret professionnel, voire à une obligation de confidentialité[1781]. Mais le DPD ne bénéficie pas

[1769] Art. 37 RGPD.
[1770] *Supra.*, n° 237 et s. sur les missions du DPD.
[1771] Les compétences requises sont tout aussi évasives que lors de la rédaction de la loi de 2004 qui précisait que « le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions », art. 22 de la LIL de 1978 modifiée par la loi de 2004.
[1772] *Supra.*, n° 237 et s.
[1773] Comme nous l'avons vu précédemment, les audits internes et externes favorisent la transparence des traitements.
[1774] CNIL, Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPD).
[1775] CNIL, Délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPD).
[1776] *Supra.*, n° 237 et s.
[1777] Il peut également s'agir d'un DPD externe, y compris une personne morale.
[1778] Art. 38, § 3 du RGPD.
[1779] *Ibid.*
[1780] *Ibid.*, § 2.
[1781] *Ibid.*, § 5.

du statut de salarié protégé pour autant[1782], ce qui constitue à notre sens une entrave à l'indépendance réelle de celui-ci. Cette ambiguïté, déjà présente dans la réglementation antérieure avec le CIL, n'a pas été rectifiée, y compris lors de la transposition du RGPD en droit national.

880. Par ailleurs, Guillaume Desgens-Pasanau relevait une inquiétude, non fondée selon lui, mais bel et bien présente chez de nombreux acteurs, et que nous trouvons justifiée.

> « *cet « entre-deux » est bien souvent source d'incompréhension pour les responsables de traitements ou les CIL « pressentis ». Les premiers craignent parfois de désigner un « électron libre » qui effectuerait ses missions sans avoir à en justifier auprès de son employeur. Les seconds craignent parfois que l'absence du statut de salarié protégé ne les expose, sur le plan disciplinaire, dans le cadre de l'exercice de leurs fonctions. Cette situation est particulièrement vraie lorsque le CIL est salarié* »[1783].

881. La désignation d'un DPD ne doit pas être qu'une apparence de conformité, mais est censée constituer une protection aussi bien pour les personnes physiques faisant l'objet d'un traitement que pour faciliter la conformité. Certes, ce mécanisme de corégulation est utile, mais pour mettre en œuvre le principe de transparence que nous avons esquissé tout le long de ces travaux, il convient de lui reconnaître plus d'indépendance, notamment pour éviter les pressions sur ce dernier qui pourraient s'exercer par d'autres biais que ses missions[1784], ne serait-ce car dans les faits les possibilités de coercition à son encontre sont non négligeables lorsqu'il effectue correctement son travail.

882. De nombreux acteurs, y compris dans les organismes publics, ont désigné des DPD internes qui sont salariés, voire fonctionnaires, et dont la mission principale n'est pas de remplir ces missions[1785], ce qui pose légitimement la question de la compétence eu égard à la complexité de la réglementation, tout en soulignant un risque de conflits d'intérêts[1786] remettant en cause

---

[1782] SENAT, Statut des délégués à la protection des données, *op. cit.*
[1783] DESGENS-PASANAU G., *Le correspondant « informatique et libertés »*, *LexisNexis*, 2013, p. 43 à 44.
[1784] « *Le RGPD n'interdit les sanctions que si elles sont imposées au DPD à la suite de l'exercice de ses missions de DPD* », G29, Lignes directrices concernant les délégués à la protection des données, version révisée et adoptée le 5 avril 2017, p. 18.
[1785] Selon une étude du Ministère du travail, de l'emploi et de l'insertion, 74,2 % des DPD effectuent cette mission à temps partiel. Parmi cette proportion, le temps de travail dédié à cet exercice représente pour 57,8% d'entre eux seulement 25% et moins de leur temps, MINISTERE DU TRAVAIL, DE L'EMPLOI ET DE L'INSERTION, Etude Les enjeux emplois et compétences de la mise en œuvre du Règlement général sur la protection des données, 8 octobre 2020, p. 14.
[1786] *Ibid*., « *En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du*

l'indépendance de l'institution de DPD. En effet, selon l'étude du Ministère du travail, de l'emploi et de l'insertion, 43,6 % de ces délégués proviennent d'un domaine d'expertise autre que le juridique et l'informatique[1787].

B - Extension des missions du DPD et nouvelle profession réglementée pour les projets d'importance significative sur la société et les individus

883. Il convient de préciser en premier lieu que les deux professions que nous aborderons sont complémentaires. L'un, à savoir le DPD amélioré, portera essentiellement sur la phase de conformité du traitement à la réglementation lorsque ce dernier est en fonctionnement, tandis que l'autre, intervient en tant qu'expert indépendant lors de la maitrise d'œuvre pour concevoir les projets d'envergure, c'est-à-dire à incidence systémique.

1 - Les améliorations du DPD

884. Le DPD incarne à la fois les forces et les lacunes du régime juridique sur les données personnelles. Il repose évidemment sur une philosophie de responsabilité des acteurs, mais sans apporter suffisamment de garanties, notamment du fait d'un manque d'uniformisation sur les formations et les obligations déontologiques. Il ne peut de plus être totalement indépendant, comme l'indiquait le rapport Braibant[1788], et ce malgré les affirmations du RGPD[1789]. Ses missions ne portent de plus que sur le domaine particulier des données personnelles, ce qui aujourd'hui est insuffisant face aux nouveaux enjeux des traitements algorithmiques ne manipulant pas de données personnelles, et particulièrement sur leur transparence, parce qu'ils sont susceptibles d'exercer des effets sur les personnes et plus largement sur la société. Par ailleurs, il est à noter que la proposition de règlement européen harmonisant des règles au sujet de l'IA, et qui prévoit comme nous le verrons, de nouvelles exigences en matière de transparence[1790], n'évoque aucunement l'élargissement des missions du DPD à ces enjeux, ni l'instauration d'une quelconque autre profession à des fins de conformité. Cette position est

service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. », p. 19.

[1787] MINISTERE DU TRAVAIL, DE L'EMPLOI ET DE L'INSERTION, *Etude Les enjeux emplois et compétences de la mise en œuvre du Règlement général sur la protection des données*, 8 octobre 2020, p. 6.

[1788] *Supra*., n° 874.

[1789] Cons. 97 du RGPD, « *De tels délégués à la protection des données, qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance* ».

[1790] Proposition n° 2021/0106 (COD) 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, du 21 avril 2021.

regrettable et incompréhensible, alors que l'Union avait pourtant été à l'initiative d'une telle institution en matière de données personnelles.

885. Il est en effet attendu des informaticiens qu'ils respectent le droit[1791], même si cette mission n'est pas acquise, surtout lorsqu'il existe des angles morts juridiques, la culture des enjeux démocratiques est essentielle pour ces professionnels. Car comme nous l'avons vu, l'éthique est fluctuante.

886. En ce sens, il apparaît nécessaire d'élaborer un tissu de délégués compétents pour tirer bénéfice du principe de responsabilité[1792]. Une formation commune reprenant les critères de la certification des DPD par la CNIL, ainsi que des éléments relatifs à la gouvernementalité algorithmique, aux enjeux démocratiques du numérique, ne pourrait qu'œuvrer favorablement à l'uniformisation de cette institution. Et comme nous l'avons évoqué, certains délégués n'ont pas de compétence juridique ou inversement informatique, ce qui rend la transposition opérationnelle de la réglementation difficile, raison pour laquelle nous nous prononçons en faveur d'une qualification avec un tronc commun couplée à une formation pratique[1793]. Il ne pourrait seulement s'agir d'un correspondant des données personnelles, mais aussi du respect des droits fondamentaux dans l'environnement numérique, qui rappelons-le « *doit être au service de chaque citoyen* »[1794].

887. L'avantage de l'extension des missions du DPD est qu'il permet *de facto* de bénéficier d'un maillage existant sur lequel s'appuyer, mais dont il conviendrait toutefois de renforcer pour combler les lacunes existantes. Au même titre que la recommandation du Conseil général de l'économie de 2016[1795] sur les modalités de régulation des algorithmes de traitement de contenus, nous nous prononçons en faveur de l'idée de l'extension des missions du DPD. Ainsi, un « *chief algorithm officer* », responsable chargé du fonctionnement de l'algorithme, serait identifié et aurait pour mission de communiquer auprès du public « *les objectifs, les finalités et les contraintes du systèmes* » et expliciter l'algorithme[1796].

[1791] VILLIANI C., SCHOENAUER M., BONNET Y., et *al.*, Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne, *op. cit*., p. 146.
[1792] Supra., n° 208 et s.
[1793] Les DPD disent connaître des difficultés à retranscrire le RGPD de manière opérationnelle. Une formation commune a également pour vertu de créer un tissu de délégué pouvant par la suite converser.
[1794] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 1.
[1795] CONSEIL GENERAL DE L'ECONOMIE DE L'INDUSTRIE, DE L'ENERGIE ET DES TECHNOLOGIES, *Rapport, Modalités de régulation des algorithmes de traitement des contenus*, 13 mai 2016, p. 44 à 45.
[1796] *Ibid*., recommandation n° 3, p. 45. Ce rapport n'aborde que la question des traitements de contenus, mais nous sommes favorables à ce que cette extension puisse concerner une large gamme de traitements que nous aborderons par la suite.

888. Le DPD a fait l'objet d'une tentative de réglementation par la déontologie, mais elle ne s'applique qu'aux personnes certifiées, ce qui est encore très minoritaire selon les dernières études[1797]. Alors que le projet de charte déontologique de la CNIL à destination des DPD certifiés évoque qu'il « *doit superviser de manière adéquate leur activité sans dissimuler des erreurs ou des non-conformités et corriger toute non-conformité ou irrégularité détectée* »[1798], il s'agirait d'y ajouter à l'instar des devoirs d'information d'un médecin à l'encontre de ses patients, une plus grande obligation d'information au public au sujet des traitements algorithmiques. En cas de doute sur la nature et le degré de la transparence à opérer auprès des personnes concernées ou plus largement du public, il devrait pouvoir contacter l'autorité de contrôle des traitements algorithmiques que nous proposons. Il serait intéressant qu'elle mette à disposition un registre public anonymisé des questions et réponses apportées, pour que chaque acteur puisse consulter la doctrine de l'autorité dans chaque domaine. En cas de litige avec les demandeurs sur les modalités de transparence, c'est l'instance de contrôle des traitements algorithmiques, en tant que tiers de confiance, qui statuerait sur la nature de la communication à effectuer. S'il s'agit par exemple d'une transparence indirecte, c'est-à-dire portant seulement sur l'explication des principales caractéristiques du traitement en fonctionnement, l'autorité de contrôle devra se voir transmettre tous les éléments démontrant la véracité de cette communication afin d'empêcher une asymétrie informationnelle. Si la loi l'exige, la transparence s'appliquerait directement avec les précautions nécessaires comme l'anonymisation des données personnelles, par la transmission des jeux de données et du code source.

889. Le projet de charte de la CNIL prévoit la possibilité en cas de violation des obligations déontologiques d'une sanction disciplinaire allant de la suspension au retrait de l'agrément[1799], ce qui n'empêchera pas par ailleurs de continuer à exercer. Cette approche ne nous semble pas adéquate. Cette profession n'étant pas soumise à un ordre professionnel, parce qu'elle ne peut être véritablement indépendante, il conviendrait davantage de recourir à une exigence de diplôme plutôt qu'à celle d'une certification. Nous préconisons également que cet emploi soit obligatoirement exercé à temps plein par des salariés protégés. En effet, il pourrait être tentant

[1797] Selon l'étude du Ministère du travail précitée, les DPD ne sont que 16,5 % à être certifiés sur le fondement du référentiel établi par la CNIL, p. 20.
[1798] CNIL, *Critères de certification de délégué à la protection des données (DPO)*, art. 4, Cnil.fr [en ligne]. 23 mai 2018 [Consulté le 14 février 2021]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/projet_de_referentiel_certification_dpo_pour_consultation.pdf
[1799] *Ibid*., art. 10.

pour un employeur d'arguer de fautes professionnelles détachables de ces missions pour évincer un DPD qui ferait correctement son travail.

2 - Une profession réglementée pour la conception des traitements systémiques

890. Dans les années quatre-vingt-dix lorsque l'institution CIL a été évoquée en France, le rapport Braibant notait que le délégué pourrait être « *un salarié de l'entreprise ou une personne exerçant une profession libérale, un commissaire aux données analogue au commissaire aux comptes, qui pourrait d'ailleurs cumuler les deux fonctions.* »[1800]. Puis, lorsque la question de la transparence et de l'utilisation des algorithmes a été appréhendée de manière générale et non seulement sous le prisme de la règlementation des données personnelles, la doctrine s'est prononcée en faveur d'une nouvelle profession détachable de la précédente. Ainsi, certains ont abordé également l'hypothèse de l'instauration d'un commissariat aux données « *afin de contrôler la régularité des traitements de données effectués par les organisations, puis de révéler aux autorités publiques les faits délictueux dont ils auraient connaissance* »[1801].

891. Il ne s'agit pas de faire de ces professionnels des « algorithmistes »[1802] ou des « experts publics assermentés »[1803], cette mission relevant de la commission de contrôle unique des traitements algorithmiques[1804], puisqu' il s'agit dans l'actuelle réflexion de penser une profession de maîtrise d'œuvre des systèmes, afin que la conformité et la transparence soit pensée dès la conception, et ce en toute indépendance. Cette profession interviendrait obligatoirement pour les catégories de traitement listées par le Parlement, et le cas échéant sur le fondement d'un seuil établi, c'est-à-dire pour les logiciels nécessitant une vigilance particulière du fait de leurs incidences systémiques. Il ne pourra donc s'agir que d'obligations pour les grands projets.

892. La mission de ces professionnels serait de suivre les projets dès leur commencement et de leur faire appliquer les principes juridiques, notamment ceux évoqués dans le cadre de ces travaux, raison pour laquelle il conviendrait d'en faire une profession réglementée soumis à un ordre professionnel. Ainsi, cet ordre, à l'instar des ordres professionnels existants, serait

[1800] BRAIBANT G., Rapport public données personnelles, *op. cit.*, p. 72.
[1801] BOURGEOIS M., « Vers un commissariat aux données », *La semaine juridique entreprise et affaires*, n° 48, 30 novembre 2017, p. 6
[1802] CONSEIL D'ETAT, *Le numérique et les droits fondamentaux*, *op. cit.*, p. 239. Cette idée est initialement reprise de CUKIER K., MAYER-SCHOENBERGER V., *Big Data – La révolution des données est en marche*, Robert Laffont, 2014.
[1803] VILLIANI C., SCHOENAUER M., BONNET Y., et *al.*, Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne, *op. cit.*, p. 21.
[1804] *Supra*., n° 694 et s.

consulté pour l'édiction des règles déontologiques du secteur ainsi que pour leur effectivité, et le cas échéant par la voie de sanctions disciplinaires allant jusqu'à l'interdiction d'exercer en cas de manquement grave à leurs obligations. Cet ordre serait ensuite quant à lui soumis à l'assemblée réunissant tous les ordres et composé de membres de la société civile afin d'uniformiser les pratiques sur la question des algorithmes et de leur transparence comme nous l'avons évoqué[1805].

893. Il reviendrait à ce professionnel de penser les projets dans une approche de « *transparency by design* »[1806] et de s'assurer que les modèles utilisés soient les plus représentatifs possibles afin de créer les systèmes les plus équitables et loyaux. Ces experts auraient pour mission de communiquer sur ces projets sous la forme d'une enquête publique, et ce notamment afin de recueillir les doléances du public. En effet, c'est le critère potentiellement systémique du traitement sur la société qui justifie cette approche[1807].

894. Il convient selon nous, sur le fondement de la proposition de la CNIL évoquant la délivrance d'un « *permis d'utiliser les algorithmes et l'IA* »[1808], de soumettre à autorisation, par les autorités de contrôle sectorielles existantes, l'élaboration de grands projets exigeant l'intervention d'un tel architecte du numérique. Ce professionnel veillerait à penser le projet dès sa conception en conformité avec le droit, notamment par les obligations de transparence applicables ainsi que par la réalisation d'analyse d'impact pour évaluer les incidences sur les droits et libertés. Il arbitrerait également sur les données et les algorithmes les plus opportuns à utiliser en fonction de l'objectif poursuivi, et ce au même titre qu'un architecte pense la construction d'un bâtiment en respectant les normes d'urbanisme et environnementale. Ainsi, c'est une garantie que les informaticiens respectent également le droit.

895. La déontologie doit donc s'appliquer particulièrement à ce maître d'œuvre plus qu'aux équipes dont il aura la responsabilité. Il bénéficierait de plus d'une indépendance vis-à-vis du maître d'ouvrage. Il œuvrerait dans le sens des besoins du maître d'ouvrage, mais dans le

[1805] *Supra*., n° 867.
[1806] Par syllogisme avec le « *privacy by design* » prévu par l'article 25 du RGPD. Cette disposition prévoit la protection des données dès la conception du traitement.
[1807] *Infra*., n° 1000 et s.
[1808] CNIL, Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, *op. cit.*, p. 55 : « *On pourrait ainsi imaginer la création de sorte de « permis d'utiliser les algorithmes et l'IA » dans certains secteurs, acquis grâce à des modules de formations spécifiques que délivreraient universités et écoles spécialisée* ».

respect du droit et des principes déontologiques, voire éthiques si le droit n'est pas encore intervenu[1809].

896. Ce nouveau professionnel disposera également d'une obligation d'alerte auprès du régulateur, mais aussi de son ordre, s'il constate au sein de l'organisme pour lequel il intervient des violations à la réglementation, à défaut il engagera sa responsabilité. Il suivra tout le long du projet sa conformité jusqu'à son fonctionnement. L'instance chargée du contrôle des algorithmes serait également pour ces projets tenue de les réceptionner par un audit, et de particulièrement les suivre pendant la durée du traitement. Enfin, si une modification des finalités devait intervenir *a posteriori,* une nouvelle intervention de cet expert serait sollicitée afin de s'assurer que l'architecture numérique réalisée est toujours conforme. Car comme nous l'avons évoqué, les outils numériques ne sont pas neutres et sont conçus pour des usages particuliers.

CONCLUSION DU CHAPITRE I

897. Pour qu'un système juridique cohérent puisse concourir le mieux possible à la transparence des traitements algorithmiques, notamment à des fins de confiance dans le numérique, c'est à l'Etat qu'il revient de mettre en place les conditions de l'épanouissement des différents acteurs afin qu'ils œuvrent pour une plus grande transparence des traitements. La société civile est amenée à jouer un rôle de contre-pouvoir civique par la voie des corps intermédiaires. Les comités institutionnels et les chercheurs doivent quant à eux continuer à remplir leurs missions d'intérêt général en poursuivant les réflexions sur le numérique, y compris sur les problématiques relatives à la transparence.

898. Il convient néanmoins d'être vigilant dans la mesure où tous les acteurs ne peuvent être considérés de la même manière. En effet, les acteurs concernés par la régulation doivent être suffisamment encadrés afin d'éviter tout « *transparency-washing* », et l'idée selon laquelle ils seraient capables de s'autoréguler est à rejeter. Enfin, l'Etat et les organisations publiques ont leur part de responsabilité dans l'ineffectivité du droit du numérique par l'excès de « *soft law* ». A ce titre, bien que l'éthique soit un outil intéressant de sensibilisation des acteurs et

[1809] Ainsi, en matière d'éthique, à l'instar des recommandations effectuées par le rapport d'instituer des référents déontologues, nous proposons que ce rôle soit effectué par l'ordre en cas de conflit éthique. ETALAB, Ethique et responsabilité des algorithmes publics, proposition 11, p. 23, *Etalab.gouv.fr* [en ligne], juin 2019 [Consulté le 12 décembre 2020]. Disponible à l'adresse : https://www.etalab.gouv.fr/wp-content/uploads/2020/01/Rapport-ENA-Ethique-et-responsabilit%C3%A9-des-algorithmes-publics.pdf

d' « antichambre » de la réglementation, elle ne peut se substituer au droit dur, raison pour laquelle l'élaboration d'une déontologie des concepteurs et des utilisateurs des traitements est à notre sens devenue inévitable. Cette déontologie, comprenant un volet relatif à la transparence de ces traitements, doit être appliquée et pensée en collaboration avec l'Etat et les acteurs concernés. Afin d'être le plus précis possible, une déontologie serait applicable par un ordre à une nouvelle profession de maîtrise d'œuvre intervenant dans toutes les entités susceptibles de développer des traitements algorithmiques ayant une incidence systémique sur les personnes et la société.

899. Ces nouvelles obligations de transparence ne sauraient toutefois autoriser tous les usages en matière de numérique.

CHAPITRE II - DE LA TRANSPARENCE A L'EXCLUSION DES USAGES ALGORITHMIQUES

900. La reconnaissance d'un principe de transparence des traitements algorithmiques est indispensable en ce qu'il permet d'observer le positionnement des puissances œuvrant dans le cyberespace et leurs incidences sur les libertés. Mais cette problématique ne saurait dissimuler la question de l'usage algorithmique et de ses risques. En effet, quand bien même la transparence de ces outils serait totale d'un point de vue juridique et technique, ce qui au regard de l'informatique est une illusion, cela ne saurait légitimer l'immixtion d'une technologie dans un domaine.

901. Comme le souligne Dominique Cardon, avant les récents débats de la société civile au sujet de la transparence des traitements, certains mouvements militaient pour le recours à des algorithmes neutres, ce qui relève d'une méconnaissance technique[1810]. Puis, Frank Pasquale note à cet égard deux vagues[1811] : la première vague n'est pas contre le recours aux traitements algorithmiques, mais est en quête de responsabilisation des acteurs et d'une plus grande transparence des systèmes déployés. Quant à la seconde, intervenue plus récemment, elle est davantage réfractaire à l'immixtion des algorithmes et tend à freiner leurs déploiements, voire à les exclure. Bien que Frank Pasquale craigne que ces deux vagues ne s'affrontent, ces deux mouvements ne nous semblent pas irréconciliables.

902. C'est la raison pour laquelle le droit est aussi un outil de protection de la société et des personnes qui la composent, ce qui nous pousse nécessairement à étudier l'établissement d'un nouveau régime juridique à un niveau législatif et réglementaire relatif à la transparence appliquant le principe de transparence étudié (Section I). Il convient donc précisément de s'intéresser aux domaines nécessitant une transparence accrue. Le récent projet de règlement européen de la Commission européenne[1812] esquisse notamment à cet égard un régime juridique spécifique à la transparence de l'IA qui servira notre démonstration tout le long de ce chapitre.

[1810] « *Il est en effet vain de demander aux algorithmes d'être « neutres » alors qu'ils sont généralement conçus pour choisir, trier, filtrer ou ordonner les informations selon certains principes* », CARDON D., « Le pouvoir des algorithmes », *op. cit.*
[1811] PASQUALE F., The Second Wave of Algorithmic Accountability, *LMP Project.org* [en ligne]. 25 novembre 2019 [Consulté le 12 avril 2021]. Disponible à l'adresse : https://lpeproject.org/blog/the-second-wave-of-algorithmic-accountability
[1812] Proposition n° 2021/0106 (COD) 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, du 21 avril 2021.

903. Toutefois, la transparence ne peut pas tout et pose nécessairement au-delà d'obligations de transparence d'autres exigences au déploiement de ces systèmes. Cela implique même parfois l'exclusion de certaines techniques algorithmiques ou d'usages lorsque la technologie n'est plus au service des citoyens (Section II).

SECTION I - DE L'ETABLISSEMENT D'UN NOUVEAU REGIME JURIDIQUE LEGISLATIF ET REGLEMENTAIRE RELATIF A LA TRANSPARENCE

904. La mise en œuvre de la transparence des traitements algorithmiques implique de recourir à des techniques juridiques particulières dont l'étendue, la nature et le degré doivent être précisés. Certaines de ces techniques ont déjà été abordées tout le long de ces travaux, et s'appliquent déjà, mais le droit européen, par l'intermédiaire de nouvelles propositions, s'intéresse à de nouvelles obligations. Enfin, il convient que les débiteurs de ces obligations soient correctement identifiés, ainsi que les personnes envers qui la levée de l'opacité s'effectuera (Paragraphe 1).

905. Pour ce faire, il est nécessaire de se fonder sur les risques algorithmiques ainsi que la légitimité de l'acteur en cause. Parmi les opérateurs économiques, tous ne représentent pas un risque systémique sur les personnes et la société. La puissance publique mérite également une attention toute particulière du fait de sa plus grande force (Paragraphe 2).

PARAGRAPHE 1 - Choix des techniques juridiques concourant à la transparence

906. Il convient de s'intéresser à la fois aux outils juridiques ainsi qu'aux approches prospectives et concrètes les plus adéquates à retenir dans les régimes juridiques œuvrant en faveur du principe de transparence étudié. Il est important de considérer que plusieurs approches peuvent être retenues par le droit pour réguler les traitements algorithmiques. Ainsi, la neutralité technique apparaît comme une force dans les régimes juridiques généraux (A) tandis qu'un panorama des différentes techniques juridiques nous enseigne sur ce qu'il est nécessaire de réaliser (B).

A - De la nécessaire neutralité technique des régimes juridiques généraux

907. La « neutralité technique » constitue une approche qui nous semble vertueuse en ce qu'elle est suffisamment englobante pour ne pas exclure certaines technologies du giron d'une règlementation qui se voudrait générale. Cela n'empêche nullement un régime juridique sectoriel précis en fonction de l'évolution de la technique.

908. A ce titre, la LIL de 1978[1813], à l'instar des réglementations nationales des autres Etats à cette époque, a institué une vision généraliste en visant les traitements de données personnelles pour préserver la vie privée des personnes physiques et les éventuelles discriminations qui en découleraient[1814]. Quel que soit le procédé utilisé en informatique, c'est la manipulation de données personnelles qui rend applicable ce régime juridique. L'objet saisi, les données personnelles, doit donc être protégée indépendamment de la technologie numérique mise en œuvre. C'est aussi cette philosophie qui est reprise par le RGPD ou la convention 108[1815].

909. Mais la vie privée étant une liberté individuelle rattachée aux personnes physiques, les personnes morales ne bénéficiaient pas d'une quelconque protection alors que des traitements étaient tout aussi susceptibles de les affecter. Indépendamment des exceptions prévues par le texte, le responsable de traitement, qu'il soit public ou privé, est tenu de communiquer à la personne physique concernée des informations sur ce traitement.

910. Les règlementations sectorielles intervenues plus tardivement ont également fait le choix de la neutralité technologique. Ainsi, dans le cadre de la LRN, elle n'a pas fait l'erreur d'exclure certaines méthodes algorithmiques préférant saisir les décisions administratives individuelles prises sur le fondement d'un traitement algorithmique[1816]. A l'exception des secrets protégés par la loi, une certaine transparence s'appliquera donc à l'intéressé au sujet du traitement ayant fondé la décision, et ce quel que soit le logiciel utilisé. Il en est de même lorsque ladite loi désigne l'opérateur de plateforme en ligne soumis à des obligations particulières de loyauté, clarté et de transparence, les personnes, physiques ou morales, agissant

[1813] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1814] A cette époque, cette législation vise le respect de la vie privée. Il n'existe pas à ce moment le début d'une autonomisation du respect des données personnelles. Voir en ce sens le rapport de la commission informatique et libertés, dit « Tricot », La Documentation Française, 1975, p. 49. Depuis, il est en effet intéressant de noter que le respect des données personnelles figure dans certains textes, comme c'est le cas pour la Charte des droits fondamentaux de l'Union européenne à l'article 8, détachée du respect de la vie privée et familiale, ce qui ouvre la voie à un régime juridique totalement différent de celui de la vie privée.
[1815] *Supra.*, n° 80 et s.
[1816] *Supra.*, n° 404 et s.

à titre professionnel, opérant notamment « *le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ; »*[1817]. Le caractère générique, et donc neutre de la formulation, offre une adaptabilité de ces régimes juridiques dans le temps.

911. Arnaud Latil observait dans son panorama des déclarations des droits du numérique publiés lors de la dernière décennie que le principe de neutralité technique est présent dans une grande partie de ces textes[1818], ce qui signifie que « *les auteurs évitent le plus possible de se référer à une technologie particulière »* et que *« cet objectif rédactionnel vise à éviter l'obsolescence juridique et donc à lutter contre la réduction prématurée de leur domaine d'application due au développement, par nature imprévisible, de nouvelles techniques. Les textes étudiés se bornent à faire référence à Internet (rarement au web), aux données et aux processus de décisions automatisées* »[1819].

912. Tandis que l'informatique n'a pas attendu l'IA pour avoir des incidences sur les droits fondamentaux des personnes et sur la société, une nouvelle approche complémentaire semble se dessiner, notamment pour assurer une transparence de ces systèmes, à savoir par les risques par domaine d'intervention[1820]. Mais le choix de la neutralité technique ne semble pas être celui emprunté par la Commission européenne, risquant une obsolescence prématurée et une insécurité juridique aussi bien pour les acteurs soumis à ces obligations que pour les personnes subissant ces systèmes.

913. Il aurait été ainsi préférable d'évoquer tout traitement de données à caractère personnel ou non, intervenant dans les domaines énoncés par la proposition. En effet, la dénomination de « *systèmes d'intelligence artificielle* » telle que retenue renvoie à une ou plusieurs catégories de techniques utilisées dans un logiciel[1821]. Dès lors, les techniques en question sont listées en annexe du projet et nous y retrouvons les « *approches d'apprentissage automatique, y compris d'apprentissage supervisé, non supervisé et par renforcement, utilisant une grande variété de*

[1817] *Supra.*, n° 269 et s.
[1818] FJELD J, ACHTEN N, HILLIGOSS H, NAGY A, SRIKUMAR M., *Principled Artifical Intelligence : Mapping Consensus in Ethical and Rights-Based Approches to Principles for AI*, *op. cit.*
[1819] LATIL A., « En attendant la Déclaration de droits fondamentaux du numérique », *op. cit*.
[1820] Proposition n° 2021/0106 (COD) 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, du 21 avril 2021. Il convient toutefois de noter que ce projet n'est pas si général en ce qu'il ne régule pas par exemple les réseaux sociaux, la commission ayant préférée de le compléter par l'adoption d'une règlementation particulière. En ce sens, *Supra.*, n° 260 et s.
[1821] Art. 3, § 1 du projet.

méthodes, y compris l'apprentissage profond »[1822]. Les systèmes logiques sont également pris en considération par la présente proposition[1823]. Enfin, les dernières techniques saisies par la nouvelle réglementation en cours d'élaboration sont les systèmes statistiques qui comportent les « *approches* statistiques, *estimations bayésienne, méthodes de recherche et d'optimisation* »[1824]. Paradoxalement, bien qu'il s'agisse en apparence d'une certaine neutralité technique, car la proposition ne fait aucunement référence à une marque ou à un logiciel particulier, il s'agit d'une approche excluant de fait certaines techniques même si l'annexe utilise sans plus de précisions le terme « incluant » ces méthodes. Cela sera donc à l'appréciation des tribunaux, ce qui n'est pas sans provoquer une certaine insécurité juridique. Il est difficile pour l'heure de savoir si ces trois grandes catégories de techniques sont suffisamment exhaustives ou si elles sont lacunaires au point d'engendrer un contournement du régime juridique, puisque la Commission estime qu'elles sont à elles seules responsables d'un risque, notamment pour les droits fondamentaux. En effet, dans les hypothèses où une technique n'est pas abordée par le règlement, le régime juridique en construction ne s'appliquerait pas, y compris en cas d'effets sur les personnes ou la société, à l'exception naturellement des réglementations généralistes déjà en vigueur comme le RGPD (mais uniquement parce que son champ d'application porte sur les données à caractère personnel). Ainsi, même si les concepts utilisés par la Commission sont larges, tous les systèmes d'IA ne sont pas concernés par cette proposition[1825]. Quand bien même cette approche pourrait être considérée de neutre d'un point de vue technique, elle n'est pas si générale et ne peut valoir la dénomination générale de « traitement algorithmique » ou « de traitement de données ». Il serait effectivement dommageable qu'en essayant de réglementer l'IA, plus précisément lesdits systèmes, nous exclurions de fait des techniques futures ou non anticipées au moment de la rédaction du texte. L'adaptabilité de ce nouveau régime juridique à des nouvelles techniques pouvant émaner par exemple de l'ordinateur quantique, amenées à potentiellement révolutionner l'informatique interroge tout autant. Bien que la Commission ait voulu s'émanciper des définitions littéraires ou encore informatique de l'IA, n'est-ce pas une erreur d'avoir voulu donner une définition juridique à un concept aussi discuté par les sciences informatiques ?

[1822] Annexe I a) du projet.
[1823] Annexe I b) : les systèmes logiques sont les *« approches fondées sur la logique et les connaissances, y compris la représentation des connaissances, la programmation inductive (logique), les bases de connaissances, les moteurs d'inférence et de déduction, le raisonnement (symbolique) et les systèmes experts* ».
[1824] Annexe I c).
[1825] CRICHTON C., « Projet de règlement sur l'IA (I), des concepts larges retenus par la Commission », *Dalloz IP/IT*, 2021.

914. Au-delà des techniques saisies par le projet, un système d'IA est qualifié comme tel par le règlement uniquement s'il « *peut, pour un ensemble donné d'objectifs 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* »[1826]. L'association des techniques étudiées à des fins spécifiques rend donc ce régime juridique plus restrictif. Comme le note Cécile Crichton, il est troublant que la Commission ait fait par exemple le choix de préciser que les objectifs soient définis par une intervention humaine, ce qui n'est déjà plus toujours le cas[1827]. Et *a contrario*, un système d'IA ne générant pas du contenu, des prédictions ou des décisions produisant des effets avec son environnement, ne serait pas concerné par ces nouvelles obligations, y compris de transparence, alors même qu'il pourrait exercer une incidence indirecte sur la société et les personnes. Les concepts utilisés demeurent en l'état relativement flou juridiquement. La difficulté serait un contournement aisé du régime juridique par les acteurs, rendant inopérant la volonté initiale de la Commission.

B - Panorama des techniques juridiques concourant à la transparence des traitements algorithmiques

1 - Les débiteurs et destinataires des obligations de transparence

915. Souhaiter la transparence des traitements algorithmiques impose nécessairement de désigner le ou les débiteur(s) de ces obligations ainsi que leur destinataire. En d'autres termes, quel sera l'acteur qui devra expliquer le traitement, et à qui.

916. L'étude du droit positif sur ces thématiques[1828] démontre que les acteurs sont actuellement parfaitement ciblés, notamment car les régimes juridiques abordés sont en réaction à des faits juridiques particuliers. Ainsi, ces réglementations sont apparues de manière chronologique au fur et à mesure que les effets de l'informatique ont été démontrés, dans une approche libérale. Tel est le cas en matière de données personnelles en mettant en œuvre un principe de transparence et un droit d'accès aux données par les personnes physiques auprès des responsables du traitement[1829]. De la même manière, lorsque les plateformes en ligne sont accusées de manipulation par l'intermédiaire de recommandations, le législateur leur impose

[1826] Art. 3 § 1 du projet.
[1827] CRICHTON C., « Projet de règlement sur l'IA (I), des concepts larges retenus par la Commission », *op. cit.*
[1828] Il s'agit de la première partie de ces travaux, *Supra*., n° 72 et s.
[1829] *Supra*., n° 80 et s.

des obligations vis-à-vis des consommateurs[1830]. Dans ce cas de figure il s'agit surtout d'une transparence conditionnant le consentement des individus.

