

INTERNATIONAL JOURNAL OF DIGITAL AND DATA LAW

REVUE INTERNATIONALE DE DROIT
DES DONNÉES ET DU NUMÉRIQUE

Vol. 5 - 2019



ISSN 2553-6893

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

*Les propos publiés dans cet article
n'engagent que leur auteur.*

*The statements published in this article
are the sole responsibility of the author.*

Droits d'utilisation et de réutilisation

Licence Creative Commons – Creative Commons License -



Attribution

Pas d'utilisation commerciale – Non Commercial

Pas de modification – No Derivatives

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, elle est avocate au barreau de Paris, associée de BeRecht Avocats.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il aussi avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons **CC-BY-NC-ND** :

- 1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;
- 2) la *Revue internationale de droit des données et du numérique (RIDDN)/ International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. She is an attorney at law at the Paris Bar and a partner of BeRecht Avocats.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license **CC-BY-NC-ND**:

- 1) the *International Journal of Open Governments/ la Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;
- 2) the *International Journal of Digital and Data Law / la Revue internationale de droit des données et du numérique (RIDDN)* [ISSN 2553-6893].

QUARANTE ANS DE CONSTRUCTION DU DROIT DU NUMÉRIQUE. LES ENJEUX JURIDIQUES DE L'AVÈNEMENT D'UN MONDE INTELLIGENT

par **William GILLES**, Directeur du master Droit des données, des administrations numériques et des gouvernements ouverts, Président de l'IMODEV, Avocat au barreau de Paris (BeRecht Avocats) et **Irène BOUHADANA**, Directrice du master Droit des données, des administrations numériques et des gouvernements ouverts, Secrétaire générale de l'IMODEV.

L'ère du numérique est porteuse d'une révolution des savoirs et de l'information en permettant une meilleure diffusion des données. La circulation de l'information permise par les technologies contemporaines constitue un enjeu géostratégique et juridique majeur du monde contemporain. À cet égard, nous assistons aujourd'hui à une révolution industrielle, économique et démocratique comparable à celle qui se produisit à l'époque de Gutenberg¹ avec l'invention de l'imprimerie. Si Internet est l'héritage des recherches menées après la Seconde Guerre mondiale pour permettre l'émergence du réseau Arpanet en 1969², ces avancées n'ont été possibles que parce que des soubassements plus anciens ont permis d'ouvrir la voie à de tels progrès.

Parmi ces innovations, il faut évoquer l'invention des premiers calculateurs au XVII^e siècle, époque à laquelle furent inventées notamment la Pascaline puis la machine Arithmétique en 1642³. Sans exhaustivité, il est aussi possible de mentionner l'invention au même siècle de la machine de Leibniz⁴ que son auteur nomma lui-même : « banque à calculer vivante », car grâce à elle il était désormais possible de réaliser non seulement les quatre opérations de base de calcul (addition, multiplication, soustraction, division), mais aussi des opérations plus complexes dont les racines carrées et cubiques.

Au XIX^e siècle, Babbage fut le premier à concevoir une machine à calculer programmable en faisant évoluer les premiers calculateurs vers des machines analytiques⁵. Si Babbage ne put construire complètement sa machine analytique faute de moyens financiers et techniques, il faut cependant relever que la structure de la machine

¹ R. WEAVER, *From Gutenberg to the Internet: Free Speech: Advancing Technology and the Implications for Democracy*, Carolina Academic Press, 2013.

² Cf. M. WALDROP, « DARPA and the Internet Revolution », 50 years of Bringing the Gap, Faircount Media Group, 2016.

³ Cf. B. PASCAL, « Machine Arithmétique. À Monseigneur le chancelier [Pierre Seguier] (1645) », in B. PASCAL, *Œuvres complètes*, Hachette, 3^e édition, 1872.

⁴ G. LEIBNIZ, « Trois lettres à Jean-Frédéric de Hanovre sur le problème de la liberté », *Philosophie*, n°4, 2002.

⁵ Ch. BABBAGE, *Passages from the Life of a Philosopher*, Longmann-Green-Longman-Roberts & Green, 1864.

analytique de Babbage était proche de celle des ordinateurs actuels. Une différence notable sépare néanmoins l'invention de Babbage et nos ordinateurs contemporains puisque dans le premier cas le mode d'alimentation reposait sur une machine à vapeur alors que nos ordinateurs fonctionnent grâce à l'électricité qui a constitué une autre révolution majeure.

Pour réaliser son invention Babbage a su s'appuyer sur des innovations existantes qu'il a perfectionnées, comme le système de cartes perforées du métier à tisser Jacquard inventé en 1801, mais il a aussi bénéficié de l'assistance de Augusta Ada King dite comtesse de Lovelace qui est considérée comme la première programmeuse de l'histoire de l'informatique pour avoir créé le premier algorithme exécutable par une machine⁶.

D'autres perfectionneront la machine de Babbage ou s'inspireront de ses travaux pour développer les machines que nous connaissons actuellement.

Le futurologue Ray Kurzweil expliquait en 2005⁷ qu'avec le doublement du taux de progrès technologiques tous les dix ans ou presque, nous assisterions à autant de changements dans les 90 prochaines années qu'au cours des 10 000 dernières années et que les changements des 100 prochaines années seraient équivalents à ceux des 20 000 dernières années.

Ces prédictions font prendre conscience que les évolutions technologiques que nous avons connues au cours de ces dernières années, si elles apparaissent importantes au regard des siècles passés, ne sont pourtant que les prémices des innovations futures. En effet, il nous semblait que nous sommes seulement entrés dans l'an IV de la révolution informatique/numérique et que de nombreux défis techniques, institutionnels et juridiques restent à relever.