917. Et plus généralement, les décisions administratives individuelles prises sur le fondement d'un traitement algorithmique impliquent que l'administration soit en mesure d'expliquer les principales caractéristiques du traitement dès lors que l'intéressé en fait la demande[1831]. L'objectif poursuivi est ici de réduire le risque d'arbitraire de la part de l'administration.

918. Puis, parmi les régimes juridiques sectoriels étudiés, nous avons également constaté que la personne faisant l'objet d'un traitement de données n'était pas toujours au cœur de la transparence. C'est particulièrement le cas dans les régimes juridiques faisant intervenir des obligations d'informations de la part du concepteur du logiciel à son utilisateur (comme c'est le cas pour les outils d'aide à la prise de décision en matière médicale). Il en est de même concernant les constructeurs de véhicule à délégation de conduite ou de leur mandataire auprès de l'autorité de contrôle chargée d'assurer leur conformité[1832]. Le constructeur se voit bénéficier d'un droit d'accès aux données du véhicule quand celui-ci est en fonctionnement afin de constater qu'il fonctionne correctement, et le cas échéant améliorer la sécurité[1833]. Cela s'explique car cette transparence conditionne essentiellement la sécurité des personnes et la mise en jeu de la responsabilité.

919. Plus récemment, la proposition de règlement européen général au sujet de l'IA évoque quant à elle plusieurs acteurs de la chaîne algorithmique, ce qui n'est pas sans complexifier pour les personnes subissant ces systèmes l'identification des débiteurs des nouvelles obligations de transparence. Son ambition est de proposer d'uniformiser de nombreux régimes juridiques existants essentiellement au nom de la protection des droits fondamentaux. En cela, elle participe à une autonomisation de la transparence des traitements algorithmiques dans un but de respect des droits et libertés. Le projet concerne les opérateurs[1834], tels que les

[1830] *Supra.*, n° 260 et s.
[1831] *Supra.*, n° 404 et s.
[1832] *Supra.*, n°372 et s.
[1833] *Ibid.*
[1834] Art. 3 (8) du projet.

fournisseurs[1835], l'utilisateur[1836], le mandataire[1837], l'importateur[1838], et le distributeur[1839], ce qui n'est pas sans rappeler les acteurs traditionnels appréhendés par le droit de l'Union comme par exemple sur la réglementation relative à l'intermédiation entre professionnels[1840]. A ce titre, certains auteurs reprochent déjà la complexité de la distinction entre le fournisseur et l'utilisateur dans la mesure où elle empêcherait de saisir certaines réalités techniques comme en matière d'agent conversationnel[1841]. Ces logiciels sont notamment configurables et personnalisables par l'utilisateur. Ainsi, imposer des obligations d'information aux professionnels au sens large comme cela est le cas en droit de la consommation semblerait plus adapté pour le consommateur. Cela rappelle à quel point il convient d'être le plus général possible, puisqu'à défaut, la désignation d'une pluralité de débiteurs est contreproductive à l'effectivité d'une règlementation générale relative à la transparence de l'environnement numérique.

920. L'ambition du projet est pourtant de prendre en considération le plus d'acteurs possibles de façon à ce que les nouvelles obligations de transparence renforcent la confiance aussi bien des entreprises envers leurs clients que des administrations à l'encontre de leurs administrés[1842]. Toutefois, ces obligations que nous verrons ultérieurement ne s'appliquent pas à tous les systèmes d'IA[1843], mais surtout à ceux considérés comme étant à « *haut risque* »[1844].

921. Toutefois, les personnes subissant ces systèmes ne sont aucunement définies par le règlement, ce qui est dommageable. En effet, convient-il par exemple de considérer qu'un utilisateur, à qui pourtant s'appliquent de nouvelles obligations, n'est pas en situation de vulnérabilité vis-à-vis d'un outil dont le traitement lui échapperait, ne serait-ce car il ne peut

[1835] Selon l'article 3 (2) du projet, le fournisseur est « *une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit* ».
[1836] Art. 3 (3), l'utilisateur est 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 professionnel* ».
[1837] Art. 3 (5), le mandataire est « *toute personne physique ou morale établie dans l'Union ayant reçu mandat écrit d'un fournisseur de système d'IA pour s'acquitter en son nom des obligations et des procédures établies par le présent règlement* ».
[1838] Art. 3 (6), l'importateur est « *toute personne physique ou morale établie dans l'Union qui met sur le marché ou met en service un système d'IA qui porte le nom ou la marque d'une personne physique ou morale établie en dehors de l'Union* ».
[1839] Art. 3 (7), le distributeur est « *toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fournisseur ou l'importateur, qui met un système d'IA à disposition sur le marché de l'Union sans altérer ses propriétés* ».
[1840] Règlement UE 2019/1150 du Parlement Européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne. *Supra.*, n° 304 et s.
[1841] VEALE M., ZUIDERVEEN BORGESIUS F., « Demystifying the Draft EU Artificial Intellingence Act », *Computer Law Review International*, 2021, p. 97.
[1842] Proposition n° 2021/0106 (COD) 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, du 21 avril 2021, p. 10.
[1843] *Ibid.*, p. 9.
[1844] *Infra.*, n° 946 et s.

vérifier lui-même que les informations du fournisseur sont véridiques[1845] ? De la même manière, l'Etat doit-il également être considéré comme potentielle victime de ces systèmes, c'est-à-dire en situation de vulnérabilité ? Tel est par exemple le cas des traitements par l'exploration de données qui sont amenés à orienter les politiques publiques[1846].

922. La règlementation prévoit parfois qu'une transparence doit s'opérer auprès des régulateurs et non des personnes ou de la société. Il s'agit donc dans ce cas d'une transparence indirecte, mais cela ne veut pas dire pour autant que l'autorité de contrôle a la nécessité de communiquer ensuite dessus, quand bien même les secrets seraient protégés. Le projet précise à cet égard que le contrôleur qui devra être désigné est soumis à des obligations renforcées de confidentialité[1847]. Il ne faudrait pas que la levée des opacités des algorithmes se heurte de nouveau à une autre opacité : celle du contrôleur. Concernant la problématique de la symétrie informationnelle, c'est-à-dire s'assurer que l'information révélée par le débiteur à l'intéressé est véridique, elle devrait relever de fait de notre instance de contrôle unique que nous proposons dans l'immense majorité des cas[1848] en raison des secrets protégés par la loi. Et parfois, nous avons même proposé que pour certaines matières sensibles, ladite instance ait la charge d'effectuer cette transparence mais de manière indirecte, en tant que tiers de confiance. Cela implique dans cette hypothèse que pour exercer une transparence indirecte, les acteurs concernés aient également des obligations de transparence totale vis-à-vis de cette instance de contrôle au même titre que la réglementation sur le *trading algorithmique*[1849], et que cette dernière communique ensuite sous une forme intelligible à propos de ces systèmes.

2 - La nature et le degré de transparence

923. Comme nous l'avons vu, il existe des techniques juridiques plus traditionnelles participant à la transparence des traitements algorithmiques sans pour autant avoir été pensées pour cela initialement. Tel est le cas par exemple de l'allègement de la charge de la preuve, voire le cas échéant de son renversement[1850], qui peuvent être efficaces pour obtenir d'un acteur

[1845] Il est par ailleurs à noter que l'utilisateur qui va enrichir un système d'apprentissage avec des données peut pervertir le système volontairement ou non.
[1846] *Supra.*, n° 484 et s.
[1847] Proposition n° 2021/0106 (COD) 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, du 21 avril 2021, *op. cit.*, p. 11.
[1848] *Supra.*, n° 717 et s.
[1849] *Supra.*, n° 316 et s.
[1850] *Supra.*, n° 287 et 371.

des informations sur le fonctionnement des traitements. Tout comme le juge judiciaire bénéficie au titre de pouvoirs d'instruction prévus par l'article 145 du Code de procédure civile de la faculté d'obtenir la communication de documents techniques sur ces systèmes[1851]. L'obligation de publication de rapports réguliers et d'analyses d'impact est aussi une méthode pouvant éclairer les citoyens ou le pouvoir politique sur le comportement et les incidences des outils algorithmiques, ce qui n'a malheureusement pas été suffisamment le cas en matière de renseignement[1852] ou lors de la crise de la Covid-19[1853]. Mais il sera question ici de s'interroger sur les techniques propres à la compréhension des traitements.

924. La nature et le degré de transparence sont variables en fonction du déploiement du traitement. La transparence peut être préalable à la mise en œuvre du traitement, ou être *a posteriori* vis-à-vis des régulateurs ou des personnes subissant ces systèmes, ou intéressés au titre de leur qualité de justiciable.

925. Nous retrouvons toutefois parmi les régimes juridiques en vigueur ou en cours d'élaboration des approches communes même s'il convient de considérer que la transparence en tant que telle est un ensemble de techniques juridiques ne reposant pas sur une unité conceptuelle[1854]. Le même constat peut être effectué en matière de traitement algorithmique. Bien que les exceptions demeurent nombreuses, la communication du code source des logiciels utilisés par l'administration peut être sollicitée par les administrés, sans oublier la documentation afférente pour la comprendre. La LRN a également prévu une mention explicite informant l'intéressé qu'une décision administrative individuelle à son encontre est fondée sur un traitement algorithmique, ce qui permet ensuite le cas échéant de demander la communication des principales caractéristiques du traitement, que l'intéressé soit par ailleurs une personne physique ou morale[1855]. Et plus récemment, le RGPD, dans la continuité de la directive 95/46/CE et de la LIL de 1978, prévoit la communication d'un certain nombre d'informations lors de la collecte et du traitement des données personnelles. La nouvelle

---

[1851] *Supra*., n° 337.

[1852] En ce sens, comme l'indique la députée Paula Forteza il est à noter que les parlementaires ne bénéficient pas par exemple des informations suffisantes au sujet du déploiement des outils algorithmiques utilisés à titre expérimental dans le cadre de la loi renseignement. « *À ce jour, l'étude d'impact présentée par le gouvernement est très parcellaire du fait de la confidentialité de la technologie appliquée. Nous savons seulement que cette technologie a permis de générer 1739 alertes qui ont conduit à lever l'anonymat.* », FORTEZA P., L'utilisation des nouvelles technologies par les pouvoirs publics, *op. cit.*

[1853] Alors que le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommés « *Stopcovid* » prévoyait en son article 5 un rapport public du responsable de traitement sur le fonctionnement de l'application dans les trente jours suivant sa mise en œuvre, et au plus tard le 30 janvier 2021, le décret 2021-157 du 12 février 2021 est venu substituer à cette obligation une publication « *dans les trente jours suivant le terme de la mise en œuvre de l'application* », ce qui dénature la prétention initiale et cette forme de transparence.

[1854] KERLEO J-F., *La transparence en droit, Recherche sur la formation d'une culture juridique*, *op. cit.*

[1855] *Supra*., n° 407 et s.

règlementation sur les données personnelles prévoit même un droit à l'explicabilité des décisions automatisées portant sur ces données[1856]. Quant aux plateformes en ligne, les obligations de transparence sont plutôt générales, à travers la communication d'informations précontractuelles, voire contractuelles au titre de la loyauté, de la clarté et de la transparence sur « *sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder* » [1857] notamment.

926. Les techniques juridiques précitées et abordées tout au long de ces travaux ont pour objectif de concourir à une plus grande transparence de ces systèmes même si l'objectif poursuivi n'est pas forcément la compréhension du numérique dans un but de protection des droits et libertés. Elles peinent de plus à répondre aux nouveaux enjeux comme en matière d'IA.

927. C'est la raison pour laquelle la proposition de règlement européen sur l'IA prévoit des nouvelles techniques juridiques se superposant aux régimes juridiques existants et aux objectifs déjà poursuivis pour parvenir à l'intelligibilité de ces systèmes à des fins de respect des droits fondamentaux, de la santé, mais aussi pour assurer la sécurité juridique nécessaire au développement de ces outils[1858].

928. La transparence mise en œuvre par le règlement possède de plus des degrés divers en fonction du domaine d'intervention de la technologie. Cette nouvelle règlementation prévoit aussi que pour certains systèmes d'IA[1859], « *les fournisseurs veillent à ce que les systèmes d'IA destinés à interagir avec des personnes physiques soient conçus et développés de manière à ce que les personnes physiques soient informées qu'elles interagissent avec un système d'IA* »[1860]. Il serait également nécessaire de garder une trace de cette interaction pour démontrer par exemple le choix de l'utilisateur en cas de litige, et ce en vue de lutter contre les systèmes inéquitables numériques[1861]. Cette approche est primordiale puisqu'elle conditionne la connaissance de l'intervention d'un traitement, ouvrant ensuite la voie à des demandes d'information, voire à sa contestation devant une juridiction. Elle prévoit également pour

[1856] *Supra.*, n° 80 et s.
[1857] Supra., n° 266 et s.
[1858] Parmi les objectifs visés par cette proposition de règlement (hors annexe), nous retrouvons le respect des droits fondamentaux et des valeurs de l'Union. Cette volonté est affirmée par la Commission et le terme de « droits fondamentaux » est utilisé 78 fois dans le texte. La santé et la sécurité sont également associées à l'approche par les risques. La santé est utilisée 50 fois, tandis que la sécurité l'est 143 fois. Enfin, la sécurité juridique est également une priorité de l'Union pour assurer le développement de ces technologies, raison pour laquelle elle est citée 17 fois. Tel est donc le fondement de ce projet.
[1859] *Infra*., n° 946 et s.
[1860] Art. 52 du projet.
[1861] DANET A., ENGUEHARD C., « De la preuve et de l'utilisation des Systèmes Inéquitables Numériques », Les convergences du droit et du numérique, septembre 2017, Bordeaux, *INRIA* [en ligne]. [Consulté le 22 juin 2020]. Disponible à l'adresse : https://hal.inria.fr/hal-01730375/document

certains systèmes[1862] à haut risque leur inscription dans un registre[1863] géré par *« la Commission pour accroître la transparence, améliorer le contrôle public et renforcer le contrôle ex post par les autorités compétentes »*[1864], alors que le RGPD avait donné une place moins importante que la LIL de 1978 sur ce point[1865]. Cela permettrait, comme l'indique le CEPD, de fournir des informations au grand public sur les failles et incidents connus[1866].

929. Le projet de règlement européen inaugure une approche par les risques[1867] avec le déploiement de nouvelles techniques juridiques concourant directement ou indirectement à la transparence des traitements algorithmiques. Plus l'usage est risqué eu égard à son domaine d'intervention, plus les obligations de transparence sont renforcées. Ainsi, lorsque l'usage est à haut risque, il convient de s'assurer de la conformité au droit *ex ante*, c'est-à-dire avant son déploiement[1868], et ce conformément à une procédure d'évaluation[1869]. Plusieurs obligations doivent alors être respectées par le fournisseur[1870], telles que la mise en œuvre d'un système de gestion des risques incluant la tenue d'une documentation précise par ce dernier[1871]. Dans l'hypothèse où le système d'IA ferait appel à des données, il est également prévu l'élaboration d'une surveillance des modèles, des données, de la méthodologie, et ce afin d'assurer la détection des éventuels biais[1872]. A cela s'ajoute la confection d'une documentation technique standardisée[1873] qui devra être mise à jour[1874] ainsi que la conservation de la journalisation du traitement[1875]. Ces obligations permettent aussi bien à l'acteur du marché qu'au régulateur de donner des indications sur le fonctionnement du traitement et sa traçabilité.

930. D'autres obligations prévues par le projet portent davantage sur la communication d'informations aux personnes subissant ces systèmes[1876]. Dès lors, ces derniers seraient conçus et développés pour permettre aux utilisateurs d'interpréter les résultats du système et de les

[1862] *Infra.*, n° 946 et s.
[1863] Art. 60 du projet. En ce sens, nous avions déjà abordé la manière dont la tenue des registres concourait à une meilleure transparence auprès des autorités publiques.
[1864] *Ibid.*, p.16 du projet.
[1865] *Supra.*, n° 232 et s.
[1866] EDPB-EDPS, Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p. 19, *EDPB.europa.eu* [en ligne]. 18 juin 2021. [Consulté le 22 juillet 2021]. Disponible à l'adresse : https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf
[1867] Nous développerons ultérieurement, *Infra.*, n° 946 et s.
[1868] Art. 8 § 2 du projet.
[1869] *Ibid.*, Art. 19 et 43.
[1870] *Ibid.*, Art. 16 a.
[1871] *Ibid.*, Art. 9 et art. 17.
[1872] *Ibid.*, Art. 10.
[1873] *Ibid.*, Ces éléments sont précisés en annexe 4 du projet.
[1874] *Ibid.*, Art. 11 et art. 18.
[1875] *Ibid.*, Art. 12. Voir également art. 20.
[1876] *Ibid.*, Art. 13.

utiliser de manière appropriée[1877]. Un mode d'emploi comportant des informations concises, complètes, correctes, claires et intelligibles sur le traitement est à délivrer à l'utilisateur[1878].

931. Le fournisseur est tenu de déployer un système de surveillance humaine de celui-ci[1879]. Cette supervision a pour objectif de réduire la durée d'une éventuelle violation des droits et libertés[1880]. Nous considérons notamment que les obligations prévues à l'article 15 relatives à l'exactitude du système concourent à la transparence en ce qu'elles permettent de prévenir les erreurs, les défaillances et les biais du système[1881].

932. Il est intéressant de noter que certaines obligations du fournisseur sont à tenir vis-à-vis du régulateur, comme la notification d'un dysfonctionnement[1882]. Il est également question d'une coopération avec l'autorité de contrôle[1883]. Des documents doivent aussi être tenus à disposition d'une autorité de contrôle pour une durée de dix ans[1884], ainsi qu'une surveillance postérieure à la commercialisation du système, et ce toute sa vie[1885].

933. Certains systèmes d'IA, qui sont parfois des algorithmes auto-apprenants, font l'objet d'obligations particulières auprès de l'utilisateur professionnel qui dispose d'un devoir de pertinence et de qualité des données qu'il utilise. En effet, la qualité de ces données a une incidence sur les calculs opérés par le système, raison pour laquelle il est tenu de stocker les journaux d'événements générés automatiquement par le système[1886].

934. Concernant les algorithmes non régis par ces nouvelles obligations, car jugés à faible risque, ils seraient conditionnés à une transparence minimale, notamment par l'adoption de normes volontaires tels que les codes de conduite[1887].

935. Néanmoins, la communication d'une information générale ne permet pas pour la personne subissant ces systèmes de rejouer le traitement. C'est pour cette raison qu'il est parfois préférable de transmettre plus d'éléments directement à la personne concernée ou bien à l'autorité de contrôle qui devra ensuite effectuer un rôle de tiers de confiance. Le renforcement

[1877] *Ibid*., Art. 13 § 1.
[1878] *Ibid*., Art. 13 § 2. Ces mentions doivent comporter certaines précisions minimales telles que celles prévues à l'article 13 § 3.
[1879] *Ibid*., Art. 14.
[1880] *Ibid*., Art. 14 § 2.
[1881] *Ibid*., Art. 15.
[1882] *Ibid*., Art. 22 et art. 62.
[1883] *Ibid*., Art. 23.
[1884] *Ibid*., Art. 50, y compris ceux mentionnés à l'article 11 et 17.
[1885] *Ibid*., Art. 61.
[1886] *Ibid*., Art. 29.
[1887] Art. 69 du projet.

des audits et des certifications[1888] sont par ailleurs des techniques juridiques nécessaires à prendre en considération pour amoindrir le risque.

936. Des outils juridiques ont donc été pensés spécifiquement pour concourir à la transparence des traitements, mais encore faut-il les déployer correctement de manière la plus adéquate possible.

PARAGRAPHE 2 - Etude des différentes approches permettant d'appréhender les obligations de transparence

937. Après avoir dressé la nécessité de la neutralité technique des régimes juridiques généraux et les différentes techniques juridiques concourant à une meilleure transparence qu'il est souhaitable de retenir, deux principales approches nous semblent être pertinentes dans l'appréciation du degré et de la nature de la transparence et elles doivent donc nécessairement être combinées afin que la régulation de ces algorithmes ne soient pas lacunaires. Il s'agit de l'approche par la légitimité (A) et par les risques (B).

A - L'approche fondée par la légitimité

938. Pour l'heure, et dans l'esprit du libéralisme politique, la puissance de l'Etat ne peut être appréhendée de la même manière que les entités privées puisque même lorsqu'elle semble être affaiblie, l'Etat sait faire ressurgir sa force, notamment par la voie de son exorbitance du droit commun. La mission d'intérêt général dévolue à l'administration et aux représentants du peuple souverain implique toutefois un contrôle conséquent de leur action, ne serait-ce pour s'assurer que la plus grande force de l'Etat ne soit accaparée par des intérêts particuliers[1889]. Les secrets inhérents aux intérêts de la nation sont autant de menaces planant sur les droits et libertés, ce qui nécessite un contrôle renforcé de l'action publique, car il est dans certain cas un prétexte illégitime à l'opacité.

[1888] Art. 42 du RGPD et Art. 44 du projet de règlement sur l'IA.
[1889] Guy Héraud considère par exemple qu'il « *arrive pourtant qu'une conjuration de personnes et d'intérêts accumule une force qui menace l'Etat ou le régime. Cette force peut imposer aux pouvoirs établis des décisions qui, valant officiellement comme décisions de l'Etat, seront en fait l'expression de volontés particulières. Il se peut que l'Etat devienne, comme on l'a dit, la simple résultante des féodalités modernes* », HERAUD G., « La validité juridique », *op. cit.*, p. 481.

939. Quand bien même il est d'ores et déjà possible de constater que certains géants du numérique rivalisent à certains égards avec certaines prérogatives étatiques[1890], ce pouvoir n'est pas de même nature. En effet, lorsqu'une surveillance est opérée à des fins commerciales, même si elle est problématique vis-à-vis de la vie privée, la puissance publique bénéficie d'une exorbitance légitime puisqu'elle est l'outil permettant l'autonomie des citoyens en démocratie[1891]. Mais nous imaginons mal Facebook, sur la base des renseignements dont il dispose, déployer des forces de police et sa justice pour ensuite incarcérer un individu qui contreviendrait à ses conditions générales d'utilisation. Il ne s'agit pas de nier que les acteurs privés n'exercent pas par la voie des algorithmes des incidences sur la société, mais de reconnaitre que les incidences sur les individus ne sont pas à l'heure actuelle identiques entre ces deux entités. A moins qu'ils ne soient amenés à collaborer entre eux, voire à converger car leurs intérêts seraient communs. Il n'est donc pas possible que le droit saisisse le marché de la même façon qu'il appréhenderait l'Etat.

940. Nous avions indiqué que la constitutionnalisation du principe de transparence des traitements se devait d'être générale en ciblant aussi bien les acteurs publics que privés, car d'une part les administrations sont amenées à recourir à des algorithmes privés, ce qui implique de les contrôler, et d'autre part car l'incidence de cette source est qu'elle effectue une hiérarchisation entre différentes libertés, droits et principes, puisque nous estimons qu'ils ne peuvent tous être considérés à égalité. Cela ne veut nullement dire pour autant que la transparence applicable à l'administration serait de même nature et du même degré qu'à l'encontre des acteurs du marché. Certaines valeurs doivent effectivement primer sur d'autres, en particulier dans l'environnement numérique, et lorsque la transparence est une clé de voûte de l'ordre juridique, il convient que le secret ne puisse par exemple être opposé à l'Etat, justement parce qu'il est la force la plus légitime. Cela ne peut s'opérer qu'à la condition que suffisamment de garanties soient mises en œuvre pour que les gouvernants ne neutralisent le délicat équilibre institutionnel nécessaire à mettre en place[1892].

941. L'approche par la légitimité pose donc la question de la nature du contrôle. Dans le cadre de l'Etat, les personnes juridiques sont davantage susceptibles de demander des comptes à leur administration par l'intermédiaire d'un contrôle direct. La LRN a œuvré en ce sens, mais les exceptions demeurent nombreuses et ont même été accentuées au regard de l'action

[1890] PASQUALE F., From territorial to functional Sovereignty: The case of Amazon, *op. cit.*
[1891] *Supra.*, n° 634 et s.
[1892] Supra., n° 690 et s.

publique[1893]. En revanche, une transparence indirecte des opérateurs économiques effectuée par une autorité de contrôle semble plus opportune dès lors que ce travail est correctement opéré. C'est pour cela que dans le respect du droit des tiers, l'instance unique de contrôle des traitements algorithmiques que nous proposons pourra œuvrer à son effectivité, et ce en toute indépendance, notamment vis-à-vis des gouvernants.

942. Ce n'est donc pas seulement en fonction du risque d'une technique particulière ou d'un usage que l'on appréhende la nécessité de transparence, mais parce qu'il s'agit évidemment dans l'esprit de la DDHC que l'administration doit rendre compte[1894], notamment car l'exercice d'une telle force implique un contrôle renforcé pour qu'elle ne soit pas le cas échéant usurpée. Quelle que soit la technique utilisée, systèmes d'IA ou non, les algorithmes doivent être expliqués à chaque personne intéressée y compris en vue de pouvoir rejouer le traitement. Et lorsqu'interviennent certains secrets protégés, dont on comprend par ailleurs l'existence, c'est à l'instance de contrôle, avec du personnel habilité, qu'il conviendra d'effectuer ce contrôle et de transmettre ensuite au public les éléments communicables. Le problème est qu'aujourd'hui la multiplication des instances de contrôle nuit à l'effectivité des réglementations. Quoi qu'il arrive, la transparence sera réalisée, même si elle n'intervient que par la voie de cette instance qui pourra attester que les grandes caractéristiques communiquées par l'administration sont véridiques, et que la situation de l'intéressée a bien été calculée. En matière de renseignement, il existe naturellement des cas où le droit d'accès à certains fichiers de données personnelles est indirect pour les intéressés également[1895], ce qui limite par ailleurs l'exercice d'autres droits, comme celui de rectification des données collectées ou traitées. Dans cette hypothèse, un recours doit permettre que l'instance vérifie ensuite la véracité des informations détenues par l'administration, que les données soient personnelles ou non. Dans l'immense majorité de cas, la transparence devra donc être directe, tandis que dans quelques rares circonstances, comme dans le domaine de la défense nationale, les traitements seront vérifiés par des spécialistes en toute indépendance pour vérifier leur conformité au droit, même si elle ne pourra être effectuée par tous les acteurs de la société civile que nous avons abordés[1896]. Ce contrôle est d'autant plus nécessaire qu'il est une garantie pour l'Etat, à savoir le souverain, que l'administration et les gouvernants respectent bien le droit édicté.

[1893] Voir par exemple en ce sens les exceptions aux dispositions du CRPA dans le code de l'éducation au sujet de l'explicabilité de « *Parcoursup* » au regard des algorithmes locaux. *Supra.*, n° 468.
[1894] Art. 15 DDHC de 1789.
[1895] Certains fichiers jugés sensibles par l'Etat empêchent une consultation directe par l'intéressé. Tel est par exemple le cas des fichiers de renseignement dont la vérification va être opérée par un tiers de confiance étatique, en l'occurrence un magistrat de la CNIL. Voir en ce sens, art. 118 de la LIL de 1978 modifiée et *Supra*., n° 139 et s.
[1896] *Supra.*, n° 795 et s.

943. Toutefois, certains algorithmes privés sont également des outils utilisés pour obtenir un comportement particulier des masses, qu'il s'agisse du corps social ou des individus, le plus souvent à des fins marchandes[1897]. Dans cette approche, il n'est donc pas inenvisageable d'imposer également des obligations de transparence renforcées à certains acteurs, car les décisions prises par ces plateformes en ligne sont systémiques en ce qu'elles exercent une influence significative en matière de recommandation par exemple. Certaines règlementations s'y sont attelées, mais il convient d'aller plus loin, notamment par l'intermédiaire d'une transparence indirecte opérée par notre instance de contrôle de ces traitements et dont le secret ne lui serait pas opposable. Cela implique par conséquent que ces acteurs mettent à disposition toute la documentation permettant de comprendre le fonctionnement de ces traitements, ainsi que l'accès à ces derniers pour s'assurer de la véracité des déclarations, naturellement avec des précautions prises telles que l'intervention de médecins s'il est question de données de santé par exemple.

944. Ainsi, peu importe le concepteur, le fournisseur du logiciel, c'est parce que le logiciel est utilisé par l'administration qu'il implique la transparence. C'est donc dans la définition des besoins lors des marchés publics que l'administration devra exiger des prestataires la transparence, et que toute clause contraire serait illicite. Et s'il s'agit d'un développement interne, le logiciel devra d'autant plus respecter ces obligations. Si la transparence ne peut être effectuée, elle le sera par le tiers de confiance public indépendant étudié[1898]. Comme nous l'avons vu[1899], il convient de considérer le logiciel comme un acte d'interprétation du droit, dont il faut assurer la publicité. La transparence a vocation à s'appliquer, et ce quand bien même il s'agit d'une aide à la prise de décision, c'est-à-dire dont la décision est non fondée exclusivement sur l'algorithme. C'est pour cela que, comme nous le préconisons, une exigence de publication de rapports sur le comportement de l'administration devrait être respectée pour savoir si l'administration suit ces recommandations systématiquement[1900]. En effet, les raisonnements humains sont opaques, raison pour laquelle il existe des obligations de motivation dans certains cas, comme pour les décisions administratives individuelles, mais dès lors qu'un outil informatique exerce une influence sur une personne ou un groupe, il est impératif qu'il soit explicité, et ce même s'il s'agit d'une aide à la prise de décision. La

[1897] ZUBOFF S., *L'âge du capitalisme de surveillance. Le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, *op. cit.*
[1898] *Supra.*, n° 694 et s.
[1899] *Supra.*, n° 477 et s.
[1900] *Ibid.*

transparence apparaît alors comme une contrepartie à la substitution d'un raisonnement humain à un calcul informatique, ne serait-ce pour en garder le contrôle.

945. Tandis que pour l'approche privée, c'est davantage le caractère systémique, tel que le déclenchement d'un seuil, qui nous semble opportun, ce qui rejoint l'approche par les risques.

B - L'approche fondée par les risques

946. L'approche par les risques revêt plusieurs dimensions. Cette démarche a pour objectif de faire appliquer des obligations de transparence, voire l'exclusion d'usages algorithmiques, en fonction d'une échelle de risque préalablement évaluée. L'application d'un régime juridique en fonction du risque n'est pas nouvelle puisqu'elle était déjà par exemple préconisée dans des rapports canadiens[1901] et allemands[1902], et plus récemment dans le livre blanc de la Commission européenne[1903]. Cette logique est celle retenue par le projet de règlement européen visant les « *systèmes d'intelligence artificielle* ».

947. Comme le note Cécile Crichton « *réguler une technologie dont les applications sont hétérogènes suscite une difficulté fondamentale, qui réside dans l'approche à retenir. Alors que cette approche aurait pu être sectorielle (en fonction du secteur industriel concerné) ou juridique (en fonction de la branche du droit concernée), la Commission a privilégié une troisième option déjà pressentie par ses précédents écrits : une approche fondée sur les risques* »[1904].

948. Dans le cadre de cette proposition que nous avons fait le choix d'étudier pour mieux illustrer ce propos car il s'agit de la plus aboutie à ce jour, les niveaux de risques sont principalement établis au regard des incidences sur les droits fondamentaux et la sécurité[1905]. C'est donc en plus des objectifs que nous avons abordés tout au long de cette thèse par la

---

[1901] GOUVERNEMENT DU CANADA, Directive on Automated Decision-Making, *tbs-sct.gc.ca* [en ligne]. 01 avril 2021 [Consulté le 22 juin 2021]. Disponible à l'adresse : https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

[1902] DATEN ETHIK KOMMISSION, Opinion of the Data Ethics Commission, *datenethikkommission.de* [en ligne]. [Consulté le 2 juin 2021]. Disponible à l'adresse : https://datenethikkommission.de/wp-content/uploads/191023_DEK_Kurzfassung_en_bf.pdf

[1903] « *Les États membres font observer l'absence actuelle d'un cadre européen commun. La commission fédérale allemande pour l'éthique des données a préconisé un système de réglementation fondé sur cinq niveaux de risque, allant d'une absence de réglementation pour les systèmes d'IA les plus inoffensifs à une interdiction totale pour les plus dangereux.* », COMMISSION EUROPEENNE, Livre blanc. Intelligence Artificielle. Une approche européenne axée sur l'excellence et la confiance, *op. cit.*, p. 12.

[1904] CRICHTON C., « Projet de règlement sur l'IA (II), une approche fondée sur les risques », *Dalloz IP/IT*, 2021.

[1905] « *La proposition s'appuie sur les cadres juridiques existants et est proportionnée et nécessaire pour atteindre ses objectifs, car elle suit une approche fondée sur les risques et n'impose des charges réglementaires que lorsqu'un système d'IA est susceptible de présenter des risques élevés pour les droits fondamentaux et la sécurité* », p. 8 du projet.

règlementation et les techniques juridiques mises en œuvre pour y parvenir, que des nouvelles obligations de transparence vont non pas se substituer, mais s'ajouter pour poursuivre l'objectif de protection spécifique des droits et libertés, et le cas échéant de la conformité de ces systèmes à l'ordre juridique.

949. Cela nécessite donc une excellente cartographie de l'environnement numérique puisqu'à défaut aucune obligation ne s'appliquera aux acteurs[1906]. Une liste d'usage est alors établie afin de faire la distinction parmi les niveaux de cette échelle de risque. Le déclenchement de ces niveaux permettra notamment l'application particulière d'obligations relative à la transparence, et ce conformément aux outils juridiques de transparence précédemment étudiés[1907].

950. L'approche retenue peut être résumée sous forme de pyramide : à la base de cet édifice nous retrouvons les systèmes qui ne sont pas considérés comme étant à haut risque. Ils ne sont que très peu concernés par ces nouvelles obligations[1908]. Puis, plus nous nous rapprochons du sommet de cette dernière, plus le risque identifié est significatif et les obligations de transparence se renforcent[1909], voire l'usage y est strictement interdit[1910].

951. L'article 6 §1 du projet renvoie à une annexe[1911], divisée en sections, le soin de lister les domaines harmonisés au sein de l'Union considérés comme étant à haut risque en cas de recours à une IA, mais sous conditions. Ce n'est donc pas la simple intervention d'une IA dans l'un des domaines évoqués qui justifie qu'il soit qualifié de haut risque. Sont jugés à haut risque que les systèmes d'IA ayant vocation à être utilisés comme système de sécurité d'un produit ou est le produit lui-même conformément aux règlementations évoquées[1912]. Il en est de même si « *le produit dont le composant de sécurité est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une évaluation de la conformité par un tiers en vue de la mise sur le marché ou de la mise en service de ce produit conformément aux actes législatifs d'harmonisation de l'Union énumérés à l'annexe II* »[1913]. Sont concernés ce qui relève du

[1906] Les acteurs listés sont ceux vu précédemment, *Supra.*, n° 919.
[1907] *Supra.*, n° 961 et s.
[1908] « *Pour les systèmes d'IA qui ne sont pas à haut risque, seules des obligations de transparence très limitées sont imposées, par exemple en ce qui concerne la fourniture d'informations signalant l'utilisation d'un système d'IA lorsque celui-ci interagit avec des humains* », p. 8 du projet.
[1909] *« Pour les systèmes d'IA à haut risque, les exigences en matière de données de haute qualité, de documentation, de traçabilité, de transparence, de contrôle humain, d'exactitude et de robustesse se limitent au strict nécessaire pour atténuer les risques pour les droits fondamentaux et la sécurité qui sont associés à l'IA et qui ne sont pas couverts par d'autres cadres juridiques existants », ibid.*
[1910] Nous aborderons en détail l'interdiction stricte des usages plus tardivement. *Infra.*, n° 953 et s.
[1911] Annexe II du projet.
[1912] *Ibid.*, (a).
[1913] *Ibid.*, (b).

champ-d'application de la règlementation « *machines* », de la sécurité des jouets, des bateaux de plaisance et des véhicules nautiques à moteur, des ascenseurs ainsi que leurs composants de sécurité, les appareils et systèmes utilisés en atmosphères explosibles, la mise sur le marché d'équipement radioélectrique et d'équipement sous pression, les installations à câbles, les équipements de protection individuelle, les appareils à gaz, les dispositifs médicaux et de diagnostic *in vitro* (Section A). Quant à la section B de l'annexe, elle renvoie à l'aviation civile avec notamment la conception des aéronefs, y compris ceux sans pilote, les véhicules terrestres deux, trois roues ainsi que les quadricycles, les véhicules terrestres agricoles et forestiers, les équipements marins, le système ferroviaire, les véhicules terrestres à moteurs et les systèmes afférents.

952. Quant à l'article 6 § 2, il renvoie à une annexe énumérant des domaines dans lesquels le simple usage d'un système d'IA est suffisant à le qualifier de à haut risque, et donc il est indifférent que ces algorithmes interviennent dans un composant de sécurité par exemple. Ces domaines sont si sensibles que le fournisseur ou son mandataire a pour obligation d'enregistrer le système d'IA dans une base de données prévue par l'Union européenne[1914]. Nous y retrouvons les systèmes biométriques et la catégorisation des personnes, tels que la reconnaissance faciale, que le traitement ait par ailleurs lieu en temps réel ou *a posteriori*[1915] ; La gestion et l'exploitation des infrastructure critiques[1916] ; l'éducation et la formation professionnelle[1917] ; les relations entre l'employeur et les salariés ainsi que l'accès au travail indépendant[1918] ; l'accès et l'utilisation des services publics et privés considérés comme essentiels[1919] et ce qui se réfère à l'application de la loi[1920] ; mais aussi à la gestion de l'immigration, de l'asile et du contrôle aux frontières[1921].Pour finir, l'administration de la justice et des processus démocratiques figurent également dans cette liste, toutefois seuls les systèmes assistant l'autorité judiciaire aussi bien dans la recherche que dans l'application du droit aux faits[1922] sont pour l'heure visés par des obligations de transparence. La commission se réserve néanmoins la possibilité de modifier spécifiquement cette annexe par des actes délégués[1923].

[1914] Art. 51 du projet.
[1915] Annexe III § 1.
[1916] *Ibid*., § 2.
[1917] *Ibid*., § 3.
[1918] *Ibid*., § 4.
[1919] *Ibid*., § 5.
[1920] *Ibid*., § 6.
[1921] *Ibid*., § 7.
[1922] *Ibid*., § 8.
[1923] Dans les conditions prévues à l'art. 7 du projet.

953. La proposition aborde également pour l'heure quatre cas d'usages en matière d'IA faisant l'objet d'une stricte interdiction[1924]. Tel est le cas des systèmes qui mettraient en œuvre des techniques subliminales ayant pour conséquence de modifier le comportement d'une personne physique qui cause ou est susceptible de causer, y compris à un tiers, un préjudice physique ou psychologique[1925]. Il en est de même si le système utilise les vulnérabilités d'un groupe de personnes en raison de leur âge ou de leur handicap, « *pour altérer substantiellement le comportement d'un membre de ce groupe d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique* »[1926]. Est également exclu de la mise sur le marché ou pour le compte d'un Etat un système de crédit social, comme instauré en République Populaire de Chine[1927]. Le dernier usage évoqué est toutefois soumis à des exceptions puisque sont prohibés par principe les traitements d'identification biométriques effectués au sein de l'espace public[1928], sauf s'ils permettent de rechercher des potentielles victimes de la criminalité ou des enfants disparus[1929], de prévenir des menaces substantielles et imminentes pour la vie ou la sécurité des personnes, y compris en matière d'attaque terroriste[1930] ainsi que la détection, la localisation ou la poursuite d'auteurs ou de suspects de certaines infractions pénales[1931]. Ces exceptions ne peuvent toutefois être mises en œuvre sauf urgence que sous certaines conditions telles que l'autorisation d'une autorité administrative indépendante ou de l'autorité judiciaire[1932] dans les modalités définies par le droit national[1933].

954. Il est à noter que certaines technologies peuvent notamment faire l'objet d'un régime juridique spécifique. Telle est aussi l'approche du projet de règlement européen[1934], mais à la marge de sa logique générale précédemment abordée. C'est donc parce qu'une technologie en particulier est jugée sensible qu'un régime juridique de transparence renforcée va s'appliquer en supplément des obligations déjà prévues au titre III du règlement[1935], et ce quand bien même le domaine est à faible risque. En ce sens, l'article 52 évoque précisément une transparence spécifique sauf exception[1936] pour certaines méthodes d'IA, à savoir les systèmes interagissant

[1924] Art. 5 du projet.
[1925] *Ibid*., § 1 (a).
[1926] *Ibid*., (b).
[1927] *Ibid*., (c).
[1928] *Ibid*., (d).
[1929] *Ibid*., i.
[1930] *Ibid*., ii.
[1931] *Ibid*., iii.
[1932] Art. 5 § 3.
[1933] Art. 5 § 4.
[1934] Art. 52.
[1935] *Supra.*, n° 951 et s.
[1936] En ce sens, voir art. 52.

avec les personnes physiques (bot)[1937], les dispositifs reconnaissance biométrique comportant la reconnaissance d'émotions[1938] ou portant sur « *des images ou des contenus audio ou vidéo présentant une ressemblance avec des personnes, des objets, des lieux ou d'autres entités ou événements existants et pouvant être perçus à tort comme authentiques ou véridiques (« hypertrucage »)* »[1939]. Néanmoins, de nombreuses exceptions sont à relever. Dans l'hypothèse de la reconnaissance biométrique, si elle est utilisée « *à des fins de prévention et de détection des infractions pénales et d'enquêtes* », l'obligation d'information du fonctionnement dudit systèmes aux personnes exposées n'est pas applicable[1940]. Dans son avis, le CEPD considère à cet égard que de telles exceptions pour des systèmes à haut risque sont trop larges en plus de constituer une incitation à l'usage[1941]. Le Comité se prononce par ailleurs pour l'interdiction de la reconnaissance d'émotions qu'elle juge trop intrusive sauf à des fins de santé ou de recherche[1942].

955. Il s'agit donc finalement d'une régulation du marché qui ne prend pas en considération de nombreux domaines très sensibles comme la défense ou la sécurité nationale puisqu'ils demeurent de la compétence des Etats, ce qui démontre par ailleurs que l'Union européenne, sous sa forme actuelle, ne pourra convenablement réguler de tels usages, alors que, par exemple, les droits et libertés pourraient être fortement impactés par de tels systèmes.

956. De plus, à l'instar des règlementations européennes étudiées dans le cadre de ces travaux comme le RGPD, les exceptions demeurent nombreuses[1943], notamment car le libéralisme économique prime dans certains cas sur les obligations de transparence[1944]. Or, que la transparence soit effectuée directement vis-à-vis des personnes[1945] ou indirectement par l'intermédiaire d'un tiers de confiance, cela affecte ses chances de constater l'ampleur de la violation de ses droits. La proposition de règlement n'aborde pas la qualité ou la nature de

[1937] *Ibid*., § 1.
[1938] *Ibid*., § 2 du projet.
[1939] Art. 52 § 3.
[1940] Art. 52 § 2.
[1941] EDPB-EDPS, Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *op. cit*., § 70.
[1942] *Ibid*., § 35.
[1943] *Ibid*.
[1944] « *Les obligations en matière de renforcement de la transparence ne porteront pas non plus atteinte de manière disproportionnée au droit à la protection de la propriété intellectuelle (article 17, paragraphe 2), puisqu'elles seront limitées aux informations strictement nécessaires pour permettre aux personnes d'exercer leur droit à un recours effectif et à la transparence requise de la part des autorités de contrôle et d'exécution, conformément à leurs mandats. Toute divulgation d'informations sera effectuée conformément à la législation en vigueur dans le domaine concerné, notamment la directive 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites. Lorsque les autorités publiques et les organismes notifiés doivent avoir accès à des informations confidentielles ou à un code source pour vérifier le respect d'obligations essentielles, ils sont soumis à des obligations de confidentialité contraignantes* », p. 13 du projet.
[1945] Art. 70 et art. 17 § 2 du projet.

l'information que les autorités de contrôle vont effectuer auprès du public[1946]. Quand bien même il existe une transparence minimale pour que les personnes puissent exercer leur droit à un recours effectif, il convient de reconnaître que nous aurions préféré que ce soit à l'autorité de contrôle d'établir ce qui est à considérer comme minimal et non à l'acteur soumis à ces obligations de les apprécier. Il est en effet tentant pour le débiteur de ces obligations d'occulter certaines informations pour éviter des éventuelles poursuites, même si l'autorité de contrôle pourra *a posteriori* confronter ces éléments et infliger le cas échéant des sanctions. Mais pour cela, faut-il encore que ces autorités bénéficient des moyens suffisants pour y parvenir.

957. La transparence des traitements est la clé de voûte du respect des droits et libertés, et donc la condition *sine qua non* du déploiement sans risque de ces systèmes. Mais ce principe ne peut être une fin en soi car d'une part, quand bien même un usage est entièrement expliqué et contrôlé, le recours à la technologie n'en demeure pas moins problématique, ne serait-ce car la transparence permet surtout de constater la nature du fait juridique afin de le soumettre ensuite au régime juridique adéquat. Et d'autre part, de manière paradoxale, un système opaque, utilisé dans un secteur dont l'usage n'a potentiellement que très peu d'incidences juridiques, ne nécessite pas d'exigence de clarté particulière.

958. Il s'agit donc d'une ambivalence à corriger. En ce sens, l'approche par le risque est intéressante sans être irréprochable. C'est pour cette raison qu'il convient d'interdire certains usages et de combiner les différentes approches étudiées, ce que ne parvient pas suffisamment à effectuer le projet de règlement à notre sens.

SECTION 2 - LES LIMITES AU PRINCIPE DE TRANSPARENCE DES TRAITEMENTS ALGORITHMIQUES

959. Bien que le principe de transparence des traitements algorithmiques soit essentiel pour les raisons évoquées tout au long de ces travaux, force est de reconnaître qu'il ne saurait résoudre toutes les difficultés inhérentes au numérique. L'objectif primaire de la transparence est l'observation des faits juridiques induits par le numérique en prenant connaissance du positionnement des puissances au sein de cyberespace, afin de saisir notamment l'étendue des

[1946] En effet, le CEPD précise dans son avis sur la proposition de règlement que lorsque le secret s'oppose à une communication directe de certaines informations, ces systèmes doivent faire l'objet d'une inscription particulière dans un registre afin qu'ils puissent être surveillés par une autorité de contrôle compétente pour assurer sa transparence. Voir en ce sens, EDPB-EDPS, Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *op. cit.*, § 71.

violations des droits et libertés. Mais son accomplissement ne peut légitimer à lui seul le recours à des technologies. Ce n'est donc pas parce qu'une technologie serait à la fois transparente d'un point de vue juridique que technique qu'il devrait en légitimer l'usage.

960. Nous nous efforçons cependant à proposer une classification générale relative à la transparence des traitements et à l'exclusion des traitements (Paragraphe 1), sans négliger qu'au-delà de la réforme institutionnelle proposée censée restaurer l'équilibre des pouvoirs dans un monde de plus en plus numérique[1947], le principe de transparence se doit être complété par un principe de participation des citoyens aux décisions numériques (Paragraphe 2).

PARAGRAPHE 1 - Essai de classification générale relative à la transparence et l'exclusion des traitements

961. Comme nous l'avons vu, la régulation des traitements algorithmiques peut s'opérer par des approches relatives aux risques ou à la légitimité[1948]. Mais le projet de règlement européen, qui est par ailleurs la première règlementation à aborder l'approche par le risque en la matière, comporte une importante lacune ; à savoir la volonté de réguler avant tout le marché en se souciant assez peu des risques engendrés par les usages algorithmiques de la puissance publique. Cette ambition européenne ne peut donc en l'état être pleinement satisfaisante puisqu'elle fait fi de l'approche par la légitimité. En effet, la puissance de l'Etat ne peut être appréhendée de la même manière que les puissances privées[1949]. Nous ne reviendrons cependant pas en détail sur la régulation du marché, déjà longuement détaillée et opérée dans l'étude du projet de règlement européen.

962. La combinaison de l'approche par la légitimité et le risque nous impose par conséquent deux régimes juridiques distincts. D'une part, il convient donc de convenir d'une approche par le risque pour le marché, et d'autre part, pour la puissance publique. Dans cette hypothèse, il est opportun de se focaliser sur un régime spécifique de transparence pour l'action publique, ce que ne prend pas en compte le projet de règlement (A) et de l'autre une réflexion plus approfondie au sujet de l'exclusion de certains usages (B), car quand bien même la transparence serait absolue, elle n'a pas vocation à légitimer des technologies liberticides.

[1947] *Supra.*, n° 690 et s.
[1948] *Supra.*, n° 937 et s.
[1949] *Supra.*, n° 613 et s.

A - De la nécessaire transparence spécifique à l'action publique

963. L'approche par le risque ne peut être générique. En effet, des exclusions ou des obligations de transparence accrues peuvent avoir lieu dans l'administration et non dans le secteur privé, ce que ne fait pas le règlement européen. Il conviendrait donc davantage de réaliser deux pyramides, c'est-à-dire un risque établi en fonction de la légitimité de la puissance de l'Etat qui de fait engendre un risque sur les individus et groupes, et une autre correspondant au marché telle que proposée par la Commission.

964. Il serait intéressant à notre sens de préciser davantage l'approche par le risque dans le cadre spécifique de l'action administrative puisque ce n'est pas celle explorée par le projet de règlement. Dans une approche sectorielle, contrairement au projet de règlement européen qui se veut général, un rapport de l'ENA avait déjà évoqué une démarche spécifique par le risque en matière d'« *éthique et de responsabilité des algorithmes publics* »[1950], proposition que nous souhaitons combiner par une approche par la légitimité. Et c'est aussi la raison pour laquelle certains auteurs, comme Jean-François Kerléo, se prononcent en faveur de la constitutionnalisation d'un principe de transparence de la vie publique[1951].

965. Nous considérons pour les raisons évoquées que la transparence directe doit être privilégiée vis-à-vis de l'Etat, et ce quel que soit le risque sur les droits et libertés ou la société en général, car son action est légitimée par la poursuite de l'intérêt général. Il convient donc que cette transparence soit du plus haut degré, surtout lorsqu'il y a usage de prérogatives de puissance publique, comme pour les collectes et les traitements de données obligatoires, mais ce dans le respect de la vie privée des tiers. A minima, le caractère indirect de la transparence implique que notre commission unique est tenue et habilitée à vérifier les informations déclarées par l'administration. C'est effectivement parce que la puissance de l'Etat légitime de tels traitements qu'il est impératif d'attendre en retour des garanties de transparence.

966. Dans les hypothèses où une transparence directe s'opérerait, les personnes concernées ou la société, par l'intermédiaire de la société civile, pourraient accéder au code source, à la documentation afférente, et pourraient solliciter l'autorité de contrôle pour qu'elle s'assure que le code source communiqué est par exemple conforme au logiciel utilisé par l'administration.

[1950] RAPPORT ENA, Ethique et responsabilité des algorithmes publics, annexe 3, p. 30, *Etalab.gouv.fr* [en ligne]. Juin 2019. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https://www.etalab.gouv.fr/wp-content/uploads/2020/01/Rapport-ENA-Ethique-et-responsabilit%C3%A9-des-algorithmes-publics.pdf

[1951] Voir en ce sens, KERLEO J-F., « La constitutionnalisation d'un principe de transparence de la vie publique », *ADJA*, 2020. *Supra.*, n° 675.

Les systèmes les plus risqués exigeraient des autorisations pour leur déploiement, y compris dans certains cas une consultation démocratique voire un scrutin, des audits réguliers et la tenue de la conservation de registre pour une meilleure effectivité des contrôles.

967. Dans la continuité de la jurisprudence du Conseil constitutionnel[1952], lorsqu'une décision automatisée administrative individuelle fait intervenir des technologies auto-apprenantes et a des effets juridiques sur les personnes, est imposée l'explication de toutes les étapes du traitement, de façon à ce que le responsable du traitement soit en mesure de le vérifier. Il est par ailleurs impératif d'aller plus loin au sujet de la transparence des traitements ne faisant pas intervenir de données personnelles, ou des données anonymisées, puisqu'elles sont susceptibles d'exercer une influence sur la prise de décision. Le rapport Tricot déclarait dès 1975 lorsqu'il se penchait sur une réglementation des données personnelles *« que nous serons sans doute amenés à nous interroger sur la possibilité et l'intérêt de consacrer d'autres libertés, telles que celles pour l'homme et les groupements de connaître les informations enregistrées à leur sujet et de pouvoir les discuter* »[1953].

968. C'est pour cette raison que nous préconisions que l'administration communique obligatoirement, sous forme de rapport annuel, des statistiques sur ces outils de recommandation, qui certes ne prennent pas de décision, mais sont susceptibles d'influencer l'agent administratif dans son jugement. S'il s'avère que la recommandation est suivie dans l'immense majorité des cas, l'agent ne pourrait pas faire écran vis-à-vis de l'algorithme, ce qui permettrait également de contester l'algorithme, dans le cadre d'un contrôle de légalité par exemple.

969. De la même manière, lorsque l'Etat ou ses représentants utilisent des technologies ayant des incidences sur les libertés ou la société, et donc pouvant desservir les intérêts de la Nation, ils doivent être dans l'obligation de solliciter une transparence vis-à-vis du fournisseur notamment pour pallier les potentielles vulnérabilités à leur encontre[1954]. En effet, ses services, et le cas échéant avec l'aide du tiers de confiance que nous avons souhaité instituer, seraient tenus d'évaluer les caractéristiques et les données utilisées par le système. Tel serait particulièrement le cas des logiciels utilisés en matière d'exploration des données lors de grandes consultations de nature politique, et qui ont ensuite des conséquences juridiques, ou

[1952] CC, décision n° 2018-765 DC, 12 juin 2018, Loi relative à la protection des données personnelles, § 70 et § 71.
[1953] Rapport de la Commission informatique et libertés, la documentation française, 1975, p. 20.
[1954] DOUVILLE T., HERVOCHON C., NOEL E., PAQUIER Y., « Les vulnérabilités numériques », *op. cit.*, p. 117.

celles qui relèveraient de prédictions comme dans le cadre d'une pandémie ou des outils de *trading* qui peuvent affecter l'économie d'une nation, voire de l'humanité[1955]. Il en est de même lorsque les algorithmes jouent un rôle en matière d'évaluation des politiques publiques, puisque s'ils sont erronés ou parcellaires dans les modélisations utilisées, ils sont susceptibles de mettre fin à tort à certaines politiques au nom d'une prétendue « scientificité ». En effet, en informatique, ce qui n'est pas dans le modèle algorithmique est hors modèle et ne pourra donc être pris en compte. Il convient de démontrer que certains outils présentés comme impartiaux ne sont autre que des impostures.

970. Concernant la participation à la vie démocratique, nous rejoignons la prise de position de Eric Buge et Camille Morio disposant que « (…) *La sincérité implique notamment, en matière de décision publique, la reconnaissance d'un principe de transparence. Cette dernière concerne les modalités de la consultation, qui doivent être publiquement explicitées. Elle doit aussi porter sur ses résultats, qui appartiennent tant au commanditaire de la consultation qu'au public qui y a participé. Un principe d'open data est donc à affirmer. Enfin, s'agissant spécifiquement des plateformes numériques utilisées par les pouvoirs publics, la garantie minimale voudrait que, dans un domaine qui touche à l'exercice de la démocratie, les algorithmes sous-jacents (codes source) soient accessibles et étudiables, c'est-à-dire publiés en open source* »[1956]. Il est aussi nécessaire que des missions de surveillance diligentées par notre autorité de contrôle indépendante soit chargées de vérifier leur analyse, y compris quand cette tâche est déléguée à des personnes privées comme cela a été cas dans le cadre du grand débat[1957]. Parallèlement, et à titre préventif, cette approche par les risques et sur le fondement de la légitimité devrait nous amener, comme le préconise le défenseur des droits, à « *réviser le seuil d'évaluation des marchés publics informatiques et d'intégrer à leur contrôle au-delà des seuls aspects budgétaires, une appréciation des risques de discrimination, et plus généralement d'atteinte aux libertés et droits fondamentaux* »[1958].

971. Quant à la transparence des traitements du marché à laquelle il est moins question de s'étendre car le règlement européen y consacre un régime juridique complet, il convient davantage de la considérer de manière indirecte vis-à-vis des personnes, à la condition que le

[1955] AÏT-KACIMI N., Trading : les « robots » rechignent à livrer leurs secrets au régulateur, *Les Echos* [en ligne]. 14 novembre 2019. [Consulté le 26 février 2020]. Disponible à l'adresse : https://www.lesechos.fr/finance-marches/marches-financiers/les-robots-rechignent-a-livrer-leurs-secrets-au-regulateur-1147749
[1956] Voir en ce sens, BUGE E., MORIO C., « Le Grand débat national, apports et limites pour la participation citoyenne », *op. cit.*, p. 1205.
[1957] *Supra.*, n° 487 et s.
[1958] DEFENSEUR DES DROITS, Rapport, Technologies biométriques : l'impératif respect des droits fondamentaux, 2021, p.19.

contrôle étatique soit suffisant. Cela n'empêche nullement, comme dans le cadre du règlement européen, qu'une transparence d'une autre nature, c'est-à-dire faisant référence davantage à l'intelligibilité, à l'explication des principales caractéristiques, soit opérée vis-à-vis des personnes, qu'elles soient physiques ou morales dès lors que ces informations sont vérifiées par ledit tiers de confiance. Dans le cadre de la régulation du marché, la nature et le degré de transparence en fonction des usages nous semble être une assez bonne avancée, raison pour laquelle nous n'y reviendrons pas dès lors que le tiers de confiance institué est fiable et lui-même transparent sur les missions qu'il effectue[1959].

972. Mais la transparence ne saurait justifier pour autant tous les usages technologiques. Ce principe ne peut faire l'impasse sur l'acceptabilité, ne serait-ce car sa raison d'être juridique est de pouvoir observer le positionnement des puissances. En ce sens, il est la clé de voûte de l'ordre juridique et participe notamment à assurer la publicité des normes étatiques et privées. La crainte est donc de constater que ce principe est utilisé à d'autres fins, dont de légitimation d'un usage attentatoire aux libertés. La transparence n'est là que pour s'efforcer à comprendre le fonctionnement de ces outils.

973. Ainsi, au-delà de la transparence, l'acceptation d'une technologie peut être subordonnée à des conditions particulières, ou à défaut à une stricte exclusion d'un usage.

B - Conditionnalité et exclusion ferme des traitements algorithmiques

974. Quand bien même la transparence de ces systèmes serait absolue, certains usages algorithmiques doivent soit faire l'objet de garanties particulières, soit d'une exclusion. Ce que nous appelons conditionnalité est l'acceptation d'un usage sous réserve qu'il remplisse des garanties autres qu'en matière de transparence. Mais cela implique une excellente connaissance de la technologie utilisée afin de s'assurer que dans les faits, elle respecte les objectifs fixés en démocratie. A titre d'exemple, une architecture technique ou un design logiciel serait autorisé parce qu'il est plus respectueux de l'environnement qu'un autre[1960]. Il pourrait s'agir également

[1959] *« Le ministre de l'Intérieur a tenté, fin 2020, d'échapper à une sanction de la Cnil qui enquêtait sur cette surveillance illégale. Il a surtout réclamé que cette sanction, une fois prononcée, soit dissimulée aux citoyens et aux parlementaires. »*, LE FOLL C., POURE C., Drones : comment Gérald Darmanin a voulu échapper à toute sanction, *Mediapart* [en ligne]. 8 mai 2021 [Consulté le 2 juin 2021]. Disponible à l'adresse : https://www.mediapart.fr/journal/france/080521/drones-comment-gerald-darmanin-voulu-echapper-toute-sanction

[1960] MATHIS B., « Faut-il réglementer les crypto-actifs en fonction de leur consommation d'électricité », *Revue internationale des services financiers*, 2020, p. 59 à 62.

d'autoriser le recours à des algorithmes dès lors qu'il existe un interlocuteur humain, comme en matière d'accès à un service public. En d'autres termes, il ne serait pas possible qu'une administration dématérialise exclusivement toutes ses procédures ou l'accueil du public. La conditionnalité peut aussi impliquer qu'un usage soit autorisé à la seule condition qu'il s'agit d'une gestion purement publique, voire nécessitant le recours à des logiciels libres et ouverts. Tel serait le cas d'une plateforme publique offrant plus de garantie qu'une gestion privée comme cela est actuellement le cas avec le « *Health data hub* »[1961], car au-delà des impératifs de transparence, c'est prendre le risque que des données ne soient transmises à d'autres opérateurs à des fins commerciales, et ce même illicitement.

975. Il en est de même dans le cadre du renseignement où de nombreux logiciels privés américains sont utilisés et détournés en tant que cheval de Troie. Le logiciel libre utilisé par l'Etat, même s'il est parfois moins efficace, offre au moins une meilleure compréhension de ce dernier et la garantie qu'il ne sera pas détourné à d'autres fins, car rappelons-le, l'univers numérique n'est pas si facilement observable techniquement. Le logiciel est une partie importante en matière de souveraineté, mais il convient également de considérer que dans des domaines très particuliers, car sensibles, il est préférable de conditionner notamment un usage par le recours à un matériel informatique conçu et produit en France. Puisque comme nous l'avons déjà abordé[1962], le traitement algorithmique implique l'exécution d'un code source par un ordinateur qui lui-même est susceptible de contourner le logiciel, aussi transparent soit-il. En ce sens, certains usages doivent donc être conditionnés à des garanties de bout en bout, de la conception du logiciel à celle de l'ordinateur.

976. Quant à l'exclusion, elle doit parfois être stricte du fait du domaine d'intervention ou en fonction de la technologie utilisée, car l'usage ne peut du fait de sa nature offrir des garanties suffisantes et engendre un risque trop important sur la société et les libertés. L'exclusion des usages algorithmiques n'est pas une approche nouvelle. L'étude des premiers régimes juridiques nous apprend, comme dans de nombreux domaines, que la LIL de 1978 prévoyait qu'au-delà de la transparence des traitements tel que le droit d'accès à ses données nominatives, certains usages devaient toutefois être prohibés. L'article 2 de la LIL[1963] disposait dès 1978 qu'« *aucune décision de justice impliquant une appréciation sur un comportement humain ne*

[1961] Pour plus de précisions au sujet du « *Health data hub* », *Supra.*, n° 631 et s.
[1962] *Supra.*, n° 13.
[1963] Art. 47 modifié et art. 2 ancien de la LIL de 1978.

peut avoir lieu pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité ».

977. Il en était de même concernant les décisions administratives ou privées prises sur le fondement d'un profilage opéré par un traitement automatisé[1964]. Mais la tentation du recours à l'informatique, y compris pour combler la faiblesse de moyens matériels et humains, a conduit à ce que des systèmes automatisés privés ou publics puissent s'y substituer, sous réserve d'une certaine transparence[1965], comme si cette dernière légitimait à elle seule l'usage autrefois interdit pour des motifs de préservation des droits et libertés.

978. Il apparait donc que, compte tenu des nouvelles technologies pourtant parfois séduisantes, il faille recourir davantage à l'interdiction de certains usages. Le projet de règlement européen esquisse cette éventualité, mais manque à notre sens d'ambition, surtout concernant l'exclusion des usages relatifs à la vie démocratique ou à l'action administrative, sans doute car l'approche par la légitimité n'a pas été combinée avec celle par les risques. Et comme nous l'avons abordé, l'approche par les risques nécessite une excellente cartographie des domaines d'intervention des traitements algorithmiques, ce qui peine à être satisfaisant dans le projet de la Commission. L'avis du CEPD sur ladite proposition évoque de plus à juste titre que l'information est difficile à apporter quant aux systèmes d'IA et qu'il conviendrait davantage de « *promouvoir de nouvelles manières plus proactives et opportunes d'informer les utilisateurs des systèmes d'IA du statut (de décision) dans lequel se trouve le système à tout moment, en les avertissant rapidement des conséquences potentiellement néfastes, de sorte que les personnes dont les droits et libertés peuvent être altérés par les décisions autonomes de la machine peuvent réagir, ou redresser la décision* »[1966]. La transparence n'est toutefois pas simplement qu'une question de volonté, mais aussi de faisabilité technique. A l'évidence puisque l'immixtion de ces technologies dans des usages trop sensibles ne saurait offrir des garanties suffisantes de transparence et de respect des exigences démocratiques en général, leur exclusion est nécessaire dans de nombreux domaines.

[1964] Art. 2 ancien de la LIL de 1978.
[1965] Art. 42 al. 2 de la LIL de 1978 modifiée. Voir également en ce sens, CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*, § 70 et § 71. Pour plus de précisions, *Supra.*, n° 435 et s.
[1966] Traduit de l'anglais, « *The Regulation should promote new, more proactive and timely ways to inform users of AI systems on the (decision-making) status where the system lays at any time, providing early warning of potential harmful outcomes, so that individuals whose right and freedoms may be impaired by machine's autonomous decisions may react, or redress the decision* », EDPB-EDPS, Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *op. cit.*, § 72.

979. Il est également possible de trouver trace dans le code pénal de pratiques répréhensibles, car fondées sur la collecte de données non seulement personnelles mais pluripersonnelles tels que les tests génétiques récréatifs[1967]. C'est la dimension collective de la collecte et du traitement qui est dangereuse et justifie son interdiction. En effet, la collecte d'un ADN n'engage pas seulement la personne concernée, puisqu'elle permet notamment l'identification de plusieurs individus, voire d'un groupe ethnique, sans que ces derniers n'aient à donner leur consentement[1968]. De plus, le traitement illicite d'une telle information serait irréversible en ce que nous ne pouvons modifier notre ADN contrairement à des données d'une autre nature tels qu'un numéro de téléphone ou une adresse postale.

980. L'immixtion des algorithmes dans le cadre de la prévention des atteintes à l'ordre public ou à la recherche des auteurs d'infraction est par ailleurs un domaine très sensible. A titre d'exemple, le caractère systémique de la surveillance des télécommunications opérée par ces nouveaux outils laisse à penser que le glissement d'une surveillance de masse vers une surveillance généralisée relève davantage d'une simple différence de degré que de nature. Sans surprise, la Cour EDH ne s'oppose pas à une telle surveillance de masse au motif qu'il y aurait une prolifération des menaces, notamment permis par l'environnement numérique[1969]. Au nom des marges d'appréciation des Etats, l'absence de contrôle de nécessité ouvre la voie à des usages liberticides, et ce quand bien même des garanties seraient posées par l'intermédiaire d'un contrôle de proportionnalité[1970]. Or, c'est la nature de ces techniques qui les rend intrusives, ces outils n'étant pas neutres puisqu'ils sont conçus pour détecter un très grand nombre de données sans le moindre discernement. Certes, il est possible de penser des garanties sur la procédure de déploiement de ces outils, mais nullement sur le traitement lui-même, dans la mesure où ils progressent sans la connaissance de notre tradition juridique.

[1967] L'article L. 226-28-1 du Code pénal dispose que « *Le fait, pour une personne, de solliciter l'examen de ses caractéristiques génétiques ou de celles d'un tiers ou l'identification d'une personne par ses empreintes génétiques en dehors des conditions prévues par la loi est puni de 3 750 € d'amende* ».

[1968] CHATELLLIER R., Des tests génétiques dits récréatifs, mais pas inoffensifs, *Linc.cnil.fr* [en ligne]. 13 septembre 2018. [Consulté le 2 octobre 2020]. Disponible à l'adresse : https://linc.cnil.fr/fr/des-tests-genetiques-dits-recreatifs-mais-pas-inoffensifs#:~:text=En%20France%2C%20ce%20type%20de,'un%20tiers%2C%20ou%20l'

[1969] Cour EDH, Big brother watch Ru, et Centrum för rättvisa c. Suède, 25 mai 2021. Point 347 *« Certes, l'article 8 de la Convention n'interdit pas de recourir à l'interception en masse afin de protéger la sécurité nationale ou d' autres intérêts nationaux essentiels contre des menaces extérieures graves, et les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de régime d'interception ils ont besoin à cet effet, cependant la latitude qui leur est accordée pour la mise en œuvre de ce régime doit être plus restreinte et un certain nombre de garanties doivent être mises en place.* ». Voir également au plan national, CE, Ass, 21 avril 2021 req. n° 393099, 394922, 397844, 397851, 424717, 424718 ; DUBOUT E., « Le Conseil d'Etat, gardien de la sécurité », *RDLF*, 2021, chron. n° 18, *Revuedlf.com* [en ligne] [Consulté le 23 avril 2021]. Disponible à l'adresse : http://www.revuedlf.com/droit-ue/le-conseil-detat-gardien-de-la-securite/

[1970] SIZAIRE V., « L'art du trompe l'œil », *La Revue des Droits de l'Homme*, [en ligne]. Septembre 2021 [Consulté le 22 septembre 2021]. Disponible à l'adresse : https://journals.openedition.org/revdh/12968#abstract.

981. Ce risque de généralisation de la surveillance même au-delà de circonstances exceptionnelles a également été soulevé lors de l'urgence sanitaire par la CNIL, craignant un effet cliquet[1971]. D'une part concernant le déploiement de « vidéos intelligentes »[1972] pour mesurer le port du masque dans les transports, et d'autre part au sujet du recours au « passe sanitaire » [1973]. Elle a en ce sens indiqué pour la vidéo intelligente que « *même s'il est limité au cadre de l'état d'urgence sanitaire, un tel déploiement présente le risque réel de généraliser un sentiment de surveillance chez les citoyens, de créer un phénomène d'accoutumance et de banalisation de technologies intrusives et, en définitive, d'engendrer une surveillance accrue* », tandis que pour le « passe sanitaire », l'accoutumance et une banalisation pourrait aboutir à ce que de plus en plus de lieux, tels que l'accès au cinéma, seraient conditionnés à sa présentation, ce qui a finalement été le cas[1974]. Par ailleurs, la modification de la finalité d'un traitement à des fins liberticides apparaît aisée avec le temps.

982. D'autres techniques, telle que la reconnaissance faciale, traitent les données biométriques des personnes comme si elles étaient suspectes, parfois sur de simples émotions[1975] et ce sans le moindre soupçon raisonnable. Le fait de scanner des visages rend chaque individu présumé suspect, en plus de la collecte et du traitement d'un gabarit biométrique intrusif sans leur consentement. Il s'agit d'une automatisation de la suspicion, ayant par ailleurs des incidences sur l'exercice des autres libertés comme la liberté d'expression ou de manifestation[1976]. On a donc du mal à comprendre que la reconnaissance faciale soit interdite par principe sur le fondement du risque dans le projet de la Commission européenne alors qu'elle est autorisée par voie d'exception pour les usages les plus intrusifs tels que le maintien de l'ordre public[1977]. Les lignes directrices du Conseil de l'Europe sont à cet égard bien plus protectrices puisque dans la prolongation de la convention 108+ il se prononce en

[1971] Ce terme ne doit pas être appréhendé conformément à la jurisprudence du conseil constitutionnel, mais dans l'acception qu'une technologie, une fois déployée, a tendance à se pérenniser.
[1972] CNIL, Délibération n° 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports
[1973] CNIL, Délibération n° 2021-024 du 12 mai 2021 portant avis sur le projet de mise en place d'un passe sanitaire conditionnant l'accès à certains lieux, évènements ou établissements impliquant de grands rassemblements de personnes. Voir également en ce sens, délibération n° 2021-097 du 6 août 2021 portant avis sur un projet de décret modifiant le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire et le décret n° 2021-901 du 6 juillet 2021 relatif au traitement automatisé de données à caractère personnel dénommé « Convertisseur de certificats ».
[1974] Loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire, art. 1.
[1975] SIRINELLI P., PREVOST S., « Reconnaissance émotionnelle, connaissance irrationnelle ? », *Dalloz IP/IT*, 2021, p. 237.
[1976] Un sondage a révélé au Royaume-Uni que parmi les 16-24 ans interrogés, 38% ont déclaré « qu'ils éviteraient de participer à une manifestation si la police y utilisait la reconnaissance faciale. », DUCOURTIEUX C., « Le Royaume-Uni, champion de la reconnaissance faciale », *Le Monde*, 4 septembre 2019.
[1977] Art. 5 du projet de règlement.

faveur de l'interdiction de la reconnaissance comportementale et émotionnelle[1978] à l'inverse de la commission qui conditionne son usage à une transparence accrue[1979].

983. Il existe d'ailleurs une éventualité pour que ces outils soient un jour performants en plus d'être transparents, ce qui légitimerait leur usage sur le fondement de la seule problématique de transparence. Ainsi, le seul rempart contre des technologies liberticides ne peut qu'être l'exclusion. Ces outils sont autant de tentations à l'illusion d'un contrôle sur la vie des personnes et des sociétés. L'autorisation de la reconnaissance faciale sous condition, y compris pour des raisons d'ordre public tel que prévu par le règlement européen, feint d'ignorer tout à la fois le respect des droits et libertés et les principes juridiques traditionnels des démocraties libérales. Ainsi, lorsque la reconnaissance faciale est autorisée, elle remet de fait en cause la présomption d'innocence et les règles du procès équitable. L'immixtion des traitements algorithmiques en matière de police administrative ou judiciaire à des fins prédictives ne relève pas plus de la science puisqu'il n'est pas possible de prédire l'avenir. L'utilisation d'un logiciel de prédiction des infractions, comme certains sont actuellement développés par la police et la gendarmerie[1980], nourrissent une vision irrationnelle de la société, et sont sources de nombreuses boucles de rétroaction et de violation potentielles systémiques de droits et libertés[1981]. La justice n'est de plus pas à l'abri d'une tentation de l'automatisation à outrance de la procédure jusqu'au jugement[1982] ainsi que dans le suivi des peines. L'outil, même utilisé en tant qu'aide à la prise de décision sur l'évaluation d'une récidive par exemple, est en mesure d'exercer une incidence telle sur le discernement des magistrats qu'il est préférable de prohiber un tel usage[1983].

[1978] « *De même, la reconnaissance des affects peut également être effectuée au moyen des technologies de reconnaissance faciale pour prétendument détecter les traits de personnalité, les sentiments intérieurs, la santé mentale ou l'engagement des travailleurs à partir d'images des visages. Lier la reconnaissance de l'affect, par exemple au recrutement de personnel, à l'accès à l'assurance, à l'éducation peut présenter des risques très préoccupants, tant au niveau individuel que sociétal, et devrait être interdit* », Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel, « Lignes directrices sur la reconnaissance faciale », 28 janvier 2021, p. 4.

[1979] Art. 52 du projet de règlement.

[1980] Voir en ce sens, CASTETS-RENARD C., BESSE P., LOUBES J-M, PERRUSSEL L., Centre des Hautes Etudes du ministère de l'Intérieur, Rapport relatif Encadrement des risques techniques et juridiques des activités de police prédictive, *op. cit.*, et FERET C., POINTEREAU R., Rapport d'information n° 621, op. cit., faisant état du développement d'un logiciel de police prédictive par la gendarmerie afin d'anticiper les cambriolages sans avoir recours à des données à caractère personnel.

[1981] Voir en ce sens, THE CITIZEN LAB, To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada [en ligne]. [Consulté le 2 décembre 2020]. Disponible à l'adresse : https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

[1982] DUCLERCQ J-B., « Les algorithmes en procès », *op. cit.*, p. 131.

[1983] Suprem Court of Wisconsin, State of Wisconsin v. Loomis, case 2015AP157-CR [en ligne]. [Consulté le 2 mars 2021]. Disponible à l'adresse : https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690. Pour plus de précisions, *Supra.*, n° 658.

984. Il existe par ailleurs des hypothèses où l'absence de transparence technique, comme c'est aujourd'hui le cas pour les boîtes noires[1984], ou à l'inverse l'excès de transparence, justifierait l'exclusion du recours au numérique. Bien que revêtant des problématiques différentes, le vote par correspondance par internet ou le recours à des machines à voter pour des scrutins locaux et nationaux sont autant de risque pour la démocratie au sens large, la confiance en celle-ci, et spécifiquement pour les principes traditionnels du droit électoral[1985].

985. Au-delà de l'exclusion des usages ou de leur conditionnalité pour que le numérique soit autorisé, se pose également la question de l'interdiction de la recherche dans certains domaines. La recherche est libre par principe, mais une découverte implique par son existence un risque de déploiement, et parfois rapidement, sans analyse d'impact. En effet, nous apprenons beaucoup des incidences des technologies sur les individus et la société qu'ultérieurement à leur déploiement, raison pour laquelle certains universitaires se prononcent dans certains domaines en faveur de moratoires[1986]. Nous recommandons, au même titre qu'il existe des limites en matière de recherche en matière de clonage humain[1987], des limitations à la recherche dans le domaine des systèmes d'armement létaux autonomes (SALA), dont la recherche implique inéluctablement la prolifération[1988]. La doctrine du « zéro mort », mythe sur lequel repose le développement de ces dispositifs purement autonomes consiste à ce que chaque puissance militaire pense engager un conflit armé sans subir de pertes humaines[1989]. Le gouvernement français, bien que s'opposant aux SALA[1990], puisque préférant le recours aux systèmes d'armes létaux intégrant de l'autonomie car demeurant sous planification humaine[1991], n'a pas souhaité pour l'heure engager des négociations internationales sur leur interdiction[1992].

[1984] *Supra*., n° 16.

[1985] En effet, par exemple, dans le cadre du vote électronique la vérifiabilité impose par nature le fait de mette en place un système de retraçage de son vote numériquement afin de s'assurer que notre choix a correctement été pris en compte par la machine, ce qui peut être vu comme un excès de transparence remettant en cause le secret du vote. C'est donc ici le numérique, du fait de son utilisation pour plus de facilité qui a des incidences sur les principes traditionnels du droit électoral. Sur ce point, voir notamment *supra*., n° 607.

[1986] Voir en ce sens, THE CITIZEN LAB, To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada, *op. cit*.

[1987] Art L. 2151-2 du Code de santé publique précise que « *La conception in vitro d'embryon ou la constitution par clonage d'embryon humain à des fins de recherche est interdite. La création d'embryons transgéniques ou chimériques est interdite.* ».

[1988] NEVEJANS N., « La légalité des robots de guerre dans les conflits internationaux », *Recueil Dalloz.* 2016, p. 1273.

[1989] RUFFO M., « La robotisation de la guerre et de la décision militaire : efficacité et éthique », in JACQUEMIN H., DE STREEL A. (dir.), *L'intelligence artificielle et le droit, Larcier*, 2017, p. 437.

[1990] DE GANAY C., GOUTTEFARDE F., Rapport d'information n°3248 de l'Assemblée nationale, 15e législature, fait au nom de la commission de la défense nationale et des forces armées, enregistré à la Présidence de l'Assemblée nationale le 22 juillet 2020., p. 4, in *Assemblee-nationale.fr* [en ligne] 22 juillet 2020 [Consulté le 2 mai 2021]. Disponible à l'adresse : https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b3248_rapport-information

[1991] Comité d'éthique de la défense - Avis sur l'intégration de l'autonomie des systèmes d'armes létaux [en ligne]. [Consulté le 2 mai 2021]. Disponible à l'adresse : https://www.defense.gouv.fr/salle-de-presse/communiques/communique_le-comite-d-ethique-de-la-defense-publie-son-rapport-sur-l-integration-de-l-autonomie-des-systemes-d-armes-letaux

[1992] « (...)l'ouverture immédiate de négociations en vue d'un traité d'interdiction des "robots tueurs" ne serait pas la réponse pertinente », Ministère des Armées, Assemblée Nationale, réponse écrite à la question n° 15168 publiée au JO le 19 mars 2019,

De plus, comme l'indique Nathalie Nevejans, la conception implique la compréhension des règles du droit international humanitaire, ce qu'aucune IA n'est par ailleurs capable d'effectuer.

PARAGRAPHE 2 - L'exercice de la démocratie numérique

986. Le choix de la nature et du degré de transparence ou de l'exclusion d'un usage ne peut que s'opérer par le débat démocratique, ce que ne saurait retirer la technicité de l'informatique, souvent arguée pour cantonner ces choix à des débats d'experts[1993]. Nous aborderons donc la façon dont il convient d'appréhender la mince frontière qui sépare la transparence d'une exclusion du fait de l'environnement numérique (A). Enfin, au même titre qu'il existe une démocratie environnementale, il apparaît nécessaire qu'il existe une démocratie numérique (B).

A - La théorie de l'environnement numérique

987. La théorie des environnements n'est qu'une proposition pour établir des choix politiques précis. Elle peut néanmoins être utilisée en tant que méthode d'interprétation *in concreto* pour la justice. Cette méthode a pour objectif de déterminer s'il convient d'exclure une technologie, mais aussi la façon dont la conciliation juridique doit être opérée au sein de l'environnement numérique afin de poursuivre un système de valeur.

988. Comme nous avons pu le constater tout le long de ces travaux, les techniques juridiques employées à l'environnement numérique sont souvent celles de l'environnement classique, ce qui n'est pas sans incidence. Pour préserver les principes juridiques traditionnels inhérents à l'Etat de droit, cela implique la connaissance des caractéristiques de la technologie, parce que les algorithmes ne sont ni neutres, ni souvent conçus spécifiquement pour être respectueux de l'usage souhaité. Cela implique une fine analyse de l'architecture technique de la technologie, ce qui est nécessairement fluctuant et mouvant, et en rupture avec la neutralité technique des régimes généraux abordés. Cette prise en compte spécifique de la technologie vise à se prémunir de conciliations ou d'usages qui rendraient ineffectifs ou inopérants les droits et libertés au sein de cet environnement et emporterait ensuite des conséquences sur le terrain classique puisque ces deux sphères ne sont pas cloisonnées[1994].

15e Législature [en ligne]. [Consulté le 3 avril 2021]. Disponible à l'adresse : http://questions.assemblee-nationale.fr/q15/15-15168QE.htm

[1993] BENAYOUN Y., REGNAULD I., *Technologies partout, démocratie nulle part*, *FYP*, 2020, 240 p.

[1994] L'interaction du logiciel avec le monde physique n'est rendue possible uniquement parce que nous avons fait le choix de leur immixtion dans les domaines dans lesquels ils sont censés résoudre ou faciliter la résolution de problèmes. A titre d'exemple, recourir à un logiciel à des fins de pure simulation n'a aucune incidence sur le terrain classique puisqu'il est

989. Il ne s'agit pas ici d'appréhender la transparence ou l'usage en fonction du domaine d'intervention mais de la caractéristique technique de l'architecture qui va être déployée. Cet enjeu est éminemment démocratique. L'environnement numérique est régi par des règles dont la nature n'est pas exactement la même que sur le terrain classique, ce qui nécessite parfois une adaptabilité en fonction des caractéristiques techniques des outils[1995].

990. Pour illustrer ce propos, nous souhaiterions retracer brièvement la construction du droit du respect de la vie privée et la manière dont son régime juridique a bifurqué à cause du numérique pour donner naissance à la protection des données à caractère personnel, lui conférant ainsi une quasi-autonomie par rapport à son initial droit de rattachement[1996]. La vie privée est une notion relativement récente tant la promiscuité était importante dans les habitations de l'époque médiévale. C'est notamment la raison pour laquelle cette notion ne se retrouve pas protégée par la DDHC de 1789[1997]. Sa protection est plus tardive puisque le fruit d'une longue construction, parmi laquelle l'émergence de la photographie n'est pas étrangère par la voie de procédure pour diffamation[1998]. Il convient donc d'attendre 1970 pour que le respect de la vie privée fasse son entrée dans le code civil[1999] et soit par la suite constitutionnellement protégé[2000]. En droit français, et à l'inverse de la notion anglophone de « *privacy* »[2001], la motivation première de la LIL de 1978 est pourtant le respect de la vie privée aussi bien vis-à-vis de l'Etat que des acteurs privés à un niveau législatif, n'hésitant pas à

---

cantonné à sa sphère immatérielle. Voir en ce sens, PELLEGRINI F., CANEVET S., *Droit des logiciels*, *op. cit.*, p. 285, *« En effet, un logiciel ne peut avoir, par lui-même, aucune action sur le monde physique. Nous en donnons pour preuve qu'il est possible de faire fonctionner un logiciel au sein d'un simulateur sans qu'il produise les effets qu'il était censé avoir sur son environnement. C'est ainsi que l'on teste par exemple les logiciels embarqués de guidage des fusées : l'exécution de ces logiciels s'effectue non pas au sein du calculateur de la fusée, comme ce sera le cas en conditions réelles, mais au sein d'un environnement logiciel qui simule le fonctionnement de ce calculateur et de tous ses périphériques* ». Dès lors, lorsque le choix a été pris d'utiliser une technologie pour résoudre des problèmes humains, c'est prendre le risque de subordonner le monde physique aux caractéristiques du logiciel et de l'ordinateur qui l'exécute, et donc des limites de cet univers.

[1995] *Supra.*, n° 605 et s.

[1996] TAMBOU O., *Manuel de droit européen de la protection des données à caractère personnel*, *op. cit.*, p. 21.

[1997] LASCOMBE M., VANDENDRIESSCHE X., DE GAUDEMONT C., *Code constitutionnel et des droits fondamentaux*, *Dalloz*, 2016, spec. p. 19.

[1998] Tribunal civil de la Seine, Félix c. O'Connell, 18 juin 1858.

[1999] Loi n° 70-643 du 17 juillet 1970, art. 22 introduit à l'article 9 du Code civil que « *Chacun a droit au respect de la vie privée* ».

[2000] Ce n'est qu'après une construction progressive en droit national que le Conseil constitutionnel, en 1995, confronté à des dispositions relatives à l'installation de la vidéosurveillance, disposa « *que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* » prévue par l'article 66 de la Constitution. Voir en ce sens, CC, décision n° 94-352 DC, 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, cons. 3. Puis, en 1999, lorsque se pose l'instauration de la carte électronique individuelle pour la couverture maladie universelle, le Conseil précise finalement que « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression*. » ; « *que la liberté proclamée par cet article implique le respect de la vie privée* ; » sur le fondement de l'article 2 de la DDHC de 1789 ; CC, décision n° 99-416 DC, 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, cons. 45.

[2001] Voir en ce sens, WHITMAN J. Q., The Two Western Cultures of Privacy : Dignity versus Liberty, 2003, *Papers.ssrn.com* [en ligne]. [Consulté le 5 avril l2021]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=476041 ; HALPERIN J-L., « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », Les nouveaux Cahiers du Conseil constitutionnel, *Lextenso*, n° 48, 2015, p. 59.

interdire certains traitements de données pour protéger les personnes physiques[2002]. C'est sous l'impulsion de conventions internationales que la notion de données personnelles a pris toute son autonomie par rapport au respect de la vie privée[2003].

991. L'autonomie d'une telle notion est en principe justifiée pour mieux protéger les libertés au sein de l'environnement numérique, mais cela offre également paradoxalement la possibilité d'offrir un niveau de protection amoindri. En effet, bien que le respect de la vie privée soit matriciel dans la construction de la protection des données personnelles, c'est aussi la possibilité une fois cette nouvelle source créée, d'obtenir un régime juridique qui bifurquerait de sa source originelle, au point d'ouvrir droit à une nouvelle conciliation possible propre à la sphère numérique. La reconnaissance d'une nouvelle source doit alors permettre des prises en compte spécifiques à cet environnement pour parvenir à l'objectif de protection souhaité. Ces principes ne sont d'ailleurs pas ceux du terrain classique, mais bien du cyberespace, sphère sans laquelle ils n'auraient pas existé, et dont on voit bien que les régimes juridiques ne sont pas identiques et ne poursuivent pas toujours les mêmes buts. Mais le caractère pernicieux des algorithmes informatiques encourage l'acceptabilité de pratiques que l'on n'accepterait jamais sur le plan physique, et pourtant que le pouvoir politique et juridictionnel nous impose, parfois par méconnaissance de la technique. C'est donc par l'étude de la technique que le droit doit aussi être modelé en conséquence, mais volontairement. Alors qu'en apparence le droit est en réaction à un fait juridique, c'est désormais la technologie qui modifie le droit sans que nous nous en apercevions. Il ne s'agit plus d'une réaction politique à un fait juridique, mais d'un dégât collatéral au déploiement d'une technologie dont l'impact aurait mal été évalué. C'est pour cette raison que la théorie de l'environnement numérique vise à pallier ce risque.

992. Même si les régimes juridiques généraux sont tenus d'aborder de tels domaines avec une neutralité technique, il convient cependant dans certains cas d'entrer dans le détail de certaines technologies dans le débat politique ou pour l'application de la loi, ne serait-ce car des technologies sont amenées à conditionner l'exercice des droits et libertés.

993. Nous avons néanmoins conscience que cette approche peut légitimer une restriction des libertés puisque le régime juridique qui est l'émanation du terrain classique ne peut pas toujours être identique à celui nécessaire pour poursuivre l'exercice d'une liberté sur le terrain numérique. En effet, certains pourront toujours arguer que l'environnement numérique exige

[2002] *Supra.*, n° 148.
[2003] *Supra.*, n° 908 notamment.

d'amoindrir des droits et libertés, et qui légitimerait des usages particulièrement intrusifs qu'il est pourtant impensable d'opérer sur le terrain classique. A titre d'exemple, la Cour EDH reconnait que la sphère numérique est source de nouvelles menaces, ce qui implique le recours à des outils de surveillance de masse[2004]. En d'autres termes, cela revient à considérer que le régime juridique applicable à l'environnement numérique et donc aux droits et libertés à cet environnement, ne peuvent être les mêmes que sur le terrain classique, et ce alors que cette nouvelle conciliation est défavorable pour les libertés, et emporte physiquement des conséquences. Nous imaginons pourtant mal la Cour de Strasbourg admettre une surveillance physique de masse aussi intrusive que ne l'est la surveillance numérique à des fins de préservation de l'ordre public. Pourtant, les conséquences d'un tel postulat sont tout aussi graves. Au même titre que le numérique est facilitateur en matière de liberté d'expression, il l'est tout aussi en termes de surveillance qu'elle soit privée ou publique.

994. Nous pensons contrairement à la Cour, et ce quelles que soient les garanties qui seraient mises en œuvre, que du fait de sa nature, l'environnement numérique demande plus de protection tant les outils qui y sont déployés ont des incidences systémiques et potentiellement liberticides. Raison pour laquelle il serait même envisageable de reconnaître des sanctuaires dans l'environnement numérique, où l'on pourrait même imaginer que des droits de détachement seraient absolus, car à défaut le principe même d'une conciliation les rendrait inopérants.

995. Même si aujourd'hui il existe également « *Law is code* » aux cotés de « *Code is Law* »[2005], c'est le matériel informatique et le logiciel qui conditionnent en partie l'exercice de l'Etat de droit dans cet environnement, et qui par ricochet impacte le terrain classique. Ne serait-ce car si un Etat devait par exemple imposer une porte dérobée dans un système de télécommunication centralisé, quand bien même il serait chiffré, il permettrait à toute personne connaissant cette ouverture d'accéder aux messages échangés. C'est donc la nature même de la communication qui est modifiée par le numérique puisqu'en effet, on imagine mal comment sur le terrain classique il serait possible d'opérer l'ouverture et la lecture de tout le courrier postal, et d'y faire humainement des recoupements identiques à ce que permet l'informatique, preuve que la nature y est différente.

[2004] Cour EDH, Grande chambre, Big brother watch c. Ru, du 25 mai 2021 « *Il y a là une menace grave pour la sécurité nationale qui, par définition, n'existe que dans le domaine numérique et ne peut donc être détectée et investiguée qu'à l'aide de moyens numériques.* », § 323.
[2005] GROFFE-CHARRIER J., « La loi est-elle dictée par le code ? », *op. cit*.

996. Reconnaître une autonomie de l'environnement numérique, c'est accepter qu'un régime juridique ne puisse être identique entre ce terrain classique et l'environnement numérique. Ainsi, l'attention faite à une liberté hors ligne ne peut être en réalité identique dans la sphère numérique. En ce sens, l'interdiction d'un usage au sein de cet environnement ne signifie pas qu'il n'existe pas d'alternative dans l'autre monde. Ne pas souhaiter recourir à des dispositifs à des fins de surveillance de masse, n'implique pas un renoncement d'opérations de surveillance par des voies plus traditionnelles car nos capacités humaines ont des limites observationnelles qui sont par ailleurs des protections physiques pour les libertés. Ainsi, le fait qu'un agent du renseignement intègre, comme cela est déjà le cas, une cellule djihadiste qui communiquerait par la voie d'une messagerie chiffrée est moins attentatoire aux droits et libertés que l'instauration de portes dérobées[2006] dans un tel système, ce qui offrirait la possibilité d'une captation de tout cet environnement.

997. De la même manière, et bien que nous soyons conscients des avantages du vote électronique tendant vers un exercice plus direct de la démocratie[2007] pour les scrutins nationaux et locaux, l'appréhender comme simple dématérialisation du vote traditionnel papier, c'est faire fi de l'environnement numérique qui exerce une pression sur les principes traditionnels du scrutin. L'étude des architectures techniques proposées dans le cadre des machines à voter ou du vote par internet ne saurait permettre une transparence directe, sans remettre en cause le secret du scrutin. Telle est actuellement la nature de l'informatique, que nous le voulions ou non. La matière électorale est par ailleurs si sensible quant aux incidences démocratiques que même la désignation d'un tiers de confiance ne saurait empêcher un risque de fraudes ou d'erreurs significatif sur le résultat du scrutin[2008]. De la même manière, concernant le vote par internet, c'est prendre le risque que des données personnelles, portant notamment sur les opinions politiques puissent être manipulées et piratées. Il convient alors de garder une garantie collective lors des opérations de vote, ce que seul le scrutin traditionnel sur support papier en dehors de tout vote par correspondance est pour l'heure en mesure d'assurer[2009], ce qui permet

[2006] « *Le principe de la mise en œuvre d'une « Backdoor » ou porte dérobée correspond à prévoir un accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel. Le principe de la mise en œuvre d'une « Master Key » ou « clé maître » correspond à prévoir ouvertement un tel accès, mis en œuvre via cette clé, aux données chiffrées contenues dans un logiciel ou sur un matériel.* », définition donnée par la CNIL [en ligne]. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://www.cnil.fr/fr/definition/porte-derobee-ou-backdoor

[2007] Ces facilités logistiques semblent même au premier abord susceptibles de favoriser l'exercice de la souveraineté politique par le Peuple, laissant entrevoir de nouveaux mécanismes démocratiques.

[2008] *Supra*., n° 538 et s.

[2009] Pour le professeur Jean-Philippe Derosier, la technicité du vote par Internet *« semble a priori empêcher le contrôle éclairé des citoyens ». La CNIL souligne également « l'opacité et la technicité importante des solutions mises en œuvre ». Elle reste, d'une manière générale, « réservée quant à l'utilisation de dispositifs de vote par correspondance électronique, notamment via Internet, pour des élections politiques »*, BUFFET F-N., Rapport d'information n° 240 relatif au vote à distance du Sénat, session ordinaire 2020-2021, fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du

notamment de conserver l'effectivité des autres principes du droit électoral qui auraient été remis en cause par nature par l'utilisation de ces techniques pour les raisons explicitées.

998. Il y a donc des domaines dans lesquels le recours exclusif à l'environnement classique offre le plus de garanties, et quand bien même le numérique serait plus efficace. C'est donc aussi parce qu'une technologie est trop efficace qu'il est nécessaire de l'exclure pour s'en prémunir, et ce que quel que soit les garanties de transparence et de contrôle humain sur l'outil. Ainsi, l'interdiction du recours au numérique dans un environnement ne veut pas dire que l'on obtiendra aucun résultat sur le terrain classique.

999. Les parlementaires et les citoyens ont donc besoin de discuter précisément des technologies qui vont être déployées, raison pour laquelle notre autorité de contrôle unique aura également pour mission de cartographier les technologies et leurs incidences sur les libertés et la société, ce qui conditionne leur choix. Nous gageons donc que la révision des institutions[2010] que nous souhaitons offrira plus de protection et empêchera cette déviance.

B - Principe de participation aux décisions en tant que composante de la démocratie numérique

1000. La transparence ne pouvant pas apporter toutes les garanties nécessaires à l'épanouissement de l'Etat de droit, le choix de l'exclusion ou d'une plus grande transparence d'un usage, doit aussi pouvoir s'effectuer à travers la participation du public, ce qui vient compléter la démocratie représentative telle qu'abordée précédemment[2011].

1001. La démocratie numérique dont il est question dans cette démonstration n'est pas l'évolution des institutions par les nouveaux outils[2012], mais la façon dont il est possible pour le public de participer aux prises de décisions qu'elles soient d'ailleurs publiques ou privées.

1002. Pour l'heure, la démocratie environnementale, partie intégrante de la démocratie administrative[2013], connait une expansion et ne peut que servir de modèle à bien des égards en matière de participation numérique. Elle est intéressante en ce qu'elle illustre l'émergence d'un

---

Règlement et de l'administration générale, enregistré à la Présidence du Sénat le 16 décembre 2020, p. 49, *Senat.fr* [en ligne]. [Consulté le 2 mai 2021]. Disponible à l'adresse : http://www.senat.fr/rap/r20-240/r20-2401.pdf

[2010] *Supra*., n° 694 et s.

[2011] *Ibid.*

[2012] Certains auteurs pensent en effet que les nouveaux outils numériques peuvent modifier la nature de la participation citoyenne, ce que nous ne nions pas, mais cela n'est pas l'objet de l'actuelle démonstration.

[2013] Voir en ce sens, CHEVALLIER J., « De l'administration démocratique à la démocratie administrative », *Revue française d'administration publique, ENA*, 2011/1, p. 217 à 227.

fait juridique contemporain et une réponse juridique particulière, parmi laquelle nous retrouvons le principe de participation du public[2014], qui par ailleurs est désormais intégré au bloc de constitutionnalité[2015]. Même si la mise en œuvre de ce principe demeure imparfaite[2016], nous souhaiterions que la démocratie numérique puisse s'en inspirer. Il convient toutefois d'aller plus que ce que permet la démocratie environnementale et administrative. En effet, la participation du public que nous souhaiterions, ne poursuit pas totalement les mêmes objectifs puisqu'au-delà de la participation aux prises de décision publique, il s'agirait également d'un principe hybride prenant en compte aussi bien la problématique de la démocratie administrative que de la démocratie directe.

1003. Contrairement au principe de participation en matière environnementale qui a été le fruit de décennies de construction notamment par la voie de conventions internationales[2017], les sources manquent cruellement dans le domaine numérique. En effet, il n'y a pas pour l'heure de source internationale pouvant influencer une éventuelle transposition rapide dans le droit régional ou national. Il reste donc tout à bâtir. Certaines déclarations de normes informelles telles que la déclaration de Montréal pour une IA responsable évoquent toutefois un tel principe[2018]. Par exemple, au même titre que la convention d'Aarhus pour l'environnement, nous retrouvons dans la convention sur l'IA l'accès à l'information, et donc à la transparence de ces outils, pour que puisse s'exercer le débat et le contrôle démocratique. Il existe donc une troublante symétrie avec la démocratie environnementale, à la différence que le numérique ne peut se cantonner qu'aux prises de décision publique. C'est donc en ce sens qu'il ne sera pas possible de qualifier cela de démocratie administrative.

1004. La transparence juridique que nous nous sommes efforcés à construire tout au long de ces travaux rencontre donc nécessairement l'une de ses finalités essentielles, à savoir la participation du public grâce au droit à l'information, offrant un débat et une prise de décision éclairée. En effet, comme le note Julie Arroyo au sujet de la transparence administrative, ce que nous pouvons dupliquer à la transparence générale des traitements algorithmiques, elle

[2014] VAN LANG A., « Le principe de participation : un succès inattendu », *Les nouveaux Cahiers du Conseil constitutionnel*, n° 43, 2014, p. 25.
[2015] « *Toute personne a le droit, dans les conditions et les limites définies par la loi, d'accéder aux informations relatives à l'environnement détenues par les autorités publiques et de participer à l'élaboration des décisions publiques ayant une incidence sur l'environnement.* » art 7, Charte de l'environnement.
[2016] *Infra*., n° 1006 et s.
[2017] La démocratie environnementale est composée du triptyque de l'information, de la participation et de l'accès à la justice telle que présentée notamment par la Convention sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement, dite d'Aarhus, du 25 juin 1998.
[2018] Principe 5 : « principe de participation démocratique », Déclaration de Montréal pour un développement responsable de l'intelligence artificielle [en ligne]. [Consulté le 15 juin 2021]. Disponible à l'adresse : https://www.declarationmontreal-iaresponsable.com/la-declaration

« *participe à la réalisation de ces nouvelles exigences démocratiques en assurant l'information des administrés, cette information leur permettant de se livrer à une forme de contrôle du pouvoir ainsi que, dans une certaine mesure, d'y participer* »[2019].

1005. Ainsi, il convient de déduire que lorsque cette transparence ne peut être exercée techniquement, du fait d'une architecture opaque par nature, cela peut être légitimement un motif à son exclusion. C'est la raison pour laquelle le droit d'information en tant que technique juridique de mise en œuvre du principe de transparence des traitements algorithmiques, ne doit connaître que de rares exceptions[2020]. Dans ces rares hypothèses c'est à la commission technique de contrôle unique qu'il reviendra alors de procéder à ces expertises et de diffuser les rapports et études d'impact nécessaires à l'épanouissement du débat. En effet, des informations minimales certifiées seront nécessaires au public pour qu'il puisse également se prononcer sur certaines orientations privées.

1006. Le droit interne nous renseigne déjà en droit de l'environnement ou en urbanisme sur la forme que pourrait prendre cette participation même si elle ne s'applique qu'aux décisions d'autorités publiques[2021]. Nous retrouvons par exemple en amont de la mise en œuvre des projets les procédures de participation du public au débat ou à la décision finale aussi bien au plan local que national. Bien que ces procédures soient critiquables à certains égards, car elles ne lient pas la décision finale dans la plupart des cas, il convient de s'en inspirer. De nombreuses collectivités territoriales[2022] sont par exemple tentées par des expérimentations attentatoires aux libertés comme le déploiement de drones, de la reconnaissance faciale, ou des détecteurs de bruits dans l'espace public, sans qu'il ne soit spécifiquement possible pour les administrés de s'y opposer publiquement autrement que par la voie d'élections générales, de collectifs ou judiciairement.

1007. A l'inverse de la participation aux débats publics en matière environnementale qui s'apparente davantage à un processus de légitimation[2023] d'un projet, les réserves émises par le

[2019] ARROYO J., Un droit à l'oubli dans le champ des documents administratifs ?, *RDLF*, chron. n° 6, 2016 [en ligne]. [Consulté le 15 juin 2020]. Disponible à l'adresse : http://www.revuedlf.com/droit-administratif/un-droit-a-loubli-dans-le-champ-des-documents-administratifs/#note-6120-99
[2020] *Supra*., n° 938 et s.
[2021] *Infra*., n° 1007.
[2022] FRENOIS M., Nice : Caméra, reconnaissance faciale, détecteur de bruits… Un collectif lancé pour « résister à la surveillance », *20 minutes.fr* [en ligne] 17 septembre 2019 [Consulté le 3 février 2021]. Disponible à l'adresse : https://www.20minutes.fr/nice/2605395-20190917-nice-camera-reconnaissance-faciale-detecteur-bruits-collectif-lance-resister-surveillance
[2023] Comme l'indique Jacques Chevallier « *Les procédures délibératives apparaissent, dès lors, moins l'instrument permettant aux citoyens de définir, par le biais de leurs discussions, les contours de l'action publique, que le moyen pour les gouvernants*

public devraient être prises en compte lors de la phase d'élaboration du projet numérique, ou à défaut permettre par un droit de pétition facilité la possibilité d'une consultation locale ou nationale qui lierait le maître d'ouvrage. Les projets concernés seraient les plus importants, et ceux nécessitant la désignation d'un architecte du numérique que nous avons abordé[2024].

1008. Il serait même concevable d'aller plus loin en incluant dans ce principe, la participation à la gouvernance de grandes plateformes numériques, y compris privées qui exercent une influence significative sur la société et les libertés. Il convient désormais que le public prenne part aux décisions des grands réseaux sociaux qui modèlent pourtant le monde par l'intermédiaire de traitements algorithmiques, notamment afin qu'ils participent au design et aux orientations des architectures techniques de ces derniers, ce qui n'empêchera pas la plateforme de pouvoir continuer à avoir une politique commerciale dans les domaines qui ne sont pas du ressort des libertés. Il ne s'agit pas pour autant par cette participation d'aboutir à l'émergence d'un droit qui bifurquerait du cadre posé par l'Etat, mais cela offrirait des marges de manœuvre suffisantes que ces espaces, devenus de fait des activités d'intérêt général par la sociabilisation humaine, puissent définir certaines orientations en tant que gestion d'un commun, et pourquoi pas de manière transnationale. Dans le cadre des réseaux sociaux centralisés par exemple, un seuil de connexion minimal comme c'est déjà le cas dans la LRN pour imposer des obligations de transparence, permettrait une participation du public à ces réseaux qui sont devenus de fait par extension des espaces publics. Cette approche admet, comme le propose Jason Barrett Prado, des règlementations particulières en fonction du nombre d'utilisateurs[2025]. Certains auteurs considèrent toutefois que la taille des services privés ne fait pas tout et que leur régulation peut notamment s'effectuer à travers plusieurs critères tels que la fonction ou le pouvoir qu'ils exercent[2026].

1009. C'est aussi une manière de contrecarrer les tentatives d'entreprises comme Facebook, qui sous réserve de conditions générales d'utilisation se permettent même de proposer une construction juridictionnelle sans légitimité, aboutissant à un droit alternatif concurrençant le

de consolider celle-ci, sur un plan pratique comme sur un plan symbolique. », CHEVALLIER J., « De l'administration démocratique à la démocratie administrative », *op. cit.*, p. 227.

[2024] *Supra.*, n° 890 et s.

[2025] Selon Jason Prado, si un service bénéficie de moins de 5 millions d'utilisateurs, il est soumis aux règles classiques de confidentialités. Entre 20 et 50 millions d'utilisateurs, la plateforme serait contrainte par des obligations de transparence telles que la publication de rapports sur les données utilisées et la manière dont elles sont utilisées. Tandis qu'au-delà de 100 millions d'utilisateurs, il ne serait plus possible de distinguer le service d'un Etat, raison pour laquelle elle doit être gouvernée démocratiquement avec un conseil d'administration représentatif. Voir en ce sens, PRADO Jason Barrett, Taxonomizing platforms to scale regulation, *Venturecommune.substack.com* [en ligne] 18 novembre 2019 [Consulté le 2 novembre 2020]. Disponible à l'adresse : https://venturecommune.substack.com/p/taxonomizing-platforms-to-scale-regulation

[2026] TARNOFF Ben, Platforms don't exist, *Bentanoff.substack.com* [en ligne] 22 novembre 2019 [Consulté le 11 janvier 2021]. Disponible à l'adresse : https://bentarnoff.substack.com/p/platforms-dont-exist

l'autonomie des citoyens en modelant par exemple l'exercice de la liberté d'expression qui s'effectue de plus en plus sur ces plateformes. Un tel principe devrait également être constitutionnalisé car il se heurte à des principes préexistants qui n'assurent pas une conciliation en ce sens[2027].

1010. Au-delà des plateformes numériques, nous considérons également que le principe de participation doit s'étendre à l'élaboration des standards techniques en informatique, voire des normes ISO, qui bien que privées, mettent en œuvre le principe de transparence d'un point de vue technique et façonnent le numérique en général. Ainsi, une convergence doit désormais s'opérer entre spécialistes et la poursuite de l'intérêt général, car mêmes les choix techniques apparaissant comme anodins sont aussi des choix de nature politique concernant la société humaine.

CONCLUSION DU CHAPITRE II

1011. Le principe de transparence des traitements algorithmiques connait des limites. Même avec les bénéfices d'une constitutionnalisation, il existe de fait plusieurs manières d'assurer sa mise en œuvre, ce qui impacte de fait la protection des droits et libertés qu'il est censé protéger. L'étude des approches effectuées dans le cadre de ce chapitre revient donc à considérer que pour garantir son effectivité, la prise en considération du risque de l'usage et de la légitimité doivent être combinées à l'inverse de ce que propose le projet de règlement européen qui doit être enrichi en ce sens.

1012. Enfin, la transparence ne peut se suffire à elle-même puisque quand bien même elle serait absolue d'un point de vue juridique et technique, elle est susceptible de légitimer des usages liberticides. Il convient alors pour les usages les plus sensibles et inconciliables avec les valeurs de notre Etat de droit, de procéder à une exclusion de ces traitements. Ces exclusions doivent être discutées grâce à un principe de participation du public à la prise de décision aussi bien publique que privée du fait des incidences sur la société que les algorithmes exercent.

[2027] SUPREME COURT OF THE UNITED STATES OF AMERICA, Manhattan community acces corp. ET AL. V. Halleck Et AL, 17 juin 2019. Voir en ce sens, G'SELL F., « Remarque sur les aspects juridiques de la souveraineté « numérique » », *La Revue des juristes de Science Po*, n° 19, octobre 2019, spec. p. 55 : « *la Cour Suprême y juge que les acteurs privés hébergeant des espaces de discussion ouverts au public sont libres de les modérer à leur discrétion.* ».

CONCLUSION DU TITRE II

1013. La mise en œuvre d'un principe général de transparence des traitements algorithmiques ne peut être effectuée que par l'intermédiaire des pouvoirs constitués de l'Etat. Mais la société civile ne saurait être en reste et doit pouvoir bénéficier d'un rôle plus significatif afin de participer à son effectivité. De nombreuses associations ou encore des lanceurs d'alerte ont par exemple démontré qu'ils concouraient à une meilleure compréhension des outils numériques. L'éthique est de plus un guide, une « antichambre » du droit, qu'il convient de prendre en considération, même si elle ne doit pas avoir vocation de se substituer au droit. Les acteurs de la chaîne algorithmique sont susceptibles de prendre part à la réalisation de cet objectif. L'institution DPD devrait être élargie afin que tout traitement de données personnelles ou non, puisse être explicité, dès lors qu'il exerce une incidence sur la société. Une nouvelle profession, comme l'architecte du numérique, pourrait être le garant, pour les plus grands projets, du respect de toutes ces nouvelles obligations.

1014. Enfin, il n'y a pas d'intérêt à ce que tous les traitements algorithmiques soient transparents. Certains algorithmes des opérateurs économiques ne sont pas susceptibles de l'être lorsqu'ils n'ont pas d'effets juridiques, tandis que ceux de l'administration, y compris lorsqu'il s'agit de simples outils d'aide à la décision politique doivent l'être pour alimenter le débat public. L'étude des nouvelles techniques juridiques proposées par la Commission européenne sont intéressantes, notamment par l'intermédiaire d'une approche graduée par les risques, c'est-à-dire que plus un traitement algorithmique est susceptible d'exercer une incidence sur les personnes et la société, plus la nature et le degré de la transparence à effectuer est important.

1015. Néanmoins, quand bien même elle serait effective, il convient dans de nombreuses hypothèses d'exclure certains usages algorithmiques car trop attentatoires aux libertés. En effet, le principe de transparence connaît des limites et n'a pas vocation à légitimer des usages. Pour ce faire, un principe de participation permettrait aux citoyens de se prémunir des effets indésirables d'une transparence utilisée en tant que faire-valoir, et de choisir le cas échéant, quels seraient les usages algorithmiques à exclure ou à autoriser sous condition.

CONCLUSION DE LA SECONDE PARTIE

1016. Nous sommes incontestablement à un tournant où les nouveaux enjeux du numérique interrogent le fonctionnement de nos institutions, mais également de la hiérarchisation des valeurs constitutionnelles entre elles. En effet, le secret ou les libertés économiques doivent-elles l'emporter sur la transparence des traitements algorithmiques ? Ce débat, y compris entre juristes, n'aura jamais été aussi contemporain. A défaut, cela reviendrait à s'empêcher d'observer un environnement parallèle au terrain classique, alors que l'étude de certains outils, y compris par un tiers de confiance indépendant, est nécessaire car il conditionne l'exercice de nos libertés. Bien entendu, il est toujours possible de saisir certaines logiques sans avoir accès à toutes les informations d'un algorithme et de ses données, mais cela limiterait considérablement la compréhension de nombreux systèmes qui pourtant exercent une incidence sur la société et les personnes. C'est la raison pour laquelle pour des raisons démocratiques il est impératif qu'une telle transparence puisse s'opérer à travers un principe constitutionnel général de transparence des traitements algorithmiques qui bénéficierait d'une unicité conceptuelle, à savoir que l'observation conditionne nécessairement les choix démocratiques qui en découlent. A défaut, le secret annihilerait toute possibilité de se saisir d'un fait juridique, mais aussi de permettre l'effectivité des droits et libertés et de l'ordre juridique.

1017. Ce principe de transparence ne peut toutefois se mettre en œuvre de manière liberticide. En effet, l'excès de transparence est souvent associé au totalitarisme, surtout lorsqu'il est exigé des individus. Il convient qu'elle s'effectue dans le respect des droits et libertés et sous l'égide d'une autorité de contrôle purement technique et indépendante dont le rôle serait d'expertiser ces algorithmes. Ensuite, c'est naturellement au pouvoir politique de préciser la nature et le degré de l'information à communiquer à la société et aux personnes concernées afin de garantir d'autres exigences constitutionnelles comme la vie privée notamment. Pour ce faire, il nous est apparu opportun que les pouvoirs constitués prennent en compte les particularités du numérique pour une meilleure action de l'Etat. En ce sens, une chambre dédiée ainsi que la création de chambres spécialisées en matière du numérique semble indispensable pour que cette transparence soit effective.

1018. Pour finir, comment ne pas considérer que le rôle de la société civile doit aussi être encouragée dans cette quête de transparence, ne serait-ce parce qu'elle exerce également un contrôle sur ces algorithmes et éclaire la société dans son ensemble au sujet de leur compréhension. L'Etat gagnerait à encourager de telles initiatives qui ont déjà dans de

nombreux domaines pu faire leur preuve comme en matière d'obsolescence programmée notamment à travers des associations de consommateurs. Il en est de même concernant le rôle des lanceurs d'alerte et qui contribuent à l'observation de certains comportements au sein de l'environnement numérique.

1019. L'éthique est par ailleurs amenée à bénéficier d'un rôle de plus en plus significatif afin de penser le droit de demain. De nouvelles professions permettront également, sur le modèle du DPO, à être acteur et interlocuteur en matière de droit à l'information des traitements algorithmiques, qu'ils manipulent des données personnelles ou non, dès lors qu'ils ont une incidence sur la société. Enfin, certains grands projets recourant au numérique et ayant un potentiel caractère systémique, devraient être subordonnés à la désignation d'un architecte du numérique s'assurant que le cadre réglementaire en la matière est correctement respecté. Il s'agirait d'un contrôle *a priori* des algorithmes.

1020. La transparence ne doit cependant pas occulter la problématique selon laquelle des usages algorithmiques demeurent risqués, et ce malgré une explicabilité et un contrôle effectif. Dans cette hypothèse, il conviendrait davantage d'interdire les algorithmes d'intervenir dans le déroulement des procédures scrutins nationaux. Cette exclusion pourrait s'effectuer aussi bien par les représentants que par la voie d'un principe de participation du public.

CONCLUSION GENERALE

I - Vers une autonomie de la transparence des traitements algorithmiques

1021. Qu'il s'agisse d'une règlementation générale comme la LIL de 1978 ou de dispositions plus sectorielles portant sur l'amélioration d'un droit à l'information au sujet de ces algorithmes dans un but de protection des consommateurs, ou des administrés, le droit positif illustre une volonté de bénéficier d'une plus grande compréhension des traitements algorithmiques. Cet empilement normatif et leur articulation n'est toutefois pas sans défaut.

1022. Certaines techniques juridiques adoptées pour parvenir à cette transparence sont d'une part relativement complexe pour les personnes concernées par ces traitements et d'autre part manquent cruellement d'unicité conceptuelle. En effet, le législateur poursuit des objectifs, parfois au gré du hasard et de l'actualité, sans nécessairement penser qu'au-delà des régimes juridiques de rattachement, il convient désormais d'assurer la transparence d'un environnement numérique de manière autonome, c'est-à-dire pour ce qu'il est, à savoir une sphère dans laquelle les caractéristiques techniques ont des incidences sur l'effectivité des droits et libertés.

1023. Naturellement, la transparence peut être utilisée à des fins d'information, de loyauté, permettant un consentement libre et éclairé en droit privé ou d'un meilleur contrôle de l'action administrative en droit public, mais cela ne saurait occulter qu'il manque une source permettant d'orchestrer la compréhension de l'écosystème numérique qui s'effectue par un plus grand contrôle sur les algorithmes. Ce contrôle ne peut s'effectuer que par une meilleure cartographie du cyberespace afin que les citoyens et leurs représentants puissent œuvrer en toute connaissance de ces nouveaux enjeux, auquel cas il existe un risque que l'effectivité des valeurs de notre Etat de droits soient tributaires des technologies d'autres Etats ou d'opérateurs économiques.

1024. Les récentes propositions de règlementation de l'Union européenne vont dans le bon sens même si leur issue est incertaine au Parlement européen. Alors que le RGPD s'inscrivait vers une primauté du libéralisme économique et de la culture du secret des Etats affaiblissant le droit à l'information des personnes physiques et morales au sujet de ces algorithmes, sans que ne soit véritablement pensée l'exercice d'une transparence indirecte par le truchement d'une autorité de contrôle afin de mettre fin à toute asymétrie informationnelle, une

transparence plus aboutie vis-à-vis de tous les acteurs de la chaine algorithmique est désormais envisagée essentiellement au nom de la sécurité et de la protection des droits fondamentaux. Elle s'effectue notamment par l'utilisation de technique juridique nouvelles prenant en compte les particularités du numérique. Bien qu'imparfaite à de nombreux égards, il s'agit d'une autonomisation d'un principe général de transparence des traitements algorithmiques, ce qui n'empêche par ailleurs que ce principe se compose et participe à la transparence administrative, de la vie politique ou encore du marché.

1025. Néanmoins, cet optimisme est à nuancer, car il existe de nombreux obstacles sur la voie de la réalisation d'une telle transparence ; ils sont évidemment techniques, puisque cela dépend de l'état de l'art des sciences de l'informatique, mais surtout juridiques.

II - Un conflit inéluctable entre ordres juridiques régionaux et internationaux

1026. Pour se doter de la plus grande force permettant l'effectivité juridique d'une telle transparence, l'Union européenne offre une agrégation de puissance conséquente. Il demeure une inconnue non négligeable au sujet des conflits de normes notamment avec les intérêts nationaux des autres Etats membres avec qui nous ne partageons pas toujours la même acception de l'intérêt général. L'exemple le plus frappant étant celui de l'autorité de contrôle irlandaise qui, parce qu'elle est référente des géants du numérique, tend à l'ineffectivité des règles du RGPD, notamment en matière de transparence[2028], car il s'agit aussi d'un enjeu économique pour cet Etat. L'Union n'est de plus pas compétente pour contrôler par exemple les traitements algorithmiques en matière de défense ou de renseignement des Etats membres, alors qu'ils sont susceptibles de collecter et de traiter de nombreuses données sur des citoyens de l'Union.

1027. Au-delà du droit régional, le droit international est aussi confronté à un conflit entre les droits et libertés de génération différentes. Le libéralisme politique, puis économique, et les droits sociaux en général sont en confrontation permanentes et le numérique cristallise d'autant plus ces tensions que la technologie est un outil parfois au service de la puissance des Etats. Leur compréhension implique donc dans certains cas un regard sur des secrets protégés

[2028] Résolution du Parlement européen du 20 mai 2021 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 Maximillian Schrems (« arrêt Schrems II »).

exposant le cas échéant à l'appropriation de ces technologies par d'autres acteurs. Il est assez peu probable qu'une hiérarchisation entre droits et libertés soient opérée afin de servir une meilleure compréhension des algorithmes les plus sensibles, même par l'intermédiaire d'une autorité de contrôle quand bien même serait-elle internationale.

1028. Toutefois, si ni l'Union européenne, ni tout autre organisation internationale, ne souhaitent infléchir une politique en la matière, nous n'avons pas d'autres choix que de cultiver cette particularité de transparence à l'échelon national. C'est pourquoi une constitutionnalisation de la transparence juridique des traitements algorithmiques est en premier lieu indispensable afin de guider une action en ce sens et insuffler le cas échéant l'idée selon laquelle l'autonomie des citoyens en démocratie passe par la compréhension de ces nouveaux outils.

1029. Une charte des droits et libertés à l'ère du numérique pourrait y faire figurer le principe de transparence des traitements algorithmiques, même s'il conviendra que le législateur précise les modalités d'application. La compréhension des caractéristiques de ces algorithmes, y compris la vérification des erreurs de traitement, doit pouvoir être *a minima* effectuée par un tiers de confiance bénéficiant des capacités humaines, matérielles et techniques suffisantes. La France peut insuffler de telles avancées comme elle l'a fait avec la DDHC de 1789, mais en faisant la synthèse entre le libéralisme politique et la protection par la puissance publique de la menace du marché. La démocratie libérale française est à la croisée des deux acceptions de l'intérêt général[2029], ce qui justifie une approche nationale particulière dans la reconnaissance de droits et libertés numériques dont la transparence serait la clé de voûte.

III - L'indispensable mutation étatique

1030. L'Etat ne peut qu'être au cœur de ces nouvelles mutations parce qu'il est un outil au service de l'autonomie des citoyens en démocratie afin « *que nous n'obéissions qu'à nous-même ou au moins à la volonté de la majorité des citoyens librement exprimée* »[2030]. Même encore à ce jour, nulle puissance n'a d'égal pour imposer des exigences démocratiques aux opérateurs économiques exerçant une incidence conséquente sur les personnes et la société.

[2029] *Supra*, n° 613 et s.
[2030] COHENDET M-A., *Droit constitutionnel*, *op. cit.*, p. 71.

1031. Mais l'Etat est aussi une menace, ce à quoi a répondu le libéralisme politique en permettant la protection des droits et libertés par la réduction de l'intervention étatique notamment. La transparence juridique ne peut donc être effective à n'importe quelle condition. Avant d'être juridique, la transparence des traitements algorithmiques est de nature politique. Cela implique un perfectionnement du formalisme de l'Etat de droit au service des droits humains, ce que peuvent réaliser de nouveaux contre-pouvoirs institutionnels propres à la conciliation des libertés au sein de l'environnement numérique. La Ve République souffre pour l'heure d'une dérive présidentialiste qu'il convient de conjurer par de nouveaux mécanismes institutionnels qui seraient par ailleurs susceptibles de mettre en œuvre la transparence des traitements algorithmiques. Néanmoins, au-delà des problématiques du régime constitutionnel français, la spécialisation de certains pouvoirs constitués au numérique semble inévitable.

1032. Le pouvoir législatif doit pouvoir se spécialiser à travers une chambre dédiée aux enjeux du numérique, car la conciliation entre droits et libertés ne peut être appréhendée de la même manière que sur le terrain classique pour parvenir à des objectifs particuliers, dont de transparence. Il en est de même concernant la nature et le degré de cette dernière. C'est une manière démocratique de réintégrer des problématiques techniques et juridiques pour arrêter le pouvoir des autres chambres. Le législateur originaire de la LIL de 1978 avait souhaité que certains traitements ne soient mis en œuvre qu'après un avis conforme de la CNIL, car elle était aussi pensée comme un contre-pouvoir technique, ce qu'elle n'est plus suffisamment en mesure d'effectuer. Dans la continuité de cet esprit, cette chambre bénéficierait de la légitimité politique mais aussi d'une spécialisation lui garantissant la technicité. Le pouvoir juridictionnel également gagnerait à connaître des particularités de ces enjeux.

1033. Il convient d'œuvrer pour une société civile pour nourrir les débats sur ces questions, mais aussi dans le but de concourir à l'effectivité de cette transparence. Qu'il s'agisse des régulateurs ou de la société civile[2031], ils ne pourront correctement remplir leurs rôles sans moyens suffisants. L'effectivité de cette transparence doit également reposer sur l'éthique, mais aussi et surtout sur la déontologie des nouvelles professions du numérique.

1034. Même si nous nous sommes prononcés en faveur de la transparence de ces nouveaux outils pour des raisons juridiques à savoir le maintien de l'effectivité de l'ordre juridique et l'autonomie des citoyens en démocratie, une acception très libérale de l'intérêt général, comme

[2031] PERROUD T., « Un fond pour la démocratie : perspectives théoriques (I) », *Chemins Publics*, 5 mai 2021 ; PERROUD T., « Un fond pour la démocratie : exemples de solutions (II), *Chemins Publics*, 6 mai 2021.

c'est le cas aux Etats-Unis d'Amérique pourrait aboutir au triomphe de l'opacité pour favoriser un écosystème économique.

1035. Cultiver une souveraineté numérique nationale ou européenne par le respect des droits et libertés au sein de l'environnement du numérique n'est pas un acquis. Il existe plusieurs façons d'y parvenir. Cela passe naturellement par le recours aux logiciels libres[2032], ce qui offre de nombreuses garanties y compris en matière de transparence des outils numériques. C'est également une manière de réduire notre dépendance aux technologies propriétaires. En ce sens, il s'agit aussi d'éviter de confier à des opérateurs économiques l'exercice de certaines libertés comme la liberté d'expression, notamment par l'intermédiaire d'algorithmes.

1036. Mais la transparence n'est pas une fin en soi puisqu'elle ne peut légitimer les usages. Et certaines techniques demeureront opaques. L'enjeu démocratique, par les institutions proposées, est de permettre de prendre en compte l'environnement numérique et ses particularités. Si nous ne contrôlons pas l'écosystème numérique qui conditionne l'exercice de nos libertés au sein de l'environnement numérique, alors nous devons nous affirmer en recourant à des méthodes telles que le développement de nos propres architectures techniques, ce qui peut passer dans certains cas par le développement des composants de l'ordinateur amenés à exécuter ces logiciels comme cela devrait être le cas en matière de renseignement ou de défense nationale pour ne pas dépendre d'autres entités. Naturellement, l'autorité de contrôle proposée effectuerait une transparence indirecte au nom et pour le compte de la société.

1037. Il n'est plus à exclure qu'il nous faille rejeter les technologies qui ne seraient pas en adéquation avec notre droit. Une voie doit être trouvée entre un modèle totalitaire du numérique oppressant les individus ou à l'inverse un modèle néolibéral faisant primer l'innovation du marché sur les autres droits et libertés, ce à quoi le principe de transparence au nom de l'effectivité des libertés et de l'ordre juridique permettrait d'œuvrer conformément à nos valeurs.

1038. Les personnes physiques ne sont pas les seules à subir des vulnérabilités techniques. L'Etat est également susceptible d'en être victime surtout parce que les gouvernants peuvent être tentés par le « solutionnisme technologique » comme nous l'avons illustré avec le vote électronique. Certains usages algorithmiques doivent être exclus et ce quand bien même ils

[2032] PELLEGRINI F., Souveraineté numérique : « le recours aux logiciels libres constitue la seule alternative viable, *Le Monde* [en ligne]. 21 juin 2016. [Consulté le 21 décembre 2020]. Disponible à l'adresse : https://www.lemonde.fr/idees/article/2016/06/24/la-souverainete-numerique-passe-par-le-logiciel-libre_4957781_3232.html

seraient transparents juridiquement et techniquement, car attentatoire aux libertés. Le principe de transparence des traitements algorithmiques est au cœur de la démocratie par l'observation du positionnement des puissances concurrentes au sein du cyberespace raison pour laquelle il doit être mis en œuvre pour que tous les acteurs de la société puissent se prononcer sur le devenir des choix politiques à l'ère numérique.

BIBLIOGRAPHIE INDICATIVE

(Seules figurent ici les références citées dans la thèse)

I - OUVRAGES

A - OUVRAGES JURIDIQUES

1 - Thèses et mémoires

ACHAINTRE C., *L'instance législative dans la pensée constitutionnelle révolutionnaire (1789-1799)*, Bibliothèque parlementaire et constitutionnelle, *Dalloz*, 2008, 439 p.

BEAUD O., *La puissance de l'Etat*, *PUF*, 1994, 512 p.

GOMES B., *Le droit du travail à l'épreuve des plateformes numériques*, thèse soutenue le 3 décembre 2018 à l'Université Paris X Nanterre, 496 p.

HAULBERT M., *L'interprétation normative par les juges de la QPC*, coll. Nouvelle Bibliothèque de Thèses, *Dalloz*, 2020, 1134 p.

KERLEO J-F., *La transparence en droit, Recherche sur la formation d'une culture juridique*, Bibliothèque des thèses, *Mare & Martin*, 2015, 995 p.

KOUMPLI C., *Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données à caractère personnel : étude comparée : Union européenne, Allemagne, France, Grèce, Royaume-Uni*, Thèse de doctorat, soutenue à l'Université Paris 1 Panthéon-Sorbonne le 18 janvier 2019, 645 p.

OCHOA N., *Le droit des données personnelles, une police administrative spéciale*, Thèse de doctorat, présentée et soutenue publiquement le 8 décembre 2014 à l'Université Paris I -Panthéon -Sorbonne, 763 p.

PERROUD T., *La fonction contentieuse des autorités de régulation en France et au Royaume-Uni*, Nouvelles bibliothèques de thèses, *Dalloz*, 2013, 1292 p.

REDOR-FICHOT M.-J., *De l'Etat légal à l'Etat de droit. L'évolution des Conceptions de la Doctrine Publiciste Française, 1879-1914*, *Presses Universitaires d'Aix-Marseille*, 1992, 330 p.

VIGNAL N., *La transparence en droit privé des contrats (approche critique de l'exigence)*, *Presses Universitaires d'Aix-Marseille*, 1998, 352 p.

2 - Monographies

BARRAUD B., *Repenser la pyramide des normes à l'ère des réseaux : pour une conception pragmatique du droit*, *L'Harmattan*, 2012, 394 p.

BODIN J., *Les Six livres de la République*, *Jacques du Puis*, 1576.

BOELLSTORFF T., *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*, Princeton University Press, 2008, 344 p. (*Un anthropologue dans* Second Life*. Une expérience de l'humanité virtuelle*, trad. franç. SERVAIS O., et DHEN G., Academia-L'Harmattan, Louvain-la-Neuve, 2013, 470 p.

BROGLI M., CATELAN N., CASTETS-RENARD C., DE LA CLERGERIE M., DUBOIS L., FAVRO K., JAULT-SESEKE F., GAULLIER F., GRYNWAJC S., LE BRET A., MARTIAL-BRAZ N., MATSUBARA M., MAXWELL W., PAULIN B., ROCHFELD J, STALLA-BOURDILLON S., TOULOTTE T., ZANOTTI F., ZOLYNSKI, C., *Droit des données personnelles, Les spécificités du droit français au regard du RGPD, Dalloz décryptage*, 2019, 560 p.

CARRE DE MALBERG R., *Contribution à la théorie générale de l'Etat*, *Sirey*, 1920, t. 1, 1526 p.

CHAPUS R., *Droit administratif général*, tome 1, 15e édition, 2001, *Montchrestien*, 1440 p.
CHEVALLIER J., *L'Etat de droit*, *LGDJ*, 2017, 160 p.

COHENDET M-A., *Droit constitutionnel*, *LGDJ*, 2015, 849 p.

DE BECHILLON D., *Qu'est-ce qu'une règle de Droit ?*, *Odile Jacob*, 1997, 304 p.

DE MONTESQUIEU C., *De l'esprit des lois*, *Barrillot & fils*, 1748.

DESGENS-PASANAU G., *Le correspondant « informatique et libertés »*, *LexisNexis*, 2013, 374 p.

DOUVILLE T., *Droit des données à caractère personnel : droit de l'Union européenne, droit Français*, *Lextenso*, 2021, 432 p.

DUTHEIL P-H., *Droit des associations et fondations*, 1ere édition, *Dalloz*, 2016, 1640 p.

FERAL-SCHUHL C., *Cyberdroit. Le droit à l'épreuve de l'internet*, *Dalloz*, 2020, 1852 p.

FRIER J-L, PETIT J., *Droit administratif*, 15e édition, *LGDJ*, 2021, 814 p.

HAMILTON A., JAY J., MADISON J., *Le Fédéraliste*, PolitiqueS, Classiques Garnier, réedition, 2012, 648 p.

HAMON F., TROPER M., *Droit constitutionnel*, *LGDJ*, 36e édition, 2015, 830 p.

KELSEN H., *Controverses sur la Théorie pure du droit. Remarques critiques sur Georges Scelle et Michel Virally*, *Editions Panthéon-Assas*, 2005 186 p.

LASCOMBE M., VANDENDRIESSCHE X., DE GAUDEMONT C., *Code constitutionnel et des droits fondamentaux*, *Dalloz*, 2021, 1204 p.

LASSERE B., LENOIR N, STIRN B, *La transparence administrative*, *PUF*, 1987, 256 p.

LASSERRE CAPDEVILLE J., STORCK M., CHEVRIER E., PISONI P., « Code monétaire et financier, annoté & commenté », *Dalloz*, 2020, 3482 p.

LECUYER Y., *Le droit à des élections libres*, *Conseil de l'Europe*, 2014, 140 p.

LESSIG L., *Code and Other Laws of Cyberespace*, *Basic Books*, 1999, 320 p.

LESSIG L., *Code version 2.0*, Basic Books, 2006, 431 p.

LETTERON R., *Libertés publiques*, édition 2020, 730 p.

LE TOURNEAU P., *Contrats du numérique Informatiques et Electroniques 2021/2022*, *Dalloz*, 2020, 820 p.

NEVEJANS N., *Traité de droit et d'éthique de la robotique civile*, *LEH édition*, 2017, 1232 p.

OST F. VAN DE KERCHOVE M., *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Bruxelles, Publications des Facultés universitaires Saint-Louis, 2002, ch. IV (« Les sanctions en droit : un réseau complexe aux frontières incertaines »), 598 p.

PELLEGRINI F., CANEVET S., *Droit des logiciels*, *PUF*, 2013, 616 p.

PETIT F. (dir.), *Droit et loyauté*, Thèmes et commentaire, *Dalloz*, 2015, 158 p.

RAMBAUD R., *Droit des élections et des référendums politiques*, 1e édition, *LGDJ*, , 2019, 744 p.

ROSENBLAT A., *Uberland : How Algorithms are Rewriting the Rules of Work*, *University of California Press*, 2018, 296 p.

ROUSSEAU D., *La justice constitutionnelle en Europe*, *Montchrestien*, 3e édition, 1998, 160 p.

ROUSSEAU J-J., *Du contrat social*, *Marc-Michel Rey*, 1762.

SUPIOT A., *La gouvernance par les nombres*, Cours au Collège de France, Poids et mesures du monde, *Fayard*, 2015, 520 p.

TAMBOU O., *Manuel de droit européen de la protection des données à caractère personnel*, *Bruylant*, 2020, 486 p.

TROPER M., *La séparation des pouvoirs et l'histoire constitutionnelle française*, Anthologie du droit, *LGDJ*, 2014, 250 p.

TRUCHET D., *Le droit public*, *PUF*, 2014, 126 p.

VIGOUROUX C., *Déontologies des fonctions publiques*, *Dalloz*, 2012, 752 p.

WALINE J., *Droit administratif*, 27e édition, *Dalloz*, 834 p.

B - OUVRAGES NON JURIDIQUES

BENAYOUN Y., REGNAULD I., *Technologies partout, démocratie nulle part*, *FYP*, 2020, 240 p.

CARDON D., *Culture numérique*, *Presses de la fondation nationale des sciences politiques*, 2019, 430 p.

CASILLI A. A., *En attendant les robots - enquête sur le travail du clic*, *Le Seuil*, 2019, 394 p.

CASILLO I., BARBIER R., BLONDIAUX L., CHATEAURAYNAUD F., FOURNIAU J-M., LEFEBVRE R., NEVEU C., et SALLES D. (dir.), *Dictionnaire critique et interdisciplinaire de la participation*, Paris, GIS Démocratie et Participation, 2013 [en ligne] Disponible à l'adresse : http://www.dicopart.fr/fr/dico/

CHATEAURAYNAUD F., TORNY D., *Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque*, Éditions de l'École des Hautes Études en Sciences Sociales, 1999, 476 p.

CUKIER K., MAYER-SCHOENBERGER V., *Big Data – La révolution des données est en marche*, Robert Laffont, 2014, 296 p.

ERTZSCHEID O., *L'appétit des géants. Pouvoir des algorithmes, ambitions des plateformes*, *C&F éditions*, 2017, 384 p.

HARCOURT B. E., *La société d'exposition. Désir et désobéissance à l'ère numérique*, *Seuil*, 2020, 336 p.

ITEANU O., *Quand le digital défie l'Etat de droit*, *Eyrolles*, 2016, 188 p.

JEAN A., *De l'autre côté de la Machine, Voyage d'une scientifique au pays des algorithmes*, *Editions de l'observatoire*, 2019, 204 p.

O'NEIL C., *Algorithmes. La bombe à retardement*, *Les arènes*, 2016, 340 p.

PASQUALE F., *Black Box Society : Les algorithmes secrets qui contrôlent l'économie et l'information*, *FYP éditions*, 2015, 320 p.

SADIN E., *La Silicolonisation du monde, l'irrésistible expansion du libéralisme*, *L'échappée*, 2016, 291 p.

TREGUER F., *L'utopie déchue : une contre-histoire d'internet XVe-XXIe*, *Fayard*, 2019, 350 p.

WIENER N., *La cybernétique, information et régulation dans le vivant et la machine*, *Seuil*, 2014 [1948], 376 p.

ZUBOFF S., *L'âge du capitalisme de surveillance. Le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, *Zulma*, 2020, 864 p.

II - ARTICLES ET CONTRIBUTIONS

A - ARTICLES, ETUDES ET FASCICULES JURIDIQUES

ABITEBOUL S., G'SELL F., « Les algorithmes pourraient-ils remplacer les juges », *in* G'SELL F., (dir), *Le Big Data et le droit*, Thèmes et commentaires, *Dalloz*, 2020, p. 21 à 43.

ARROYO J., « Un droit à l'oubli dans le champ des documents administratifs ? », *in* DECHENAUD D., (dir.), *Le droit à l'oubli numérique. Données nominatives - approche comparée*, *Larcier*, 2015, p. 143 à 164.

BARBIN E., « Le contrôle juridictionnel de l'outil numérique d'aide à la décision administrative », *RFDA*, 2021, p. 491 à 500.

BARRAUD B., « Le coup de data permanent : la loi des algorithmes », *Revue des droits et libertés fondamentaux*, chron. 35, 2017.

BARRAUD B., « Un algorithme capable de prédire les décisions des juges : vers une robotisation de la justice ? », *Cahiers de la justice*, 2017/1, p. 121 à 139.

BARRAUD B., « Le coup de data permanent : la loi des algorithmes », *Revue des droits et des libertés fondamentaux*, Chron. n° 35, 2017, [en ligne]. [Consulté le 3 mars 2020]. Disponible à l'adresse : http://www.revuedlf.com/droit-fondamentaux/le-coup-de-data-permanent-la-loi-des-algorithmes/

BEAUCHESNE B., « La dépendance européenne et nationale face aux nouveaux acteurs du numérique », *Dalloz IP/IT*, 2021, p. 125 à 129.

BENHAMOU B., SORBIER L., « Souveraineté et réseaux numériques », in *Politique étrangère*, 2006/3, p. 519 à 530.

BERNHEIM-DESVAUX S, « L'association de consommateurs CLCV obtient la condamnation d'une importante plateforme numérique, comparateur de produits d'assurance », *Contrat Concurrence Consommation*, n° 3, Mars 2020, comm. 54.

BEVIERE-BOYER B., « Numérique en santé : le projet de loi relatif à la bioéthique a accouché d'une souris », NEVEJANS N., (Dir.), *Données et technologies numériques. Approches juridique, scientifique et éthique, mare & martin*, 2021, p. 243 à 256.

BEVIERE-BOYER B., « Révolution technoscientifique d'amélioration : quelle éthique pour quelle humanité ? », *in* MARTINENT E., STANTON J., MAMZER M-F., (dir), *Réflexion et recherche en éthique, Mélange en honneur du professeur Christian Hervé*, *Dalloz*, 2018, p. 295 à 310.

BLIN-FRANCHOMME M-P., « Le défi d'une IA inclusive et responsable », *Droit social*, 2021, p. 100 à 105.

BOURCIER D., DE FILIPPI P., « Transparence des algorithmes face à l'Open Data : Quel statut pour les données d'apprentissage ? », *Revue française d'administration publique*, 2018, p. 525 à 537.

BOURDIEU P., « La force du droit. Eléments pour une sociologie du champ juridique », *Actes de la recherche en sciences sociales*, 1986, 64, p. 3 à 19.

BOURGEOIS M., « Vers un commissariat aux données », *La semaine juridique entreprise et affaires*, n° 48, 30 novembre 2017, p. 5 à 6.

BRAIBANT G., « La protection des droits individuels au regard du développement », *Revue internationale de droit comparé*, 1971, p. 783 à 817.

BRAIBANT G., « Droit d'accès et droit à l'information », in *Service public et libertés, Mélanges offerts au Professeur Robert-Édouard Charlier*, Éditions de l'université et de l'enseignement moderne, 1981, p. 703 à 710.

BRAMERET S., « Les libertés économiques enfin admises au pays des droits fondamentaux », *AJDA*, 2021, p. 761 à 763.

BRUNESSEN B., « L'exigence de clarté et de sincérité du débat parlementaire. Etude sur un concept régulateur de la procédure législative sous la Ve République », *RDP*, 2011, p. 431 à 462.

BRUNET F., « De la procédure au procès : le pouvoir de sanction des autorités administratives indépendantes », *RFDA*, 2013, p. 113-126

BUGE E., MORIO C., « Le Grand débat national, apports et limites pour la participation citoyenne », *RDP*, 2019, p. 1205 à 1238.

CAGNAT A., LEFEBVRE A., « Bonne fois du lanceur d'alerte : précisions bienvenues de la chambre sociale », *Légipresse*, 2020, p. 557 à 561, note sous l'arrêt de la Cour de cassation, chambre sociale, 8 juillet 2020, req. n° 18-13.593.

CARBONNIER J., « Propos introductifs » in colloque *La transparence, RJ com.*, 1993, n° spécial, p. 11.

CARCASSONNE G., « Le trouble de la transparence », *Pouvoirs*, n° 97, 2001, p. 17 à 23.

CASTETS-RENARD C., « Régulation des algorithmes et gouvernance du machine learning : vers une transparence et « explicabilité » des décisions algorithmiques ? », *Revue Droits & Affaires*, n° 15, 2018, p. 32 à 48.

CASTETS-RENARD C., « Comment construire une intelligence artificielle responsable et inclusive ? », *Recueil Dalloz*, 2020, p. 225 à 230.

CATHERINE A., ALEXIA D., PAQUIER Y., POINSIGNON D., VICOMTE D., « Chronique de jurisprudence constitutionnelle française 2015 », *Les Cahiers de la Recherche sur les Droits Fondamentaux*, n° 14, 2016, p. 113 à 136.

CHAMPEIL-DESPLATS V., « La liberté d'entreprendre au pays des droits fondamentaux », *RDT*, 2007, p. 19 à 25.

CHANTEUR J., *« La loi naturelle et la souveraineté chez Bodin », in Théologie et droit dans la science politique de l'État moderne*, Actes de la table ronde de Rome (12-14 novembre 1987), *École Française de Rome*, 1991, p. 283 à 294.

CHAPENET J., LEQUESNE ROTH C., « Discrimination et biais genrés : les lacunes juridiques de l'audit algorithmique », *Recueil Dalloz*, 2019, p. 1852 à 1857.

CHASSIN C-A., KORSAKOFF A., MAUGER-VIELPEAU L., « La vulnérabilité des migrants », *Les Cahiers de la Recherche sur les Droits Fondamentaux*, n°18, 2018, p. 55 à 63.

CHEVALLIER J., « L'intérêt général dans l'administration française », *Revue internationale des sciences* administratives, 1975, p. 325 à 350.

CHEVALLIER J., « Le mythe de la transparence administrative », *in Information et transparence administratives*, *PUF*, 1988, p. 239 à 275.

CHEVALIER J., « Les fondements du droit administratif à l'épreuve de l'Europe », *in* RAIMBAULT P. (dir.), *La puissance publique à l'heure européenne*, *Dalloz*, 2006, p. 4 à 57.

CHEVALLIER J., « De l'administration démocratique à la démocratie administrative », *Revue française d'administration publique*, *ENA*, 2011/1, p. 217 à 227.

CHEVALLIER J., « Le droit administratif vu de la science administrative », *AJDA*, 2013, p. 401 à 403.

CLUZEL-METAYER L., « Les limites de l'*open data* », *AJDA*, 2016, p. 102 à 107.

CLUZEL-METAYER L., DEBAETS E., « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA*, 2018, p. 1101 à 1111.

CLUZEL-METAYER L., « L'influence des algorithmes sur l'édiction des décisions administratives », in *Méthodes en droit administratif*, Thèmes et commentaires, *AFDA*, 2018, p. 243 à 259.

CLUZEL-METAYER L., « L'ouverture des données publiques », *in Le droit administratif au défi du numérique*, *AFDA*, 2019, p.7 à 23.

CLUZEL-METAYER L., « La datasurveillance de la Covid-19 », *RDSS*, 2020, p. 918 à 927.

CLUZEL-METAYER L., FRANCOIS A., « La protection des données personnelles à l'épreuve de la télémédecine », *RDSS*, 2020, p. 51-59

CLUZEL-METAYER L., « L'hébergement de la plateforme des données de santé par Microsoft : une validation sous surveillance », *AJDA*, 2021, p. 741 à 748.

COMBEAU P., « L'élaboration de la décision administrative à l'ère du numérique : vers l'action administrative collaborative ? », *in Le droit administratif au défi du numérique*, *AFDA*, 2019, p. 173 à 198.

Conseil constitutionnel, commentaire de la décision n° 2020-834 du 3 avril 2020, Union Nationale des Etudiants de France, p. 18, *Conseil-constitutionnel.fr* [en ligne]. [Consulté le 20 novembre 2020]. Disponible à l'adresse : https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2020834qpc/2020834qpc_ccc.pdf

CONTAG M. *et al*., « How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles », in *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2017, p. 231 à 250.

CRICHTON C., « Cookies : la CNIL sanctionne Google et Amazon », *Dalloz actualité*, 17 décembre 2020.

CRICHTON C., « Proposition de Règlement sur l'intelligence artificielle », *Dalloz IP/IT*, 2021, p. 243 à 245.

DANET A., ENGUEHARD C., « De la preuve et de l'utilisation des Systèmes Inéquitables Numériques », Les convergences du droit et du numérique, septembre 2017, Bordeaux, *INRIA* [en ligne]. [Consulté le 22 juin 2020]. Disponible à l'adresse : https://hal.inria.fr/hal-01730375/document

DARY M., BENAISSA L., « Privacy by Design : Un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz* IP/IT, 2016, p. 476 à 480.

DEBET A., « Les nouveaux instruments de conformité », *Dalloz IP/IT*, 2016, p. 592 à 596.

DECAUX M., DUVAL L., LABBAY A., PAQUIER Y., PENITOT M., « Chronique de jurisprudence des droits numériques 2017-2018 », *Cahiers de la Recherche sur les Droits fondamentaux*, n° 17, 2019, p. 217 à 232.

DELPECH X., « Fraude à la carte bancaire : aspects juridiques », *Recueil Dalloz*, 2000, p. 219 à 223.

DELPEREE F., « L'interprétation de la constitution ou la leçon de musique », *in* MELIN-SOUCRAMANIEN F. (dir.), *L'interprétation constitutionnelle*, *Dalloz*, 2005, p. 241 à 248.

DELTORN J-M., « Le droit des données personnelles face à l'opacité des algorithmes prédictifs : les limites du principe de transparence », *in* NETTER E., (dir), *Regards sur le nouveau droit des données personnelles*, *LGDJ*, 2019, p. 153 à 206.

DE MONTECLER M-C., « Philippe Pichon, lanceur d'alerte ou indiscret », *AJDA*, 2017, p. 709 à 710, note sous l'arrêt du Conseil d'Etat, 31 mars 2017, req 392316.

DEROSIER J-P., « Les limites du concept de souveraineté numérique », TURK P., ET VALLAR C. (dir.), *La souveraineté numérique : le concept, les enjeux, mare & martin*, Droit public, 2017, p. 77 à 90.

DOUVILLE T., « Parcoursup à l'épreuve de la transparence des algorithmes », *Dalloz IP/IT*, 2019, p. 390 à 393.

DOUVILLE T., « Parcoursup et le secret des algorithmes », *Dalloz IP/IT*, 2019, p. 700 à 702.

DOUVILLE T., HERVOCHON C., NOEL E., PAQUIER Y., « Les vulnérabilités numériques », *Les Cahiers de la Recherche sur les Droit Fondamentaux*, 2020, p. 111 à 119.

DUCLERCQ J-B., « Les effets de la multiplication des algorithmes informatiques sur l'ordonnancement juridique », *Communication Commerce Electronique*, n° 11, étude 20, 2015, p. 1 à 7.

DUCLERCQ J-B., « Le droit public à l'ère des algorithmes », *RDP*, 2017, p. 1401 à 1434.

DUCLERCQ J-B., « Les algorithmes en procès », *RFDA*, 2018, p. 131 à 142.

DUBOUT E., « Le Conseil d'Etat, gardien de la sécurité », *RDLF*, 2021, chron. n° 18, *Revuedlf.com* [en ligne] [Consulté le 23 avril 2021]. Disponible à l'adresse : http://www.revuedlf.com/droit-ue/le-conseil-detat-gardien-de-la-securite/

EDWARDS L., VEALE M., Slave to the Algorithm ? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, in *Duke Law & Technology Review*, vol. 18, 2017, 67 p. [en ligne]. [Consulté le 15 juin 2020]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855

ENGUEHARD C., « Vote par internet : failles techniques et recul démocratique », *Jus Politicum*, n° 2 [en ligne]. [Consulté le 12 mars 2021]. Disponible à l'adresse : http://juspoliticum.com/article/Vote-par-internet-failles-techniques-et-recul-democratique-74.htm

ENGUEHARD C., GRATON J-D., « Machines à voter et élections politiques en France : étude quantitative de la précision des bureaux de vote », *Cahiers Droit, Sciences & Technologies*, n° 4, 2014, p. 159 à 198.

ENGUEHARD C., SHULGA-MORSKAYA T., De l'annulation d'élections par Internet par le moyen des insuffisances du système de vote, *Les convergences du droit et du numérique* [en ligne]. 13 mars 2018 [Consulté le 22 septembre 2020]. Disponible à l'adresse : https://hal.inria.fr/hal-01730380

FJELD J, ACHTEN N, HILLIGOSS H, NAGY A, SRIKUMAR M., Principled *Artifical Intelligence : Mapping Consensus in Ethical and Rights-Based Approches to Principles for AI*, Berkman Klein Center Research Publication, n° 2020-1, 39 p. [en ligne]. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482

FOEGLE J-P., SLAMA S., Refus de transmission d'une QPC sur la protection des fonctionnaires lanceurs d'alerte, *La Revue des droits de l'homme* [en ligne]. 14 mars 2014 [Consulté le 2 mai 2020]. Disponible à l'adresse : https://journals.openedition.org/revdh/628#quotation

FORTIER C., « La liberté du chercheur public », *in* LARRIEU J. (dir.), *Qu'en est-il du droit de la recherche ?*, *Presses Universitaires Toulouse 1 Capitole*, 2008, p. 113 à 129.

GHEVONTIAN R., « La notion de sincérité du scrutin », *Cahiers du Conseil constitutionnel*, n° 13, janvier 2003, p. 45 à 54.

GOODMAN B., FLAXMAN S., European Union regulations on algorithmic decision-making and a « right to explanation », *AI Magazine*, vol. 38, n° 3, 2017, p. 50 à 57.

GRABIAS F., « La transparence administrative, un nouveau principe ? », *La Semaine Juridique Administrations et Collectivités territoriales*, n° 50, n°2340, 17 décembre 2018, p. 1 à 5.

GROFFE-CHARRIER J., « La loi est-elle dictée par le code ? », *Dalloz IP/IT*, 2020, p. 602 à 606.

G'SELL F., « Remarque sur les aspects juridiques de la souveraineté « numérique » », *La Revue des juristes de Science Po*, n° 19, octobre 2019, p. 52 à 60.

HALPERIN J-L., « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *Les nouveaux Cahiers du Conseil constitutionnel*, n° 48, 2015, p. 59 à 68.

HARVARD LAW REVIEW, *State v. Loomis, Wisconsin Suprem Court Requiers Warning Before Use of Algorithmic Risk Assessments in Sentencing, Havard Law Review*, 2017, vol. 130, n° 5, p. 1530, Harvardlawreview.org [en ligne] [Consulté le 2 septembre 2020]. Disponible à l'adresse : https://harvardlawreview.org/2017/03/state-v-loomis/

HEDARY D., « Les surprises de la Charte de l'environnement : analyse des quatre années de jurisprudence », *Droit de l'environnement*, n° 171, septembre 2009, p. 11 à 15.

HERAUD G., « La validité juridique », *in Mélanges Maury*, *Dalloz*, 1960, p. 477 à 490.

JAUME L., « « Démocratie illibérale » : une nouvelle notion ? », Constitutions, *Dalloz*, 2019, p. 177 à 186.

JEGOUZO Y., « Le droit à la transparence administrative », *Etudes et documents du Conseil d'Etat*, n° 43, 1992.

JOUNIN N., « Le caché de La Poste. La genèse de temps virtuels pour organiser le travail des facteurs », *La revue de l'IRES*, n° 93, 2017, p. 25 à 50.

KAMINSKI M, E., « Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability », *Southern California Law Review*, vol. 92, n° 6, 2019 [en ligne] 03 avril 2019, mis à jour le 11 novembre 2019. [Consulté le 15 juin 2020]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351404

KERLEO J-F., « La constitutionnalisation d'un principe de transparence de la vie publique », *ADJA*, 2020, p. 1137 à 1139.

LATIL A., « En attendant la Déclaration de droits fondamentaux du numérique », *Dalloz IP/IT*, 2021, p. 593 à 597.

LEQUESNE ROTH C., « La transparence : vice ou vertu de la démocratie ? », in RIDEAU J (dir.)., *La transparence dans l'Union européenne, Mythe ou principe juridique*, 1998, *LGDJ*, p. 11 à 18.

LEQUESNE ROTH C., « De l'éthique et des algorithmes : pour une juridicisation des enjeux », *Recueil Dalloz*, 2020, p. 1833 à 1835.

LETTERON R., Parcoursup devant le Conseil d'Etat, *Liberté, Libertés chéries. Veille juridique sur les droits de l'homme et les libertés publiques* [en ligne]. 18 juin 2019 [Consulté le 18 janvier 2020]. Disponible à l'adresse : https://libertescheries.blogspot.com/2019/06/parcoursup-devant-le-conseil-detat.html?fbclid=IwAR1Wk-y44fInC6nRP_pghPwW6i-0hRDvhUJlOu-Zkt1X8-igyA3HDPWu75Y

LETTERON R., Facebook crée sa « Cour Suprême », *Liberté, Libertés chéries. Veille juridique sur les droits de l'homme et les libertés publiques* [en ligne]. 9 mai 2020 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://libertescheries.blogspot.com/2020/05/facebook-cree-sa-cour-supreme-rien-que.html

LOCHAK D., « L'alerte éthique, entre dénonciation et désobéissance », *AJDA*, 2014, p. 2236 à 2241.

LOISEAU G., « Le comité social et économique », *Droit social*, 2017, p. 1044 à 1049.

LYON-CAEN A, « L'évaluation des salariés », *Recueil Dalloz*, 2009, p. 1124 à 1227, note sous le jugement du TGI de Nanterre 5 septembre 2008, RG. 08/05737.

MARCHAND J., « Réflexion sur le principe de transparence », *RDP*, n° 3, 2014, p. 677 à 686.

MARTY F., « *La protection des algorithmes par le secret des affaires, entre risques de faux négatifs et risques de faux positifs* », *Revue internationale de droit économique*, 2019/2, p. 211 à 237.

MATHIS B., « Faut-il réglementer les crypto-actifs en fonction de leur consommation d'électricité », *Revue internationale des services financiers*, 2020, p. 59 à 62.

MAXIMIN N., « Données personnelles : pourquoi la CNIL publie-t-elle son registre RGPD ? », *Dalloz actualité*, 6 décembre 2019.

MAYSON S. G., *Bias In, Bias Out*, *The Yale Law Journal*, 2018-2019, Vol. n° 128, p. 2122 à 2473.

MEKHANTAR J., « L'annulation des retenues effectuées sur le traitement d'un directeur d'école ayant refusé de de renseigner une enquête académique », *AJFP*, 2011, p. 89 à 91.

MEKHANTAR J., « Le citoyen, la machine à voter et le juge », *in* FAVIER L., DOUEIHI M. (dir.), *La démocratie dématérialisée. Enjeux du vote électronique*, *Le Genre humain*, vol. 51, n° 2, 2011, *Le Seuil*, p. 125 à 146.

MENECEUR Y., « Les enseignements des éthiques européennes de l'intelligence artificielle », *La semaine juridique*, n°12, 2019, p. 552 à 558.

MIGAYRON S., « Contradictoire et confidentialité dans les expertises des litiges du monde numérique : une mission impossible ? », *Revue communication-commerce électronique*, n° 4, avril 2020, p. 46 à 48.

MILANO L., « Qu'est-ce qu'une juridiction ? La question a-t-elle encore une utilité ? », *RFDA*, 2014, p. 1119 à 1130.

MONTECLER M-C., « Le Conseil constitutionnel définit la manipulation de l'information », *AJDA*, 2019, p. 5 à 5.

MOURIESSE E., « L'opacité des algorithmes et la transparence administrative », *RFDA*, 2019, p. 45 à 54.

MUSSO P., « Critique de la notion de « territoires numériques », *Quaderni*, n° 66, printemps 2008, p. 15 à 29.

NETTER E., « A quoi sert le principe de transparence en droit des données personnelles ? », *Dalloz IP/IT*, 2020, p. 611 à 615.

NEVEJANS N., « La légalité des robots de guerre dans les conflits internationaux », *Recueil Dalloz.* 2016, p. 1273 à 1278.

NEVEJANS N., « Les problématiques juridiques et éthiques posées par les robots en santé mentale », *in* TISSERON S., TORDO F (dir.)., *Robots, de nouveaux partenaires de soins psychiques*, *Erès*, 2018, p. 43 à 56.

NEVEJANS N., « L'influence des logiciels d'aide à la décision sur le processus décisionnel médical à la lumière du droit et de l'éthique », *in* HERVE C., STANTON-JEAN M (dir.)., *Innovations en santé publique, des données personnelles aux données massives (BIG DATA). Aspects cliniques, juridiques et éthiques*, *Dalloz*, 2018, p.113 à 128

PAPADAMAKI I., « L'obligation de motivation en droit administratif français sous l'influence du droit de l'Union européenne », *RDP*, 2017, p. 1245 à 1260.

PASQUALE F., The Second Wave of Algorithmic Accountability, *LMP Project.org* [en ligne]. 25 novembre 2019 [Consulté le 12 avril 2021]. Disponible à l'adresse : https://lpeproject.org/blog/the-second-wave-of-algorithmic-accountability

PASQUALE F., « From territorial to functional Sovereignty: The case of Amazon », *lpeblog.com, Blog Law and Political Economy* [en ligne]. 6 décembre 2017 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/

PAULIAT H., « La décision administrative et les algorithmes : une loyauté à consacrer », *RDP*, 2018, p. 641 à 647.

PERROUD T., « Le Conseil constitutionnel et les portes étroites », *Blog Jus Politicum* [en ligne]. 16 mars 2017. [Consulté le 6 octobre 2020]. Disponible à l'adresse : https://blog.juspoliticum.com/2017/03/16/le-conseil-constitutionnel-et-les-portes-etroites/

PERROUD T., « Essai sur les caractères néolibéraux du droit administratif contemporain », *in Mélanges en l'honneur de Serge Regourd*, 2018, NC.

PERROUD, T., « L'anonymisation des décisions de justice est-elle constitutionnelle ? Pour la consécration d'un principe fondamental reconnu par les lois de la République de publicité de la justice », in *JP blog* [en ligne]. 11 mars 2019 [Consulté le 12 juin 2020]. Disponible à l'adresse : http://blog.juspoliticum.com/2019/03/11/lanonymisation-des-decisions-de-justice-est-elle-constitutionnelle-pour-la-consecration-dun-principe-fondamental-reconnu-par-les-lois-de-la-republique-de-publicite-de-la-justice/

PERROUD T., « L'open data des décisions de justice », *Recueil Dalloz*, 2021, p. 344 à 344.

PERROUD T., « Un fond pour la démocratie : perspectives théoriques (I) », *Chemins Publics*, 5 mai 2021

PERROUD T., « Un fond pour la démocratie : exemples de solutions (II), *Chemins Publics*, 6 mai 2021.

PERROUD T., BOURDON P., Cluzel-Métayer L., RENAUDIE O., « L'open data ou comment accomplir (enfin !) la promesse de publicité de la justice », *Dalloz actualité*, 12 octobre 2020.

QUILICHINI P., « Réguler n'est pas juger », *AJDA*, 2004, p. 1060 à 1069.

RATTI L., PEYRONNET M., « Controverse : algorithmes et risque de discrimination : quel contrôle du juge ? », *Revue de droit du travail*, 2021, p. 81.

RIVERO J., « La transparence administrative en Europe », rapport de synthèse « Transparence, je n'aime pas les mots flous…il y a malfaçon, opacité de la transparence », *Annuaire européen d'administration publique*, 1990, p. 307.

ROBLOT-TROZIER A., Le Conseil constitutionnel et les sources du droit constitutionnel, *Jus Politicum*, n° 21 [en ligne]. [Consulté le 15 décembre 2020]. Disponible à l'adresse : http://juspoliticum.com/article/Le-Conseil-constitutionnel-et-les-sources-du-droit-constitutionnel-1261.html

ROCHFELD J., ZOLYNSKI C., « La « loyauté » des « plateformes ». Quelles plateformes ? Quelle loyauté ? », *Dalloz IP/IT*, 2016, p. 520 à 524.

RODA J., « L'entente algorithmique », *La Semaine Juridique Edition Générale* n° 28, 15 Juillet 2019, doctr. 785, p. 1371 à 1377.

ROUSSEAU D., La démocratie continue : fondements constitutionnels et institutions d'une action continuelle des citoyens, *Confluence des droits_La revue* [en ligne]. Février 2020 [Consulté le 3 avril 2020]. Disponible à l'adresse : https://confluencedesdroits-larevue.com/?p=726

ROUX-DEMARE F.-X., « La notion de vulnérabilité, approche juridique d'un concept polymorphe », *Les cahiers de la justice, Vulnérabilités*, n° 4, 2019, p. 619 à 630

RRAPI P., Le « contrôle abstrait » de constitutionnalité comme obstacle à l'identification des discriminations, *La Revue des Droits de l'Homme*, 2016, n° 9 [en ligne]. [Consulté le 23 mars 2020]. Disponible à l'adresse : https://journals.openedition.org/revdh/2060?lang=en

RUFFO M., « La robotisation de la guerre et de la décision militaire : efficacité et éthique », in JACQUEMIN H., DE STREEL A., (dir.), *L'intelligence artificielle et le droit*, *Larcier*, 2017, p. 437 à 470.

RYAN C., KEATS CITRON D., The Automated Administrative State: A Crisis of Legitimacy, 9 Mars 2020, Emory Law Journal, Forthcoming, SSRN [en ligne]. [Consulté le 25 novembre 2020]. Disponible à l'adresse : https://ssrn.com/abstract=3553590

SABRINNI F, « La notion de plateforme au cœur des nouvelles relations entre professionnels : regards croisés entre deux réglementations : P2B vs loi pour une République numérique », *RTD com*., 2020, p. 215 à 224.

SIRINELLI P., PREVOST S., « Reconnaissance émotionnelle, connaissance irrationnelle ? », *Dalloz IP/IT*, 2021, p. 237 à 239.

SIZAIRE V., « L'art du trompe l'œil », *La Revue des Droits de l'Homme*, [en ligne]. Septembre 2021 [Consulté le 22 septembre 2021]. Disponible à l'adresse : https://journals.openedition.org/revdh/12968#abstract.

SLAMA S., « Le lanceur d'alerte, une nouvelle figure du droit public ? », *AJDA*, 2014, p. 2229 à 2235.

SMITH E., *Constitutional justice under old constitutions*, *Revue internationale de droit comparé*, 1996, n° 4, p. 972 à 974

SORDINO M-C., « Première transaction pénale en cas d'obsolescence « logicielle » constitutive de pratiques commerciales trompeuses », *RSC*, 2020, p. 960 à 961.

THE CITIZEN LAB, To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada [en ligne]. [Consulté le 2 décembre 2020]. Disponible à l'adresse : https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

TROPER M., « L'interprétation constitutionnelle », *in* MELIN-SOUCRAMANIEN F. (dir.), *L'interprétation constitutionnelle*, *Dalloz*, 2005, p. 13 à 25.

TÜRK P., « La souveraineté des Etats à l'épreuve d'internet », *RDP*, 2013, p. 1489 à 1500.

VAN LANG A., « Le principe de participation : un succès inattendu », *Les nouveaux Cahiers du Conseil constitutionnel*, n°43, 2014, p. 25 à 41.

VASSAK K., « Les différentes catégories des droits de l'homme », *in* LAPEYRE A., DE TINGUY F., VASAK K. (dir.), *Les dimensions universelles des droits de l'homme*, UNESCO-Bruylant, 1990, p. 297 à 316.

VEALE M., ZUIDERVEEN BORGESIUS F., « Demystifying the Draft EU Artificial Intellingence Act », *Computer Law Review International*, 2021, p. 97 à 112.

VEDEL G., « *Souveraineté et supra constitutionnalité* », *in* La souveraineté, *Revue Pouvoirs*, n° 67, novembre 1993, p. 79 à 97.

WACHTER S., MITTELSTADT B., FLORIDI L., « Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation », *International Data Privacy Law*, vol. 7, mai 2017, p. 76 à 99.

WHITMAN J. Q., The Two Western Cultures of Privacy : Dignity versus Liberty, 2003, *Papers.ssrn.com* [en ligne]. [Consulté le 5 avril l2021]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=476041

ZALNIERIUTE M., « « Transparency-Washing » In The Digital Age : A Corporate Agenda of Procedural Fetishism », *Critical Analysis of Law*, UNSW Law Research Paper, 8(1), 2021, p. 21 à 33.

B - ARTICLES ET ETUDES NON JURIDIQUES

CARDON D., « Le pouvoir des algorithmes », *La Datacratie*, *Revue Pouvoirs*, n° 164, janvier 2018, p. 63 à 73.

DOWEK G., « Les origines de l'informatique », *Cahiers philosophiques*, Réseau Canopé, n° 141, 2015/2, p. 7 à 15.

ERTZSCHEID O., Avec les gilets jaunes, Facebook dispose d'une formidable base de données d'opinion, *Alternatives économiques* [en ligne]. 13 décembre 2018 [Consulté le 29 novembre 2020]. Disponible à l'adresse : https://www.alternatives-economiques.fr/gilets-jaunes-facebook-dispose-dune-formidable-base-de-donnees/00087367

ERTZSCHEID O., Trump, Google, l'idiot utile, les architectures techniques toxiques et le meilleur des algorithmes possibles, *Affordance.info, Le blog d'un maître de conférences en sciences de l'information* [en ligne]. 17 décembre 2018 [Consulté le 3 mars 2020]. Disponible à l'adresse : https://www.affordance.info/mon_weblog/2018/12/meilleur-algorithmes-possibles-trump-idiot.html

FOURNIAU J-M., Le « grand débat national » : un exercice inédit, une audience modérée au profil socioéconomique opposé à celui des Gilets jaune, *Observatoire des débats* [en ligne]. 11 avril 2019 [Consulté le 26 novembre 2020]. Disponible à l'adresse : https://observdebats.hypotheses.org/413

HARNAY S., MARTY F., TOLEDANO J., Concurrence et risque algorithmique : quelle régulation des algorithmes ?, 24 p *Chairgovreg.fondation-dauphine.fr* [en ligne]. [Consulté le 12 septembre 2020]. Disponible à l'adresse : https://chairgovreg.fondation-dauphine.fr/sites/chairgovreg.fondation-dauphine.fr/files/attachments/GovRegNotes_Concurrence%20et%20risque%20algorithmique.pdf

LECUN Y., Qu'est-ce que l'intelligence artificielle ?, *Collège de France* [en ligne]. [Consulté le 28 octobre 2020]. Disponible à l'adresse : https://www.college-de-france.fr/site/yann-lecun/Recherches-sur-l-intelligence-artificielle.htm#:~:text=On%20pourrait%20dire%20que%20l,humains%20et%20%C3%A0%20certains%20animaux.&text=Le%20domaine%20de%20l'IA,comme%20essentiel%20%C3%A0%20l'intelligence

LACROIX G., « Cybernétique et société : Norbert Wiener ou les déboires d'une pensée subversive », *Terminal*, n° 61, 1993, p. 4 à 18.

LESUEUR F., Pourquoi l'open-source n'apporte (presque) rien face aux critiques contre StopCovid », *Flesueur.medium.com* [en ligne]. 13 mai 2020 [Consulté le 25 novembre 2020]. Disponible à l'adresse : https://flesueur.medium.com/pourquoi-lopen-source-n-apporte-presque-rien-face-aux-critiques-contre-stopcovid-24a9dcbb68fe

LESUEUR F., Privacy de StopCovid : La dure réalité de l'implémentation face à la théorie de la spécification, *Flesueur.medium.com* [en ligne]. 11 juin 2020. [Consulté le 26 janvier 2021]. Disponible à l'adresse : https://flesueur.medium.com/privacy-de-stopcovid-la-dure-r%C3%A9alit%C3%A9-de-limpl%C3%A9mentation-face-%C3%A0-la-th%C3%A9orie-de-la-sp%C3%A9cification-9021a4ca2b6a

MENECEUR Y., L'éthique, insuffisante à réguler seule les technologies numérique et l'intelligence artificielle, *Blog Le temps électrique* [en ligne]. 7 mai 2020 [Consulté le 2 mars 2021]. Disponible à l'adresse : https://lestempselectriques.net/index.php/2020/05/07/linsuffisance-de-lethique-a-reguler-lintelligence-artificielle/

PELLEGRINI F., « Chaînes de confiance et périmètres de certification : le cas des systèmes de "vote électronique" », Rapport de recherche, RR-8553, 30 p. 2014, *INRIA* [en ligne]. 27 juillet 2014, mis à jour le 11 février 2021. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://hal.inria.fr/hal-01010950v4

POMMIER E., « Ethique et politique chez Hans Jonas et Hannah Arendt », *Revue de métaphysique et de morale*, 2013/2, n° 78, p. 271 à 286

ROUVROY A., BERNS T., « Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps « numériques »… », *Multitudes*, n° 40, 2010/1, p. 88 à 103.

ROUVROY A., BERNS T., « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux*, 2013/1, n° 177, p. 163 à 196

UC SAN DIEGO, Researchers find Computer Code that Volkswagen Used to Cheat Emissions Tests, in *Jacobsschool.ucsd.edu* [en ligne]. [Consulté le 16 janvier 2021]. Disponible à l'adresse : https://jacobsschool.ucsd.edu/news/release?id=2213

III - AUTRES DOCUMENTS

A - DISCOURS

DE GAULLE C., Discours prononcé à Epinal 29 septembre 1946, *Mjp.univ-perp.fr* [en ligne]. [Consulté le 2 janvier 2021]. Disponible à l'adresse : https://mjp.univ-perp.fr/textes/degaulle29091946.htm

DE GAULLE C., Le discours de Bayeux (1946), *Elysee.fr* [en ligne]. [Consulté le 25 janvier 2021]. Disponible à l'adresse : https://www.elysee.fr/la-presidence/le-discours-de-bayeux-194

B - ARTICLES DE PRESSE ET SITES WEB DIVERS

ADELICO, LDH, SAF et al., Contribution extérieure (dite « porte étroite ») auprès du Conseil Constitutionnel sur la saisine n° 2020-800 DC du 9 mai 2020, p. 26 à 27, *Vox public.org* [en ligne], [Consulté le 1er juin 2020]. Disponible à l'adresse : https://www.voxpublic.org/IMG/pdf/contri_ext_loi_prorog_adelico_saf_sm_ldh.pdf

AGENCE FRANCE PRESSE, Prix des billets : Lufthansa dans le viseur du gendarme Allemand, *L'Express* [en ligne]. 28 décembre 2017. [Consulté le 25 janvier 2021]. Disponible à l'adresse : https://lexpansion.lexpress.fr/actualites/1/actualite-economique/prix-des-billets-lufthansa-dans-le-viseur-du-gendarme-allemand_1972198.html

AIDE YOUTUBE, Fonctionnement de Content ID, *Support.google.com* [en ligne]. [Consulté le 12 juin 2020]. Disponible à l'adresse : https://support.google.com/youtube/answer/2797370?hl=fr

AÏT-KACIMI N., Algorithmes en folie, Krachs en série, Les Echos.fr [en ligne]. 1er juin 2013 (consulté le 27 août 2021). Disponible à l'adresse : http://archives.lesechos.fr/archives/2013/Enjeux/00301-032-ENJ.htm

AÏT-KACIMI N., Trading : les « robots » rechignent à livrer leurs secrets au régulateur, *Les Echos* [en ligne]. 14 novembre 2019. [Consulté le 26 février 2020]. Disponible à l'adresse : https://www.lesechos.fr/finance-marches/marches-financiers/les-robots-rechignent-a-livrer-leurs-secrets-au-regulateur-1147749

Site internet de *Algorithm Watch* [en ligne] [Consulté le 25 novembre 2019]. Disponible à l'adresse : https://algorithmwatch.org/en/

Site internet de *Algotransparency* [en ligne] [Consulté le 25 novembre 2019]. Disponible à l'adresse : https://www.algotransparency.org/

AMER-YAHIA S., MULHEM P., Le testing algorithmique de la discrimination à l'embauche (2), *Binaire, Le Monde.fr* [en ligne]. 10 janvier 2020 [Consulté le 5 novembre 2020]. Disponible à l'adresse : https://www.lemonde.fr/blog/binaire/2020/01/10/le-testing-algorithmique-de-la-discrimination-a-lembauche-2/

ARBORUS, ORANGE, Charte internationale pour une I.A inclusive, *Charteia.arborus.org* [en ligne] [Consulté le 3 avril 2021]. Disponible à l'adresse : https://charteia.arborus.org/

AUSTRALIAN GOVERNMENT, DEPARTMENT OF INDUSTRY, SCIENCE, ENERGY AND RESOURCES, Al Ethics Principles, *Industry.gov.au* [en ligne] [Consulté le 22 mars 2021]. Disponible à l'adresse : https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles

BAILLY J-P., BELLAOUI N. et al., Rapport du Collège des garants du grand débat national, p. 7, *Grand Débat.fr* [en ligne]. 9 avril 2019. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://granddebat.fr/media/default/0001/01/ee2712c96c5035c3c2913174a7b5535fc52642a4.pdf

BARLOW J-P., Déclaration d'indépendance du cyberespace, *in* BLONDEAU O., éd., *Libres enfants du savoir numérique. Une anthologie du "Libre"*. Paris, Éditions de l'Éclat, « Hors collection », 2000, p. 47 à 54. [en ligne] [Consulté le 2 mars 2020]. Disponible à l'adresse : https://www.cairn.info/libres-enfants-du-savoir-numerique--9782841620432-page-47.htm

BELLANGER P., De la souveraineté en général et de la souveraineté numérique en particulier, *Les Echos* [en ligne]. 30 août 2011. [Consulté le 3 septembre 2020]. Disponible à l'adresse : http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm

BERNE X., Transparence des algorithmes publics : l'avertissement du Conseil constitutionnel, *Nextinpact* [en ligne]. 18 juin 2018. [Consulté le 12 avril 2020]. Disponible à l'adresse : https://www.nextinpact.com/article/28508/106743-transparence-algorithmes-publics-lavertissement-conseil-constitutionnel

BERNE X., Sous pression, Bercy ouvre les codes sources des modèles Mésange, Opale et Saphir, *Next-Impact* [en ligne]. 06 septembre 2018 [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.nextinpact.com/news/107001-sous-pression-bercy-ouvre-codes-sources-modeles-mesange-opale-et-saphir.htm

BINAIRE, Le testing algorithmique de la discrimination à l'embauche (2), *Le Monde.fr* [en ligne]. 10 janvier 2020 [Consulté le 12 juin 2021]. Disponible à l'adresse : https://www.lemonde.fr/blog/binaire/2020/01/10/le-testing-algorithmique-de-la-discrimination-a-lembauche-2/

BOUCHER P., « *Affaire SAFARI ou la chasse aux français* », in *Le Monde*, 21 mars 1974, p. 9

BOUNEAU C., « Introduction », in *Histoire, économie & société*, 2016/1, 35e année, p. 5 à 13, note 5 [en ligne]. [Consulté le 22 février 2020]. Disponible à l'adresse : https://www.cairn.info/revue-histoire-economie-et-societe-2016-1-page-5.htm#no5

BRANDY G., Maximilian Schrems : « Les termes de Facebook ne sont pas valides selon les lois européennes », *Le Monde* [en ligne], 04 août 2014, mis à jour le 14 août 2014. [Consulté le 04 octobre 2020]. Disponible à l'adresse : https://www.lemonde.fr/pixels/article/2014/08/07/maximilian-schrems-le-but-est-de-faire-respecter-a-facebook-la-legislation-europeenne_4468090_4408996.html

CCNE, Création du comité pilote d'éthique du numérique, *CCNE-éthique.fr* [en ligne]. 2 décembre 2019 [Consulté le 16 juin 2020]. Disponible à l'adresse : https://www.ccne-ethique.fr/sites/default/files/communique_lancement_comite_numerique.pdf

CAPITAL, Intelligence artificielle : la Bourse bientôt contrôlée par des boîtes noires ?, *Capital.fr* [en ligne]. 02 décembre 2019 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.capital.fr/entreprises-marches/intelligence-artificielle-la-bourse-bientot-controlee-par-des-boites-noires-1356599

Site internet du *Centre Internet et Société* [en ligne] [Consulté le 2 mars 2021]. Disponible à l'adresse : https://cis.cnrs.fr/about/

CHATELLLIER R., Des tests génétiques dits récréatifs, mais pas inoffensifs, *Linc.cnil.fr* [en ligne]. 13 septembre 2018. [Consulté le 2 octobre 2020]. Disponible à l'adresse : https://linc.cnil.fr/fr/des-tests-genetiques-dits-recreatifs-mais-pas-inoffensifs#:~:text=En%20France%2C%20ce%20type%20de,'un%20tiers%2C%20ou%20l'

CHIGNARD S., Algorithmes publics : des élèves de l'ENA formulent une série de recommandations sur les enjeux d'éthique et de responsabilité, *Le blog d'Etalab* [en ligne]. 20 janvier 2020 [Consulté le 30 janvier 2020]. Disponible à l'adresse : https://www.etalab.gouv.fr/algorithmes-publics-des-eleves-de-lena-formulent-une-serie-de-recommandations-sur-les-enjeux-dethique-et-de-responsabilite

CHIGNARD S., Algorithmes publics : Etalab publie un guide à l'usage des administration, *Etalab.gouv.fr* [en ligne]. 15 mars 2019. [Consulté le 16 novembre 2020]. Disponible à l'adresse : https://www.etalab.gouv.fr/algorithmes-publics-etalab-publie-un-guide-a-lusage-des-administrations

CHIGNARD S., Evaluer les impacts des algorithmes : publication d'une étude internationale réalisée à la demande d'Etalab, *Etalab.gouv.fr* [en ligne]. 13 juillet 2021. [Consulté le 21 juillet 2021]. Disponible à l'adresse : https://www.etalab.gouv.fr/evaluer-les-impacts-des-algorithmes-publication-dune-etude-internationale-realisee-a-la-demande-detalab

CIGREF, Déontologie des usages des Systèmes d'Information, Principes fondamentaux », *Cigref.fr* [en ligne] [Consulté le 2 mars 2020]. Disponible à l'adresse : https://www.cigref.fr/cigref_publications/RapportsContainer/Parus2006/2006_-_Deontologie_des_usages_des_SI_CIGREF_-_CEA-CED_Rapport_Web.pdf

CISPE, *Code de conduite des Fournisseurs d'infrastructures Cloud relatif à la Protection des données*, du 9 février 2021

CORI N., A la recherche des doléances perdues, *Les jours* [en ligne]. 18 juillet 2021 [Consulté le 23 octobre 2020]. Disponible à l'adresse : https://lesjours.fr/obsessions/cahiers-doleances-grand-debat/ep1-gilets-jaunes/

CORI N., Grand débat : l'illusion perdue de l'open data, *Les jours* [en ligne]. 3 janvier 2020 [Consulté le 23 octobre 2020]. Disponible à l'adresse : https://lesjours.fr/obsessions/gilets-jaunes/ep43-grand-debat-resultats/

COUR DE CASSATION, Open justice & L.A.B.E.L. : l'innovation technologique au service de l'anonymisation et de la diffusion de la jurisprudence, *Cour de cassation.fr* [en ligne]. [Consulté le 15 juin 2020]. Disponible à l'adresse : https://www.courdecassation.fr/institution_1/open_data_dematerialisation_7985/open_data_decisions_justice_7821/l.a.b.e.l._innovation_9130/

DECLARATION DE MONTREAL IA RESPONSABLE, La déclaration de Montréal pour un développement responsable de l'intelligence artificielle, *Declaration Montreal IA Responsable.com* [en ligne] [Consulté le 12 décembre 2020]. Disponible à l'adresse : https://www.declarationmontreal-iaresponsable.com/la-declaration

DUBARLE P., Une nouvelle science : la cybernétique. Vers la machine à gouverner…La manipulation mécanique des réactions humaines créera-t-elle un jour le « meilleur des mondes » ? Les premiers grands relais du cerveau humain - le dépassement du système nerveux – Les processus de la pensée probabiliste – Un prodigieux « jeu de l'homme » - Vers le bonheur (?) statistique des masses, *Le Monde* [en ligne]. 28 décembre 1948. [Consulté le 17 septembre 2020]. Disponible à l'adresse : http://www.nanomonde.org/IMG/pdf/Dubarle_1948.pdf

DGCCRF, Classement trompeur des hébergements touristiques par Google : une enquête de la DGCCRF conduit au paiement d'une amende transactionnelle de 1,1M€, *Economie.gouv.fr* [en ligne]. 15 février 2021 [Consulté le 18 février 2021].

Disponible à l'adresse : https://www.economie.gouv.fr/dgccrf/classement-trompeur-des-hebergements-touristiques-par-google-une-enquete-de-la-dgccrf-0

DGCCRF, Les obligations d'information des plateformes numériques, *Economie.gouv.fr* [en ligne]. 21 avril 2020 [Consulté le 5 février 2021]. Disponible à l'adresse : https://www.economie.gouv.fr/dgccrf/les-obligations-dinformation-des-plateformes-numeriques

DGCCRF, Transaction avec le groupe APPLE pour pratique commerciale trompeuse, *economie.gouv.fr* [en ligne]. 7 février 2020. [Consulté le 12 mars 2020]. Disponible à l'adresse : https://www.economie.gouv.fr/dgccrf/transaction-avec-le-groupe-apple-pour-pratique-commerciale-trompeuse

DUCOURTIEUX C., « Le Royaume-Uni, champion de la reconnaissance faciale », *Le Monde*, 4 septembre 2019.

DUTHEIL G., Boeing corrige le logiciel de stabilisation de l'avion 737 MAX après les crashs d'Ethiopian Airlines et de Lion Air, *Le Monde* [en ligne]. 28 2019. [Consulté le 25 mai 2020]. Disponible à l'adresse : https://www.lemonde.fr/economie/article/2019/03/28/boeing-a-modifie-le-logiciel-de-stabilisation-de-son-737-max_5442598_3234.html

ETALAB, Guide : comment pseudonymiser des documents grâce à l'IA, *Guides.etalab.gouv.fr* [en ligne]. [Consulté le 15 juin 2020]. Disponible à l'adresse : https://guides.etalab.gouv.fr/pseudonymisation/#a-quoi-sert-ce-guide

ETALAB, Ethique et responsabilité des algorithmes publics, proposition 11, p. 23, *Etalab.gouv.fr* [en ligne], juin 2019 [Consulté le 12 décembre 2020]. Disponible à l'adresse : https://www.etalab.gouv.fr/wp-content/uploads/2020/01/Rapport-ENA-Ethique-et-responsabilit%C3%A9-des-algorithmes-publics.pdf

ETAT FRANÇAIS, LexImpact, Aider nos parlementaires à estimer les impacts de leurs amendements avant vote !, *Beta.gouv.fr* [en ligne]. [Consulté le 2 janvier 2021]. Disponible à l'adresse : https://beta.gouv.fr/startups/leximpact.html

ETAT FRANÇAIS, Grand débat national : la lettre aux Français du président de la République, *Site du Gouvernement français* [en ligne]. 13 janvier 2019 [Consulté le 22 novembre 2020]. Disponible à l'adresse : https://www.gouvernement.fr/grand-debat-national-la-lettre-aux-francais-du-president-de-la-republique

ETAT FRANÇAIS, Conclusions de la concertation sur la mise en place d'un système universel de retraite, p. 23, *Participez.reforme-retraite.gouv.fr* [en ligne]. [Consulté le 12 mars 2021]. Disponible à l'adresse : https://participez.reforme-retraite.gouv.fr/media/default/0001/01/052fe41833cdf2384392e4e0f243bebe417f7d81.pdf

ETAT FRANÇAIS, Pour une action publique transparente et collaborative : plan d'action national pour la France, engagement n° 12, p. 31, *Modernisation.gouv.fr* [en ligne]. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.modernisation.gouv.fr/sites/default/files/fichiers-attaches/pgo_plan_action_france_2015-2017_fr.pdf

ETAT FRANÇAIS, La loi pour une République numérique se construit avec les Français, *Le portail de la transformation de l'action publique* [en ligne]. 28 septembre 2015 [Consulté le 14 décembre 2020]. Disponible à l'adresse : https://www.modernisation.gouv.fr/outils-et-methodes-pour-transformer/la-loi-pour-une-republique-numerique-se-construit-avec-les-francais

Moteur de recherche du site internet de *Exodus* [en ligne] [Consulté le 25 novembre 2019]. Disponible à l'adresse : https://reports.exodus-privacy.eu.org/fr/

FLAJOLET P., COLLARD P., ALGORITHMIQUE, *Encyclopædia Universalis* [en ligne]. [Consulté le 7 juin 2017]. Disponible à l'adresse : http://www.universalis.fr/encyclopedie/algorithmique/

FORTEZA P., L'utilisation des nouvelles technologies par les pouvoirs publics, *Site de la Fondation Jean Jaurès* [en ligne] 1er juin 2021. [Consulté le 14 novembre 2020]. Disponible à l'adresse : https://www.jean-jaures.org/publication/lutilisation-des-nouvelles-technologies-par-les-pouvoirs-publics/

FRENOIS M., Nice : Caméra, reconnaissance faciale, détecteur de bruits… Un collectif lancé pour « résister à la surveillance », *20 minutes.fr* [en ligne] 17 septembre 2019 [Consulté le 3 février 2021]. Disponible à l'adresse : https://www.20minutes.fr/nice/2605395-20190917-nice-camera-reconnaissance-faciale-detecteur-bruits-collectif-lance-resister-surveillance

GRAVELEAU S., APB : les questions que soulève le code source, *Le Monde* [en ligne]. 25 octobre 2016, mis à jour le 25 octobre 2016. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.lemonde.fr/campus/article/2016/10/25/apb-les-questions-que-souleve-le-code-source_5020076_4401467.html

GUERRY B., Etat des lieux des pratiques de publication des codes sources dans l'Enseignement Supérieur et la Recherche, *Etalab.gouv.fr* [en ligne]. 04 février 2021. [Consulté le 25 avril 2021]. Disponible à l'adresse : https://www.etalab.gouv.fr/les-pratiques-de-publication-des-codes-sources-dans-lenseignement-superieur-et-la-recherche

GUILLAUD H., Algorithmes et responsabilités, *Internetactu.net* [en ligne]. 16 mars 2016. [Consulté le 2 avril 2021]. Disponible à l'adresse : https://www.internetactu.net/2016/03/16/algorithmes-et-responsabilites/

HALTE A L'OBSOLESCENCE PROGRAMMEE, Livre blanc. 50 mesures pour une consommation et une production durables, Recommandation n° 48, *halteobsolescence.org* [en ligne]. Février 2019. [Consulté le 20 avril 2020]. Disponible à l'adresse : https://www.halteobsolescence.org/wp-content/uploads/2019/03/Livre-Blanc.pdf

INRIA, TransAlgo : évaluer la responsabilité et la transparence des systèmes algorithmiques, *INRIA.fr* [en ligne], 4 avril 2018 [Consulté le 19 mars 2020]. Disponible à l'adresse : https://www.inria.fr/fr/transalgo-evaluer-la-responsabilite-et-la-transparence-des-systemes-algorithmiques

INRIA, Régulation des plates-formes numériques : le gouvernement français prend les devants, *inria.fr* [en ligne]. 6 mai 2021. [Consulté le 10 juillet 2021]. Disponible à l'adresse : https://www.inria.fr/fr/regulation-plateformes-numeriques-peren-regalia

INSERM, Coronavirus : des chercheurs de l'Inserm proposent un modèle pour estimer le risque d'importation de l'épidémie en Europe, *Site de l'Inserm* [en ligne]. 24 janvier 2020 [Consulté le 2 mars 2020]. Disponible à l'adresse : https://presse.inserm.fr/coronavirus-des-chercheurs-de-linserm-proposent-un-modele-pour-estimer-le-risque-dimportation-de-lepidemie-en-europe/38000/

JACQUOT G., Autorités administratives indépendantes : le Sénat s'interroge à nouveau sur leur « multiplication », *Public Sénat.fr* [en ligne]. 23 janvier 2019 [Consulté le 26 novembre 2020]. Disponible à l'adresse : https://www.publicsenat.fr/article/parlementaire/autorites-administratives-independantes-le-senat-s-interroge-a-nouveau-sur

JOIGNOT F., Le Philosophe Bernard Stiegler est mort. Deux grands entretiens pour rappeler sa pensée sur la technique, l'urgence écologique, le « care », le « psycho-pouvoir », la perte du sens de nos vies, *Blog Le Monde* [en ligne]. 21 février 2011. [Consulté le 23 novembre 2019]. Disponible à l'adresse : http://fredericjoignot.blog.lemonde.fr/2011/02/21/nous-vivons-un-extreme-desenchantement-un-entretien-avec-le-philosophe-bernard-stiegler/

LAROUSSE, Définition « Algorithme », *Larousse.fr* [en ligne]. [Consulté le 2 mars 2018]. Disponible à l'adresse : https://www.larousse.fr/dictionnaires/francais/algorithme/2238

LE DORZE Y., Algorithmes et concurrence, l'Autorité et le Bundeskartellamt publient une étude commune, *Autorité de la concurrence.fr* [en ligne]. 06 novembre 2019. [Consulté le 12 novembre 2020]. Disponible à l'adresse : https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/algorithmes-et-concurrence-lautorite-et-le-bundeskartellamt-publient-une#:~:text=de%20l'institution-,Algorithmes%20et%20concurrence%2C%20l'Autorit%C3%A9%20et%20le,Bundeskartellamt%20publient%20une%20%C3%A9tude%20commune&text=Dans%20leur%20projet%20conceptuel%20commun,pouvant%20%C3%AAtre%20associ%C3%A9s%20aux%20algorithmes.

LE FOLL C., POURE C., Drones : comment Gérald Darmanin a voulu échapper à toute sanction, *Mediapart* [en ligne]. 8 mai 2021 [Consulté le 2 juin 2021]. Disponible à l'adresse : https://www.mediapart.fr/journal/france/080521/drones-comment-gerald-darmanin-voulu-echapper-toute-sanction

LEMAIRE A., Lettre de mission CNNum au Président du Conseil national du numérique, *Economie.gouv.fr* [en ligne]. 8 décembre 2016 [Consulté le 26 janvier 2021]. Disponible à l'adresse : https://www.economie.gouv.fr/files/files/PDF/Lettre_de_mission_CNNum.pdf

LE ROBERT, Définition « Cyberespace », *Dictionnaire.lerobert.com* [en ligne]. [Consulté le 25 novembre 2020]. Disponible à l'adresse : https://dictionnaire.lerobert.com/definition/cyberespace

LES ÉCHOS, Quand le logiciel de recrutement d'Amazon discrimine les femmes, *Les Echos.fr* [En ligne]. 13 octobre 2018 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.lesechos.fr/industrie-services/conso-distribution/quand-le-logiciel-de-recrutement-damazon-discrimine-les-femmes-141753

LES PARTENAIRES DE CHALLENGES, Le trading haute fréquence en mutation, *Challenges.fr* [en ligne], 30 janvier 2020 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.challenges.fr/entreprise/le-trading-haute-frequence-en-mutation_696509.

LESSIG L., *Code Is Law: on liberty in cyberspace*, Harvard Magazine, 1er janvier 2000.

LE VRAI DEBAT, Site participatif réalisé par un collectif de gilets jaunes de différentes régions de France [en ligne]. [Consulté le 2 juillet 2021]. Disponible à l'adresse : https://www.le-vrai-debat.fr/

L'EXPRESS.FR, Election de Trump : le hold-up de Cambridge Analytica sur les usagers de Facebook, *Page Actualités du site L'Express* [en ligne]. 18 mars 2018 [Consulté le 2 mai 2020]. Disponible à l'adresse :

https://www.lexpress.fr/actualite/monde/amerique-nord/election-de-trump-le-hold-up-de-cambridge-analytica-sur-les-usagers-de-facebook_1993257.html

Site du Laboratoire d'Innovation Numérique de la CNIL [en ligne]. [Consulté le 2 juillet 2021]. Disponible à l'adresse : https://linc.cnil.fr

LUMINEAU L., Satoshi Nakamoto : qui se cache derrière le créateur du bitcoin, *Capital.fr* [en ligne]. 12 novembre 2018, mis à jour le 1er avril 2021. [Consulté le 17 juin 2020]. Disponible à l'adresse : https://www.capital.fr/entreprises-marches/satoshi-nakamoto-qui-se-cache-derriere-le-createur-du-bitcoin-1315353

MANANCOURT V., Have a GDPR complaint ? Skip the regulator and take it to court, *Politico.eu*. 30 août 2020, mis à jour le 1er septembre 2020. [Consulté le 04 octobre 2020]. Disponible à l'adresse : https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/

MANDARD, S., Cinq ans après le « Dieselgate », les constructeurs bénéficient toujours d'une « clause de confidentialité », *Le Monde.fr* [en ligne]. 18 septembre 2020 [Consulté le 14 décembre 2020] : https://www.lemonde.fr/planete/article/2020/09/18/dieselgate-cinq-ans-apres-la-transparence-fait-toujours-defaut-sur-les-emissions-de-gaz-polluants_6052649_3244.html

METAIS E., SYSTÈMES INFORMATIQUES - Systèmes d'aide à la décision, *Encyclopædia Universalis* [en ligne]. [Consulté le 10 août 2021]. Disponible à l'adresse : https://www.universalis.fr/encyclopedie/systemes-informatiques-systemes-d-aide-a-la-decision/

MICROSOFT, IA responsable, *Microsoft.com* [en ligne] [Consulté le 12 mars 2021]. Disponible à l'adresse : https://www.microsoft.com/fr-fr/ai/responsible-ai?activetab=pivot1:primaryr6

MULTIPLE, Open Letter to the European Commission Artificial Intelligence and Robotics, *Robotics-Openletter.eu* [en ligne]. [Consulté le 2 mai 2021]. Disponible à l'adresse : http://www.robotics-openletter.eu/

OBSERVATOIRE DES LIBERTES ET DU NUMERIQUE, Création de l'Observatoire des Libertés et du Numérique, *IDH France.org* [en ligne]. 28 janvier 2014. [Consulté le 23 février 2020]. Disponible à l'adresse : https://www.ldh-france.org/Creation-de-l-Observatoire-des/

OPINION WAY, Analyse des contributions au Grand Débat National : Q&A, *Site d'Opinion Way* [en ligne]. 15 février 2019 [Consulté le 2 mars 2021]. Disponible à l'adresse : https://www.opinion-way.com/fr/mediatheque/presse/opinionway-q-a-sur-l-analyse-des-contributions-grand-debat-national-15-fevrier-2019/viewdocument.html

ORANGE, Orange crée un Conseil d'éthique de la Data et de l'IA, *Orange.com* [en ligne]. 23 mars 2021 [Consulté le 3 avril 2021]. Disponible à l'adresse : https://www.orange.com/fr/newsroom/communiques/2021/orange-cree-un-conseil-dethique-de-la-data-et-de-lia

PELLEGRINI F., Souveraineté numérique : « le recours aux logiciels libres constitue la seule alternative viable, *Le Monde* [en ligne]. 21 juin 2016. [Consulté le 21 décembre 2020]. Disponible à l'adresse : https://www.lemonde.fr/idees/article/2016/06/24/la-souverainete-numerique-passe-par-le-logiciel-libre_4957781_3232.html

PELLEGRINI F., « Les algos : ni loyaux, ni éthiques ! », *Blog Binaire Le Monde* [en ligne]. 27 mars 2017. [Consulté le 25 avril 2020]. Disponible à l'adresse : https://www.lemonde.fr/blog/binaire/2017/03/27/les-algos-ni-loyaux-ni-ethiques/

PIQUARD A., Amazon, accusé d'avoir enfreint les règles européennes de concurrence, visé par deux enquêtes de Bruxelles, *Le Monde* [en ligne]. 10 novembre 2020 [Consulté le 20 novembre 2020]. Disponible à l'adresse : https://www.lemonde.fr/economie/article/2020/11/10/bruxelles-accuse-amazon-d-avoir-enfreint-les-regles-europeennes-de-concurrence_6059246_3234.html

PIRE B., AL-KHWARIZMI, *Encyclopædia Universalis* [en ligne]. [Consulté le 29 juin 2021]. Disponible à l'adresse : https://www.universalis.fr/encyclopedie/al-khwarizmi/

POLE EMPLOI, Algorithmes, Tout savoir sur les algorithmes publiés par Pôle Emploi, *Pole-emploi.fr* [en ligne]. [Consulté le 28 août 2020]. Disponible à l'adresse : https://www.pole-emploi.fr/candidat/algorithmes.html

PRADO Jason Barrett, Taxonomizing platforms to scale regulation, *Venturecommune.substack.com* [en ligne] 18 novembre 2019 [Consulté le 2 novembre 2020]. Disponible à l'adresse : https://venturecommune.substack.com/p/taxonomizing-platforms-to-scale-regulation

QUERCIA Y., Le CSA pourrait étendre sa régulation aux réseaux sociaux, *Public Sénat.fr* [en ligne]. 30 janvier 2019 [Consulté le 15 janvier 2021]. Disponible à l'adresse : https://www.publicsenat.fr/article/societe/le-csa-pourrait-etendre-sa-regulation-aux-reseaux-sociaux-137387

RAMEY C., « A New York, un algorithme aide les juges à décider qui sera libre en attendant son procès », *in The Wall Street Journal & l'Opinion*, 22 septembre 2020.

REYNAUD F., Qu'est-ce que Dominion, le logiciel électoral attaqué par Donald Trump ?, *Le Monde* [en ligne]. 20 novembre 2020, mis à jour le 21 novembre 2020. [Consulté le 2 décembre 2020]. Disponible à l'adresse : https://www.lemonde.fr/pixels/article/2020/11/20/qu-est-ce-que-dominion-le-logiciel-electoral-attaque-par-donald-trump_6060562_4408996.html

SALMON C., « Bojo le clown » et son ingénieur magicien, *Médiapart* [en ligne]. 26 janvier 2020. [Consulté le 12 mars 2020]. Disponible à l'adresse : https://www.mediapart.fr/journal/international/260120/bojo-le-clown-et-son-ingenieur-magicien?onglet=full

SIMON D., Bourse, toujours plus vite : la peur du bug, *France Inter.fr* [en ligne]. 8 avril 2016 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.franceinter.fr/emissions/le-zoom-de-la-redaction/le-zoom-de-la-redaction-08-avril-2016

Site Données & Design par LINC [en ligne] [Consulté le 23 février 2021]. Disponible à l'adresse : https://design.cnil.fr/

STOLTON S., Von der Leyen s'engage à « aller plus loin » contre l'IA qui porte atteinte aux droits fondamentaux, *Euractiv.fr* [en ligne]. 31 mars 2021 [Consulté le 15 avril 2021]. Disponible à l'adresse : https://www.euractiv.fr/section/economie/news/von-der-leyen-assures-meps-well-go-further-on-ai-that-harms-fundamental-rights/

SYNDICAT DE LA MAGISTRATURE, SYNDICAT DES AVOCATS DE FRANCE, LIGUE DES DROITS DE L'HOMME, AIDES, Contribution extérieure du Syndicat de la magistrature, du Syndicat des avocats de France, de la Ligue des Droits de l'Homme et de AIDES, sur la loi visant à lutter contre les contenus haineux sur internet (affaire n° 2020-801 DC), *syndicat-magistrature.org* [en ligne]. 29 mai 2020, [Consulté le 12 juin 2020]. Disponible à l'adresse : http://www.syndicat-magistrature.org/IMG/pdf/porte_ouverte_loi_avia_saf_sm_aides_ldh-2.pdf

TARNOFF Ben, Platforms don't exist, *Bentanoff.substack.com* [en ligne] 22 novembre 2019 [Consulté le 11 janvier 2021]. Disponible à l'adresse : https://bentarnoff.substack.com/p/platforms-dont-exist

TENCENT RESEARCH INSTITUTE, « ARCC » : An Ethical Framework for Artificial Intelligence, principe n° 3, *Tisi.org* [en ligne]. 09 avril 2020 [Consulté le 16 avril 2021]. Disponible à l'adresse : https://www.tisi.org/13747

TRESOR DIRECTION GENERALE, La DG Trésor met à la disposition du public les codes sources des modèles Mésange, Opale et Saphir, *Trésor-Info [en ligne]*. 5 septembre 2018 [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.tresor.economie.gouv.fr/Articles/2018/09/05/la-dg-tresor-met-a-la-disposition-du-public-les-codes-sources-des-modeles-mesange-opale-et-saphir

TWITTERSAFETY, Calling for public input on our approach to world leaders, *Blog.Twitter.com* [en ligne]. 18 mars 2021 [Consulté le 12 avril 2021]. Disponible à l'adresse : https://blog.twitter.com/en_us/topics/company/2021/calling-for-public-input-on-our-approach-to-world-leaders.html

UNTERSINGER M., Un ambassadeur dans la Silicon Valley pour « conserver du pouvoir à l'ère du numérique », *Le Monde* [en ligne]. 6 juin 2018 [Consulté le 23 août 2020]. Disponible à l'adresse : https://www.lemonde.fr/pixels/article/2018/06/06/un-ambassadeur-dans-la-silicon-valley-pour-conserver-du-pouvoir-a-l-ere-du-numerique_5310352_4408996.html

VAVASSEUR L., CHASSON A., GHESQUIERE Q., Livre blanc, 50 mesures pour une consommation et une production durables, p. 33, *Halte à l'obsolescence programmée.org* [en ligne]. Février 2019 [Consulté le 16 mars 2020]. Disponible à l'adresse : https://www.halteobsolescence.org/wp-content/uploads/2019/03/Livre-Blanc.pdf

VIDAL F., Parcoursup, la plateforme d'admission dans l'enseignement supérieur, *Site du ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation* [en ligne]. 21 mai 2018 [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.enseignementsup-recherche.gouv.fr/cid130453/parcoursup-publication-du-code-informatique-des-algorithmes.html

IV - REFERENCES NORMATIVES

A - TEXTES ET DECISIONS D'ORIGINE NATIONALE

1 - Décisions constitutionnelles

Conseil constitutionnel, décision n° 81-132 DC, 16 janvier 1982, *Loi de nationalisation*.

Conseil constitutionnel, décision n° 83-165 DC, 20 janvier 1984, *Loi relative à l'enseignement supérieur*.

Conseil constitutionnel, décision n° 85-197 DC, 23 août 1985, *Loi sur l'évolution de la Nouvelle-Calédonie*.

Conseil constitutionnel, décision n° 94-345 DC, 29 juillet 1994, *Loi relative à l'emploi de la langue française*.

Conseil constitutionnel, décision n° 94-352 DC, 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*.

Conseil constitutionnel, décision n° 99-416 DC, 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*.

Conseil constitutionnel, décision n° 2006-544 DC, 14 décembre 2006, *Loi de financement de la sécurité sociale pour 2007*.

Conseil constitutionnel, décision n° 2007-3742/3947 AN, 20 décembre 2007.

Conseil constitutionnel, décision n° 2012-4597/4626 AN, 15 février 2013.

Conseil constitutionnel, décision n° 2015-713 DC, 23 juillet 2015, *Loi relative au renseignement.*

Conseil constitutionnel, décision n° 2017-646/647 QPC, 21 juillet 2017.

Conseil constitutionnel, décision n° 2017-655 QPC, 15 septembre 2017.

Conseil constitutionnel, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*.

Conseil constitutionnel, décision n° 2018-773 DC, 20 décembre 2018, *Loi relative à la lutte contre la manipulation de l'information*.

Conseil constitutionnel, décision n° 2018-774 DC, 20 décembre 2018, *Loi organique relative à la lutte contre la manipulation de l'information*.

Conseil constitutionnel, décision n° 2019-778 DC, 21 mars 2019, *Loi de programmation 2018-2022 et de réforme pour la justice.*

Conseil constitutionnel, décision n° 2019-796 DC, 27 décembre 2019, *loi de finances pour 2020.*

Conseil constitutionnel, décision n° 2020-834 QPC, 3 avril 2020.

Conseil constitutionnel, décision n° 2020-800 DC, 11 mai 2020, *Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions*.

Conseil constitutionnel, décision n° 2020-801 DC, 18 juin 2020, *Loi visant à lutter contre les contenus haineux sur internet*.

Conseil constitutionnel, décision n° 2021-823 DC, 13 août 2021, *Loi confortant le respect des principes de la République*.

2 - Textes de valeur législative

Loi du 29 juillet 1881 sur la liberté de la presse.

Ordonnance du 21 avril 1944 relative à l'organisation des pouvoirs publics en France après la Libération.

Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

Loi n° 79-587 du 11 juillet 1979 relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public.

Loi n° 83-609 du 8 juillet 1983 portant création d'une délégation parlementaire dénommée office parlementaire d'évaluation des choix scientifiques et technologiques.

Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication modifiée.

Loi n° 95-125 du 8 février 1995 relative à l'organisation des juridictions et à la procédure civile, administrative et pénale.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi n° 2005-516 relative à la régulation des activités postales du 20 mai 2005.

Loi n° 2007-292 du 5 mars 2007 relative à la Commission nationale consultative des droits de l'homme, modifiée.

Ordonnance n° 2007-329 du 12 mars 2007 relative au code du travail.

Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

Loi n° 2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires.

Loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière.

Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

Loi n° 2015-992 du 17 août 2015 relative à la transition énergétique pour la croissance verte.

Loi n° 77-808 du 19 juillet 1977 relative à la publication et à la diffusion de certains sondages d'opinion telle que modifiée par la loi n° 2016-508 du 25 avril 2016 de modernisation de diverses règles applicables aux élections.

Ordonnance n° 2016-827 du 23 juin 2016 relative aux marchés d'instruments financiers.

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires.

Ordonnance n° 2018-1125 du 12 décembre 2018.

Loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

Loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités.

Loi n° 2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire.

Loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19.

Loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions.

Ordonnance n° 2020-701 du 10 juin 2020 relative à la surveillance du marché des véhicules à moteur.

Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.

Loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée.

Ordonnance n° 2021-442 du 14 avril 2021 relative à l'accès aux données des véhicules.

Ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation.

Ordonnance n° 2021-580 du 12 mai 2021 portant transposition du 6 de l'article 2 et des articles 17 à 23 de la directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE.

Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

Loi n° 2021-1017 du 2 août 2021 relative à la bioéthique.

Loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire.

Loi n°2021-1109 du 24 août 2021 confortant le respect des principes de la République.

3 - Textes et décisions de valeur infra-législative

a - Règlements

Décret n° 69.296 du 2 avril 1969 décidant de soumettre un projet de loi au référendum, annexe, *Projet de loi relatif à la création de régions et à la rénovation du Sénat.*

Décret n° 74-938 du 8 novembre 1974 portant création de la commission Informatique et libertés.

Décret n° 83-132 du 23 février 1983 portant création d'un Comité consultatif national d'éthique pour les sciences de la vie et de la santé, depuis abrogé.

Décret n° 85-1152 du 5 novembre 1985 portant création d'une direction générale de la concurrence, de la consommation et de la répression des fraudes.

Arrêté du 17 novembre 2003 *portant approbation du règlement technique fixant les conditions d'agrément des machines à voter*.

Arrêté du 20 octobre 2008 portant création d'un traitement automatisé de données à caractère personnel relatif au pilotage et à la gestion des élèves de l'enseignement du premier degré.

Décret n° 2011-194 du 21 février 2011 portant création d'une mission « Etalab » chargée de la création d'un portail unique interministériel des données publiques.

Décret n° 2011-348 du 29 mars 2011 portant création de l'Agence nationale de traitement automatisé des infractions.

Décret n° 2011-476 du 29 avril 2011 portant création du Conseil national du numérique.

Arrêté du 17 mars 2017 relatif au vote par correspondance électronique pour l'élection de députés par les Français établis hors de France.

Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat.

Décret n° 2017-1677 du 8 décembre 2017 relatif au Conseil national du numérique modifié par le décret n° 2021-154 du 13 février 2021.

Arrêté du 9 mars 2018 relatif aux missions, à la composition et aux modalités de fonctionnement du comité éthique et scientifique de la plateforme Parcoursup.

Arrêté du 28 mars 2018 *autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Parcoursup »*, abrogé depuis par l'arrêté du 31 décembre 2020 portant création d'un traitement automatisé de données à caractère personnel dénommé « *Parcoursup* ».

Décret n° 2019-23 du 14 janvier 2019 instituant une mission d'organisation et de coordination du grand débat national.

Décret n° 2019-61 du 31 janvier 2019 instituant un collège des garants du grand débat national.

Décret n° 2019-231 du 26 mars 2019 relatif à la procédure nationale de préinscription pour l'accès aux formations initiales du premier cycle de l'enseignement supérieur et modifiant le code de l'éducation.

Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique.

Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques.

Arrêté du 26 mai 2020 portant nomination des membres du Comité de contrôle et de liaison Covid-19.

Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid ».

Arrêté du 10 juin 2020 portant création du service à compétence nationale dénommé service de surveillance du marché des véhicules et des moteurs (SSMVM).

Décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives.

Décret n° 2020-1045 du 14 août 2020 relatif aux attributions du secrétaire d'État auprès du ministre de l'Economie, des finances et de la relance et de la ministre de la Cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques.

Décret n° 2020-1102 du 31 août 2020 portant création d'un service à compétence nationale dénommé « Pôle d'expertise de la régulation numérique » (PEReN).

Décret n° 2021-157 du 12 février 2021 modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « *StopCovid* ».

Décret n° 2021-501 du 22 avril 2021 relatif aux indicateurs d'activité des travailleurs ayant recours à des plateformes de mise en relation par voie électronique.

Décret n° 2021-901 du 6 juillet 2021 relatif au traitement automatisé de données à caractère personnel dénommé « Convertisseur de certificats ».

Arrêté du 17 août 2021 instituant un administrateur ministériel des données, des algorithmes et des codes sources au ministère du travail, de l'emploi et de l'insertion.

b - Décisions des juridictions administratives

CE, 29 avril 2002, req. n° 228830.

CE, 23 février 2005, req. n° 241796.

CE, 13 février 2009, req. n° 306563.

CE, 4 novembre 2009, req. n° 306563.

CE, 19 juillet 2010, req. n° 317182.

CE, 19 juillet 2010, req. n° 334014.

CE, 1er décembre 2010, req. n° 337945.

CE, 9 juin 2015, req. n° 385717.

TA de Paris, 10 mars 2016, req. n° 1508951.

CE, 8 juin 2016, req. n° 386525.

CE, 6 juillet 2016, req. n° 394573.

CE, 31 mars 2017, req. n° 392316.

CE, 19 mai 2017, req. n° 396698.

TA de Guadeloupe, 4 février 2019, req. n° 1801094.

CE, 12 juin 2019, req. n° 427919.

CE, 24 octobre 2019, req. n° 427204.

CE, 15 janvier 2020, req. n° 433296.

CE, Ord., 18 mai 2020, req. n° 440442 et 440445.

CE, 12 juin 2020, req. n° 418142.

CE, 19 juin 2020, req. n° 434684.

CE, Ord., 13 octobre 2020, req. n° 444937.

CE, 21 janvier 2021, req. n° 429956.

CE, Ass, 21 avril 2021, req. n° 393099, 394922, 397844, 397851, 424717, 424718.

c - Décisions des juridictions judiciaires

Tribunal civil de la Seine, Félix c. O'Connell, 18 juin 1858.

Tribunal correctionnel de Paris, 25 février 2000, Serge H. c/ GIE cartes bancaires.

TGI Nanterre, 5 septembre 2008, RG 08/05737.

TGI, Paris, 22 octobre 2013, Ministère public c/ Pichon.

TGI de Paris, ordonnance de référé du 13 juin 2017, RG 17/51830.

TGI de Paris, jugement du 24 septembre 2019, RG 17/0622.

TGI de Paris, jugement du 17 décembre 2019, RG 17/06223.

TGI de Paris, jugement du 24 septembre 2019, RG 17/06224.

Cass. Soc., 4 mars 2020, req. n° 19-13.316.

TGI de Paris, jugement du 24 novembre 2020, association consommation, logement et cadre de vie c/ Be Labo.

Tribunal Judiciaire de Paris, n° 20/53181 du 6 juillet 2021.

d - Circulaires et réponses ministérielles

Circulaire n° 64 du Premier ministre en date du 12 mars 1993 relative à la protection de la vie privée en matière de traitements automatisés.

Réponse du Secrétariat d'État, auprès du Premier ministre, chargé du numérique publiée dans le JO Sénat du 8 février 2012, Microtransaction, loot boxes et jeu vidéo.

Réponse ministérielle publiée dans le JO du Sénat le 7 février 2019, Statut des délégués à la protection des données, p. 712.

Réponse ministérielle, écrite à la question n°15168 publiée au JO, ministère des Armées, Assemblée Nationale le 19 mars 2019, 15e Législature [en ligne]. [Consulté le 3 avril 2021]. Disponible à l'adresse : http://questions.assemblee-nationale.fr/q15/15-15168QE.htm

Circulaire n° 2020-11 du ministre de la Justice en date du 24 novembre 2020 relative à la lutte contre la haine en ligne.

Circulaire n° 6264/SG du Premier ministre en date du 27 avril 2021 relative à la politique publique de la donnée, des algorithmes et des codes sources.

e - Décisions et rapports de la CNIL

Avis et délibération

CNIL, délibération n°02017-023 du 16 février 2017 portant avis sur un projet de décret relatif aux modalités de communication des règles et caractéristiques des traitements algorithmiques.

CNIL, décision n° MED-2017-053 du 30 août 2017 mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation.

CNIL, délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPD).

CNIL, délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPD).

CNIL, délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, art. 9.

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.

CNIL, délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

CNIL, délibération n° 2019-160 du 21 novembre 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel.

CNIL, délibération n° 2020-021 du 6 février 2020 portant avis sur un projet de décret relatif à la mise à disposition du public des décisions des juridictions judiciaires et administratives (demande d'avis n° 19022713).

CNIL, délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « *StopCovid* ».

CNIL, délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « *StopCovid* ».

CNIL, décision n° MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des solidarités et de la santé.

CNIL, décision n° 2020-015 du 3 septembre 2020.

CNIL, délibération n° 2020-091 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.

CNIL, décision n° SAN-2020-012 du 7 décembre 2020.

CNIL, délibération n° 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports.

CNIL, délibération n°2021-024 du 12 mai 2021 portant avis sur le projet de mise en place d'un passe sanitaire conditionnant l'accès à certains lieux, évènements ou établissements impliquant de grands rassemblements de personnes.

CNIL, délibération n°2021-065 du 3 juin 2021 portant approbation du code de conduite européen porté par Cloud Infrastructure Service Providers Europe (CISPE).

CNIL, délibération n°2021-067 du 7 juin 2021 portant avis sur le projet de décret portant application du II de l'article 1er de la loi n°2021-689 du 31 mai 2021 relative à la gestion de la sortie de crise sanitaire.

CNIL, délibération n° 2021-097 du 6 août 2021 portant avis sur un projet de décret modifiant le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire.

Rapports et autre

COMMISSION INFORMATIQUE ET LIBERTES, Rapport, *La Documentation Française*, 1975

CNIL, *Guide du correspondant informatique et libertés*, édition 2011, p. 46.

CNIL, 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, comment permettre à l'homme de garder la main : les enjeux éthiques des algorithmes et de l'intelligence artificielle, 2017.

CNIL, Critères de certification de délégué à la protection des données (DPO), 23 mai 2018.

CNIL, Rapport d'activité, 2019.

CNIL, Rapport d'activité, 2020.

CNIL, Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur.

f - Rapports, Recommandations, avis et décisions d'autres administrations, institutions et comités

CADA

CADA, avis n° 20144578 du 8 janvier 2015.

CADA, dans son conseil n° 20155079 du 19 novembre 2015.

CADA, avis n° 20161989 du 23 juin 2016.

CADA, avis n° 20180276 du 19 avril 2018.

CADA, avis n° 20182682 du 6 septembre 2018.

CADA, avis n° 20184400 du 10 janvier 2019.

CCNE

CCNE, Avis 91 sur les problèmes éthiques posés par l'informatisation de la prescription hospitalière et du dossier du patient, 30 janvier 2006.

CCNE, Avis 129. Contribution du comité consultatif national d'éthique à la révision de la loi de bioéthique, 18 septembre 2018.

CCNE, Cnpen, Rapport du groupe de travail commandé par le comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE) avec le concours de la commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene (CERNA), 19 novembre 2018.

CCNE, Avis 130. Données massives et santé : une nouvelle approche des enjeux éthiques, 29 mai 2019.

CCNE, Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë, 7 avril 2020.

CCNE, Cnpen, Enjeux d'éthique concernant des outils numériques pour le déconfinement, 14 mai 2020.

CCNE, Consultation sur le Livre blanc sur l'intelligence artificielle. Une approche européenne, 15 juin 2020.

CCNE, Enjeux d'éthique dans la lutte contre la désinformation et la mésinformation, 21 juillet 2020.

CCNE, Enjeux d'éthique liés aux outils numériques en télémédecine et télésoin dans le contexte de la COVID-19, 21 juillet 2020.

Conseil d'Etat

CE, Rapport, « Les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives : notes, comptes-rendus d'entretiens, notes manuscrites, projet de plan, projets intermédiaires », 20050574/18, n° 2, Archives nationales, 1970.

CE, Rapport annuel, *Réflexions sur l'intérêt général*, La Documentation française, Etudes et documents, n°50, 1999.

CE, *Rapport public, Etude annuelle sur l'intérêt général*, *La Documentation française*, études et documents, 1999, n° 50.

CE, *Rapport public, Les autorités administratives indépendantes*, 2001.

CE, *Le numérique et les droits fondamentaux*, étude annuelle 2014, *La Documentation française*, 2014.

CE, avis n° 390741 sur le projet de loi pour une République numérique, 3 décembre 2015.

CE, Rapport « Révision de la loi de bioéthique : quelles options pour demain ? », *vie-publique.fr* [en ligne], 7 juillet 2018 [Consulté le 2 juillet 2020]. Disponible à l'adresse : https://www.vie-publique.fr/rapport/37442-revision-de-la-loi-de-bioethique-quelles-options-pour-demain

CE, Rapport « Étude annuelle 2017 - Puissance publique et plateformes numériques : accompagner « l'ubérisation » », p. 116, *Conseil-Etat.fr* [en ligne]. 28 septembre 2018 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2017-puissance-publique-et-plateformes-numeriques-accompagner-l-uberisation

CE, avis sur un projet de loi relatif à la bioéthique, séance du 18 juillet 2019.

CE, *Etude annuelle, Conduire et partager l'évaluation des politiques publiques, La documentation française*, 2020.

CNCDH

CNCDH, Avis relatif à la proposition de loi visant à lutter contre la haine sur internet, 9 juillet 2019.

CNCDH, Avis sur le suivi numérique des personnes, *CNCDE.fr* [en ligne], 28 avril 2020 [Consulté le 2 novembre 2020]. Disponible à l'adresse : https://www.cncdh.fr/fr/actualite/avis-sur-le-suivi-numerique-des-personnes

CNCDH, avis sur la transposition de la directive relative aux lanceurs d'alerte, 4 octobre 2020.

CSA

CSA, recommandation n° 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel *aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations.*

CSA, *Etude, capacité à informer des algorithmes de recommandation : une expérience sur le service YOUTUBE*, novembre 2019.

CSA, Pourquoi et comment le CSA a réalisé une étude sur l'un des algorithmes de recommandations de YouTube, *Actualités du CSA* [en ligne]. 12 novembre 2019 [Consulté le 1er mars 2021]. Disponible à l'adresse : https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Pourquoi-et-comment-le-CSA-a-realise-une-etude-sur-l-un-des-algorithmes-de-recommandations-de-YouTube

CSA, Observatoire de la haine en ligne : analyser pour mieux lutter, *Actualités du CSA* [en ligne]. 15 octobre 2020 [Consulté le 5 février 2021]. Disponible à l'adresse : https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Observatoire-de-la-haine-en-ligne-analyser-pour-mieux-lutter

Conseil national du numérique

CNN, Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouverte et soutenable, *CNNumérique.fr* [en ligne]. Mai 2014 [Consulté le 10 juin 2020]. Disponible à l'adresse : https://cnnumerique.fr/files/2017-09/CNNum_Rapport_Neutralite_des_plateformes.pdf

CNN, Projet de loi pour une République numérique au sujet de la loyauté des plateformes, CNNumérique.fr [en ligne]. 2015. [Consulté le 23 avril 2020]. Disponible à l'adresse : https://cnnumerique.fr/files/uploads/2015/11/CNNum_Fiche_Loyaute-des-plateformes.pdf

CNN, Position du CNNum sur les dispositions de la LOM relatives au travail des plateformes, *Cnnumerique.fr* [en ligne], 03 juin 2019 [Consulté le 12 juin 2020]. Disponible à l'adresse : https://cnnumerique.fr/position-du-cnnum-sur-les-dispositions-de-la-lom-relatives-au-travail-des-plateformes

CNN, *Avis relatif à l'application Stopcovid en date du 24 avril 2020 après saisine du 14 avril 2020* [en ligne] [Consulté le 10 juin 2020]. Disponible à l'adresse : https://cnnumerique.fr/files/uploads/2020/2020.04.17_Saisine_Stop_Covid.pdf

Défenseur des droits

DEFENSEUR DES DROITS, déc. n° 2019-021, 18 janvier 2019.

DEFENSEUR DES DROITS, Rapport, Technologies biométriques : l'impératif respect des droits fondamentaux, 2021.

Autres

AMF, décision de la Commission des sanctions du 4 décembre 2015 à l'égard des sociétés Euronext Paris SA et Virtu Financial Europe Ltd.

ANTAI, Rapport d'activité, 2018.

ARCEP, Réseaux du futur, Note n°6, L'intelligence Artificielle dans les réseaux de télécommunications, 14 janvier 2020.

CASTETS-RENARD C., BESSE P., LOUBES J-M., PERRUSSEL L., Centre des Hautes Etudes du ministère de l'Intérieur, Rapport relatif Encadrement des risques techniques et juridiques des activités de police prédictive, 2019.

Comité d'éthique de la défense - Avis sur l'intégration de l'autonomie des systèmes d'armes létaux, 29 avril 2021.

COMMISSION NATIONALE DE CONTROLE DES TECHNIQUES DE RENSEIGNEMENT, 5e Rapport d'activité 2020, 2021.

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES, avis n° 2020-08 du 12 juin 2020.

CONSEIL GENERAL DE L'ECONOMIE, Modalités de régulation des algorithmes de traitements de contenus, 13 mai 2016.

CONSEIL GENERAL DE L'ECONOMIE DE L'INDUSTRIE, DE L'ENERGIE ET DES TECHNOLOGIES, Rapport, Modalités de régulation des algorithmes de traitement des contenus, 13 mai 2016.

MINISTERE DU TRAVAIL, DE L'EMPLOI ET DE L'INSERTION, Etude Les enjeux emplois et compétences de la mise en œuvre du Règlement général sur la protection des données, 8 octobre 2020.

RAPPORT ENA, Ethique et responsabilité des algorithmes publics, 2019.

g - Autres rapports et travaux parlementaires

Assemblée nationale

ASSEMBLEE NATIONALE, 2e Conférence des réformes, Propositions des groupes de travail, Juin 2018.

BOTHOREL E., COMBES S., VEDEL R., Pour une politique publique de la donnée, mission confiée par le Premier ministre, 23 décembre 2020.

COUSTE P-B., proposition de loi n° 1004 tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens, 5eme législature, enregistré à la Présidence de l'Assemblée nationale le 4 avril 1974.

DE GANAY C., GOUTTEFARDE F., Rapport d'information n°3248 de l'Assemblée nationale, 15e législature, fait au nom de la commission de la défense nationale et des forces armées, enregistré à la Présidence de l'Assemblée nationale le 22 juillet 2020.

DE LA RAUDIERE L., MIS J-M., Rapport d'information n° 1501 de l'Assemblée nationale sur les chaînes de blocs (blockchains), fait au nom de la mission d'information commune, enregistré à la Présidence de l'Assemblée nationale le 12 décembre 2018.

DURON P., FAURE O., amendement n° 462 et n°546 au projet de loi pour une République numérique, 14e législature, 16 janvier 2016.

FALQUE-PIERROTIN I., BERRY G., CYTERMANN J-R. et al., *Comité éthique et scientifique de Parcoursup, Rapport au parlement* [en ligne]. Janvier 2020 [Consulté le 30 janvier 2020]. Disponible à l'adresse : https://cache.media.enseignementsup-recherche.gouv.fr/file/2020/28/9/Rapport_du_CESP_2019_(janvier_2020)_1227289.pdf

FAURE-MUNTIAN V., FASQUELLE D., Rapport d'information n° 3127 sur les plateformes numériques de l'Assemblée nationale, 15e législature, fait au nom de la commission des affaires économiques, 15 e législature, enregistré à la Présidence de l'Assemblée nationale le 24 juin 2020.

FOYER M., Rapport n° 3125 sur le projet de loi relatif à l'informatique et aux libertés de l'Assemblée nationale, 5e législature, fait au nom de la commission des Lois, enregistré à la Présidence de l'Assemblée nationale le 4 octobre 1977.

GOUZES G., Rapport n° 3526 sur le projet de loi n° 3250 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés de l'Assemblée nationale, 11e législature, fait au nom de la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République, enregistré à la Présidence de l'Assemblée nationale le 9 janvier 2002.

MOREL-A-L'HUISSIER P., PETIT V., Rapport d'information sur l'évaluation des dispositifs d'évaluation des politiques publiques de l'Assemblée nationale, 15e législature, fait au nom du comité d'évaluation et de contrôle des politiques publiques, enregistré à la Présidence de l'Assemblée nationale le 15 mars 2018.

PAUL C., FERAL-SCHUHL C., Rapport n° 3119 Numérique et libertés : un nouvel âge démocratique de l'Assemblée nationale, 14e législature, fait au nom de la commission de réflexion et de propositions sur le droit et les libertés l'âge du numérique, enregistré à la Présidence de l'Assemblée nationale le 9 octobre 2015.

PAULA F., BAICHERE D et al., amendement n° 2169 au Projet de loi constitutionnelle pour une démocratie plus représentative, responsable et efficace, 15e législature, Assemblée nationale, enregistré à la Présidence de l'Assemblée nationale le 6 juillet 2018.

PONIATOWSKI M., proposition de loi tendant à la création d'un comité de surveillance et d'un tribunal de l'informatique n° 1454, 4eme législature, enregistré à la Présidence de l'Assemblée nationale le 25 novembre 1970.

RAPHAN P-A., proposition de loi constitutionnelle relative à la Charte de l'intelligence artificielle et des algorithmes n° 2585, 15e législature, enregistré à la Présidence de l'Assemblée nationale le 15 janvier 2020.

THIEBAUT V., Rapport n°4196 sur la proposition de loi visant à réduire l'empreinte environnementale du numérique en France de l'Assemblée nationale, 15 e législature, fait au nom de la Commission du développement durable et de l'aménagement du territoire, enregistré à la Présidence de l'Assemblée nationale 26 mai 2021.

VILLIANI C., SCHOENAUER M., BONNET Y., et al., Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne, mission confiée par le Premier ministre Edouard Philippe, 28 mars 2018.

Sénat

BOUCHOUX C., Rapport d'information n° 589 refonder le droit à l'information publique à l'heure du numérique : un enjeu citoyen, une opportunité stratégique du Sénat, session ordinaire 2013-2014, fait au nom de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques, enregistré à la Présidence du Sénat le 5 juin 2014.

BUFFET F-N., Rapport d'information n° 240 relatif au vote à distance du Sénat, session ordinaire 2020-2021, fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et de l'administration générale, enregistré à la Présidence du Sénat le 16 décembre 2020.

CAILLAVET H., proposition de loi n° 144 tendant à créer un Directoire et un Tribunal de l'Informatique, seconde session ordinaire 1973-1974, Sénat, enregistrée à la Présidence du Sénat le 2 avril 1974.

DEROMEDI J., DETRAIGNE Y., Rapport d'information n° 73 réconcilier le vote et les nouvelles technologies du Sénat, session ordinaire 2018-2019, fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le vote électronique, enregistré à la Présidence du Sénat le 24 octobre 2018.

DETRAIGNE Y., ESCOFFIER A-M., Rapport d'information n° 441 relatif au respect de la vie privée à l'heure des mémoires numériques du Sénat, session ordinaire 2008-2009, fait au nom des lois constitutionnelles, de législation, du suffrage universel, Règlement et d'administration générale, enregistré à la Présidence du Sénat le 27 mai 2009.

EBLE M., Amendement Article additionnel n° II-682 au projet de loi de finances pour 2018, session ordinaire 2017-2018, Sénat, enregistré à la Présidence du Sénat le 6 décembre 2017.

FERET C., POINTEREAU R., Rapport d'information n° 621 sur l'ancrage territorial de la sécurité intérieure du Sénat, session ordinaire 2019-2020, fait au nom de la délégation aux collectivités territoriales, enregistré à la Présidence du Sénat le 9 juillet 2020.

LONGUET G., Rapport n° 7 sur le devoir de souveraineté numérique du Sénat, session ordinaire 2019-2020, fait au nom de la commission d'enquête, enregistré à la Présidence du Sénat le 1er octobre 2019.

MEZARD J., Rapport n° 126 sur le bilan et le contrôle de la création, de l'organisation, de l'activité et de la gestion des autorités administratives indépendantes du Sénat, session ordinaire de 2015-2016, fait au nom de la commission d'enquête, enregistrée à la Présidence du Sénat le 28 octobre 2015.

PRIMAS S., ARTIGALAS V., BABARY S et al., proposition de loi n° 48 2019-2020, visant à garantir le libre choix du consommateur dans le cyberespace, *seconde session ordinaire de 2019-2020, Sénat,* enregistrée à la Présidence du Sénat le 10 octobre 2019.

SAVOLDELLI P., GAY F., APOURCEAU-POLY C et al., proposition de loi n° 717 relative au statut des travailleurs des plateformes numérique, Sénat, Session extraordinaire de 2018-2019, enregistrée à la Présidence du Sénat le 11 septembre 2019.

SIDO B., Rapport d'information n° 570 les robots et la loi du Sénat, session ordinaire 2015-2016, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, enregistré à la Présidence du Sénat le 3 mai 2016.

TURK A., Rapport public n°218 sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés du Sénat, session ordinaire de 2002-2003, fait au nom des lois constitutionnelles, de législation, du suffrage universel, Règlement et d'administration générale, enregistré à la Présidence du Sénat le 19 mars 2003.

Gouvernement

BRAIBANT G., Rapport public données personnelles et société de l'information Premier ministre sur la transposition en droit français de la directive n° 95-46, 1998.

CASTELLAZI M., MOATTI A et al., Rapport CGEDD n°013416-01 et CGE 2020/11/CGE/SG du gouvernement, février 2021.

MOCHON J-P., Rapport Vers une application effective du droit d'auteur sur les plateformes numériques de partage : Etat de l'art et propositions sur les outils de reconnaissance des contenus du gouvernement, 28 novembre 2019.

Projet de loi n° 338 pour une République numérique, étude d'impact, 9 décembre 2015.

Projet de loi n° 2187 relatif à la bioéthique du 24 juillet 2019.

Projet de loi n° 418 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, 9 mai 2020.

Projet de loi n° 3875 portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets, du 10 février 2021.

Projet de loi n° 523 relatif à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique du 8 avril 2021.

Projet de loi n° 4104 relatif à la prévention d'actes de terrorisme et au renseignement du 28 avril 2021.

B - TEXTES ET DECISIONS D'ORIGINE INTERNATIONALE

1 - Textes et décisions du Conseil de l'Europe

a - Instruments normatifs

Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (CEDH), Rome, 4 novembre 1950.

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dite « Convention 108 »), STE n° 108, Strasbourg, 28 janvier 1981.

Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dite « Convention 108+ ») du 18 mai 2018.

b - Travaux et actes non normatifs

Recommandation Rec(2004)11 du Comité des ministres aux Etats membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique.

Recommandation CM/Rec(2009)1 du Comité des Ministres aux Etats membres sur la démocratie électronique, adoptée le 18 février 2009.

Recommandation CM/Rec(2014)*7* du Comité des Ministres aux Etats membres sur la protection des lanceurs d'alerte, adoptée le 30 avril 2014.

CEPEJ, Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, adoptée le 4 décembre 2018.

Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel, Lignes directrices sur la reconnaissance faciale, 28 janvier 2021.

c - Décisions de la CEDH

CEDH, 26 novembre 1991, Observer et Guardian c. Royaume-Uni, req. n° 13585/88.

CEDH, Grande chambre, 12 février 2008, Guja c. Moldava, req. n° 14277/04.

CEDH, 21 juillet 2011, Heinisch c. Allemagne, req. n° 28274/08.

CEDH, 25 mai 2021, Big brother watch et autres c. Royaume-Uni, req. n° 58170/13, 62322/14 et 24960/15.

CEDH, 25 mai 2021, Centrum för rättvisa c. Suède, req. n° 35252/08.

2 - Textes et décision de l'UE et de l'EEE

a - Traités et Charte

CDFUE, *Journal officiel* n° C 326, 26/10/2012, p. 391-407

b - Règlements

Règlement (CE) n° 715/2007 – Véhicules à moteur – Émissions de polluants – Dispositif d'invalidation – Programme agissant sur le calculateur de contrôle moteur – Technologies et stratégies permettant de limiter la production des émissions de polluants – Moteur diesel.

Règlement (UE) 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission.

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).

Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) no 715/2007 et (CE) no 595/2009 et abrogeant la directive 2007/46/CE.

Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) no 2111/2005, (CE) no 1008/2008, (UE) no 996/2010, (UE) no 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) no 552/2004 et (CE) no 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) no 3922/91 du Conseil.

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 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 délégué (UE) 2019/945 de la Commission du 12 mars 2019 relatif aux systèmes d'aéronefs sans équipage à bord et aux exploitants, issus de pays tiers, de systèmes d'aéronefs sans équipage à bord.

Règlement (UE) 2019/1150 du Parlement Européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne.

Règlement (UE) 2019/2144 du Parlement Européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) no 78/2009, (CE) no 79/2009 et (CE) no 661/2009 du Parlement européen et du Conseil et les règlements (CE) no 631/2009, (UE) no 406/2010, (UE) no 672/2010, (UE) no 1003/2010, (UE) no 1005/2010, (UE) no 1008/2010, (UE) no 1009/2010, (UE) no 19/2011, (UE) no 109/2011, (UE) no 458/2011, (UE) no 65/2012, (UE) no 130/2012, (UE) no 347/2012, (UE) no 351/2012, (UE) no 1230/2012 et (UE) 2015/166 de la Commission (Texte présentant de l'intérêt pour l'EEE).

Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

c - Directives

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 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 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (refonte).

Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE Texte présentant de l'intérêt pour l'EEE et ses règlements délégués n° 2017/591 et 592 de la Commission en date du 1er décembre 2016.

Directive UE 2015/1535 du Parlement Européen et du Conseil du 9 septembre 2015.

Directive (UE) 2016/680 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) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.

Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (Texte présentant de l'intérêt pour l'EEE).

Directive (UE) 2019/771 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens, modifiant le règlement (UE) 2017/2394 et la directive 2009/22/CE et abrogeant la directive 1999/44/CE (Texte présentant de l'intérêt pour l'EEE).

Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union.

d - Décisions et actes *sui generis*

COMMISSION EUROPEENNE, décision du 27 juin 2017, affaire AT.38740, Moteur de recherche Google (Shopping).

e - Travaux et actes non normatifs

Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique, 2015/2103(INL).

COMMISSION EUROPEENNE, *Livre blanc. Intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance, Ec.europa.eu* [en ligne]. 19 février 2020 [Consulté le 2 mars 2021]. Disponible à l'adresse : https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf

Proposition n°2020/0361 de Règlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, 15 décembre 2020.

Proposition n° 2020/0374 de Règlement du Parlement européen et du Conseil relatif aux marchés numériques (législation sur les marchés numériques) en date du 15 décembre 2020.

COMMISSION EUROPEENNE, Projet de décret relatif à l'information du consommateur sur les mises à jour de logiciel, *ec.europa.eu* [en ligne]. 18 décembre 2020. [Consulté le 12 février 2021] Disponible à l'adresse : https://ec.europa.eu/growth/tools-databases/tris/fr/search/?trisaction=search.detail&year=2020&num=830

COMMISSION EUROPEENNE, Ethics guidelines for trustworthy AI, Digital-strategy.ec.europe.eu [en ligne]. 8 mars 2021 [Consulté le 15 avril 2021]. Disponible à l'adresse : https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Proposition n° 2021/0106 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, du 21 avril 2021.

Résolution du Parlement européen du 20 mai 2021 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 Maximillian Schrems (« arrêt Schrems II »).

COMMISSION EUROPEENNE, Orientations relatives à l'article 17 de la directive 2019/790 sur le droit d'auteur dans le marché unique numérique, in *eur-lex.europa.eu* [en ligne]. 04 juin 2021. [Consulté le 21 juin 2021]. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1625142238402&uri=CELEX%3A52021DC0288

f - Décisions des juridictions de l'UE

CJUE, grande chambre, 6 octobre 2015, affaire C-362/14.

CJUE, Grande chambre, 16 juillet 2020, affaire C-311/18.

g - Avis et documents de travail du groupe de l'article 29 et du CEPD

G29, avis n°3/2010 sur le principe de responsabilité, WP 173, adopté le 13 juillet 2010.

G29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679.

G29, Lignes directrices concernant les délégués à la protection des données, version révisée et adoptée le 5 avril 2017.

G29, lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 du 3 octobre 2017, version révisée le 6 février 2018.

G29, Lignes directrices sur la transparence au sens du RGPD du 11 avril 2018.

CEPD, Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement, version 3.0 du 4 juin 2019.

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, version 2.0, 4 juin 2019.

CEPD, lignes directrices 4/2019 relatives à l'article 25, protections des données dès la conception et protections des données par défaut, version 2.0, adoptées le 20 octobre 2020.

EDPB-EDPS, Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), du 18 juin 2021.

C - TEXTES, RAPPORTS ET JURISPRUDENCES D'ETATS ETRANGERS

Allemagne

BVERFG, Judgment of the Second Senate of 03 March 2009 - 2 BvC 3/07 -, paras. (1-166), *Bundesverfassungsgericht.de* [en ligne]. [Consulté le 2 avril 2021]. Disponible à l'adresse : https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html

DATEN ETHIK KOMMISSION, Opinion of the Data Ethics Commission, *datenethikkommission.de* [en ligne]. [Consulté le 2 juin 2021]. Disponible à l'adresse : https://datenethikkommission.de/wp-content/uploads/191023_DEK_Kurzfassung_en_bf.pdf

DEUTSCHER BUNDESTAG, Loi fondamentale pour la République fédérale d'Allemagne, art. 38, *Bundestag.de* [en ligne]. Mis à jour en novembre 2012. [Consulté le 15 janvier 2020]. Disponible à l'adresse : https://www.bundestag.de/resource/blob/189762/f0568757877611b2e434039d29a1a822/loi_fondamentale-data.pdf

Canada

GOUVERNEMENT DU CANADA, Directive on Automated Decision-Making, *tbs-sct.gc.ca* [en ligne]. 01 avril 2021 [Consulté le 22 juin 2021]. Disponible à l'adresse : https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

Etats-Unis d'Amérique

DEPARTMENT OF JUSTICE, Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations, *The United States, Department of Justice* [en ligne]. 27 Janvier 2020 [Consulté le 13 mars 2020]. Disponible à l'adresse : https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0

SUPREME COURT OF THE UNITED STATES OF AMERICA, Manhattan community acces corp. ET AL. V. Halleck Et AL, 17 juin 2019.

SUPREM COURT OF WISCONSIN, State of Wisconsin v. Loomis, case 2015AP157-CR [en ligne]. [Consulté le 22 juin 2020]. Disponible à l'adresse : https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690

Italie

Cour de cassation Italienne, chambre civile 1, 25 mai 2021, req. n° 14381.

Tribunal ordinaire de Bologne, 27 novembre 2020, RG 2949/2019.

D - ORGANISATIONS INTERNATIONALES

LA RUE F., *Report of the special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Rapport des Nations Unies, mai 2011.

NATIONS UNIES, CRC, Comité des droits de l'enfant, Examen des rapports soumis par les Etats parties en application de l'article 44 de la convention, p. 12, *Tout sur les droits de l'enfant.fr* [en ligne]. 22 juin 2009 [Consulté le 12 octobre 2019] https://www.toutsurlesdroitsdelenfant.fr/documents/cclfinalescomite2009.pdf

OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel en date du 23 septembre 1980.

INDEX

TABLE DES MATIERES

La transparence des traitements algorithmiques : de l'étude juridique d'un enjeu démocratique

The transparency of algorithmic processing: a legal study of a democratic issue

Résumé

Ces travaux s'inscrivent dans l'étude des principales réglementations portant sur la transparence des traitements algorithmiques. Il apparait que ces régimes juridiques poursuivent des objectifs et des techniques juridiques de différentes natures. Cette transparence ne constitue pas une unicité conceptuelle puisqu'elle renvoie le plus souvent à la réalisation de la démocratie administrative, et dans d'autres cas, en un droit à l'information permettant à une personne physique ou morale d'assurer un consentement libre et éclairé notamment.

Cette situation a pour incidence que des faits juridiques, ayant par ailleurs des effets sur les personnes, ne sont pas totalement appréhendés, car la transparence des traitements algorithmiques s'opère surtout par des régimes juridiques de rattachement, poursuivant des objectifs antérieurs à l'avènement de l'informatique, ce qui affecte la pertinence et l'efficacité de certaines règlementations. Or, la transparence des outils numériques devient la clé de voûte indispensable au respect des droits et libertés, et plus largement de l'ordre juridique, aussi bien pour les traitements publics que privés.

Pour ce faire, la compréhension des traitements implique une nouvelle conciliation avec les libertés économiques. Toutefois, quand bien même la réalisation de cette transparence s'opérerait juridiquement et techniquement, il convient de considérer qu'elle ne peut légitimer le recours au numérique à tous les usages tant certains sont attentatoires aux libertés. C'est la raison pour laquelle est suggéré un écosystème juridique intégrant un nouvel équilibre des pouvoirs à l'ère numérique.

Abstract

This work is part of the study of the main regulations on the transparency of algorithmic processing. It appears that these legal systems pursue different objectives and legal techniques. This transparency does not constitute a conceptual uniqueness since it refers most often to the realisation of administrative democracy, and in other cases, to a right to information allowing a natural or legal person to ensure free and informed consent in particular.

This situation has the effect that legal facts, which otherwise have effects on individuals, are not fully understood, because the transparency of algorithmic processing is carried out mainly through legal regimes, pursuing objectives that predate the advent of information technology, which affects the relevance and effectiveness of certain regulations. However, the transparency of digital tools is becoming the keystone for the respect of rights and freedoms, and more broadly of the legal order, for both public and private processing.

In order to do this, the understanding of processing implies a new conciliation with economic freedoms. However, even if this transparency can be achieved legally and technically, it should be considered that it cannot legitimise the use of digital technology for all purposes, as some of them infringe on freedoms. This is why a legal ecosystem is suggested that integrates a new balance of power in the digital age.

Mots-clés : transparence, algorithme, démocratie, intelligence artificielle (IA), souveraineté, libertés, droit, Etat, loyauté, vulnérabilité, intelligibilité, décision automatisée

Keywords : transparency, algorithm, democracy, artificial intelligence (AI), sovereignty, freedoms, law, State, fairness, vulnerability, intelligibility, automated decision