§ 1 – LA CONSTRUCTION INSTITUTIONNELLE ET JURIDIQUE DE LA REVOLUTION NUMERIQUE : DE L'AN I A L'AN IV

Quatre étapes charnières ont marqué l'histoire de la révolution informatique, puis numérique, allant de l'an I à l'an IV. Cette structuration est le fruit de notre réflexion. Elle peut faire l'objet de débats, mais elle nous semble bien refléter les différentes évolutions juridiques et institutionnelles qui ont accompagné les progrès technologiques depuis le lancement de l'ARPANET en 1969.

L'an I est marqué par le contexte géopolitique de la guerre froide et la nécessité des grandes puissances de marquer leur autonomie technologique. Internet est le fruit de ces rivalités scientifiques et géostratégiques. En effet, il est la conséquence de la création de l'agence ARPA, qui fait suite au choc créé par le lancement de

⁶ Ch. BABBAGE, *op. cit.*

⁷ R. KURZWEIL, *Kurzweil's Law*, 23 septembre 2005, accessible à : <http://longnow.org/seminars/02005/sep/23/kurzweils-law/>

Spoutnik et les autres innovations soviétiques⁸. Cette agence pilotera le développement d'Arpanet, ancêtre d'Internet.

Alors que les États-Unis développent l'ARPANET et travaillent à son basculement vers l'Internet, la France doit faire face aux conséquences des échecs de ses choix politiques et institutionnels en matière d'innovation. Les succès du plan calcul lancé en 1966 ne furent qu'éphémères : la délégation de l'informatique créée en 1967 fut supprimée par Valéry Giscard d'Estaing en 1974 et la grande compagnie informatique française, à savoir la compagnie internationale pour l'informatique créée en 1966 fut vendue à une entreprise américaine en 1975 alors qu'elle avait créé le premier ordinateur français en 1968⁹. De même, la France se retira du projet européen Unidata¹⁰. Pourtant, la France disposait de scientifiques reconnus, dont Louis Pouzin dont les travaux sur le Datagramme ont inspiré Vinton Cerf et Robert Kahn dans le développement du protocole TCP-IP créé en 1973¹¹ qui permit le basculement de l'ARPANET vers Internet en 1983.

Si au regard de ces éléments, l'apport de la France et de l'Europe est donc à nuancer du point de vue technologique, il en est tout autrement sur plan juridique.

L'an I a permis à la France de jeter les bases d'une législation qui fut à l'époque l'une des plus avancées en matière de régulation technologique.

Les années 1970 sont pour la France l'occasion de réfléchir à l'impact de la société de l'information et à sa régulation juridique. Plusieurs commissions sont mises en place pour répondre aux préoccupations des Français nées notamment de l'affaire Safari. Ce « Système Automatisé pour les Fichiers administratifs et Répertoires des Individus » révélé par le Journal *Le Monde* en 1974 suscita un émoi auprès des Français, car il devait permettre la création d'une base de données centralisée de la population utilisant un identifiant commun à l'ensemble des fichiers administratifs¹². La crainte était que cet identifiant soit utilisé par l'administration pour interconnecter les fichiers administratifs.

Pour remédier au climat de méfiance vis-à-vis de l'utilisation de l'informatique dans la société, et notamment par son administration, la France se dota d'un cadre juridique reposant sur deux lois destinées à devenir de grandes lois. D'une part, la loi du 6 janvier 1978¹³ créa la Commission nationale de l'informatique et des libertés (CNIL) et affirma à son article 1^{er} que l'informatique doit être au service de chaque citoyen. D'autre part, la loi du 17

⁸ DARPA, *Innovation at DARPA*, 2016.

⁹ T. GASTON-BRETON, « Le Plan Calcul, l'échec d'une ambition », *Les Échos*, 20 juillet 2012.

¹⁰ Ibidem.

¹¹ Cf. V. CERF, R. KAHN, « A Procol for Packet Network Intercommunication », *IEEE Trans on Comms*, Vol Com-22, n° 5, mai 1974.

¹² Ph. BOUCHER, « SAFARI ou la chasse aux Français », *Le Monde*, 21 mars 1974.

¹³ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

juillet 1978¹⁴ créa la Commission d'accès aux documents administratifs (CADA) et institua un régime d'accès aux documents administratifs.

La prise de conscience des enjeux relatifs à l'informatique et des dangers sur la vie privée n'est cependant pas propre à la France, puisqu'au niveau international, l'OCDE publie en 1980 les lignes directrices régissant la protection de la vie privée et les flux transfrontières des données de caractère personnel¹⁵, alors que le Conseil de l'Europe adopte le 28 janvier 1981 la Convention 108 qui est la première convention internationale sur le traitement automatisé des données à caractère personnel¹⁶.

L'an I a donc jeté les bases technologiques, mais aussi juridiques de la révolution contemporaine, avec une prédominance de l'influence américaine sur le plan technique et au contraire une prééminence européenne en matière de législation. Cette répartition perdure aujourd'hui comme le montre la portée de la jurisprudence européenne et du règlement général sur la protection des données, qui, en l'an IV de la révolution numérique, n'ont pas uniquement une influence dans l'Union européenne, mais invitent plus largement les démocraties à se préoccuper de la régulation de la donnée.

En 40 ans, les enjeux juridiques sont à la fois restés les mêmes dans leur fondement et ont connu une évolution dans leur mise en œuvre. Quant au fondement des enjeux juridiques, il s'agit toujours de s'assurer que l'informatique reste au service du citoyen et qu'elle ne porte pas une atteinte excessive à la vie privée. Quant à la mise en œuvre de ces enjeux sont intervenus entre temps l'an II et l'an III de la révolution numérique qui nous placent désormais dans un contexte radicalement différent.

L'an II qui s'étend dans notre raisonnement sur toute la décennie 1990 et la première moitié de la décennie 2000 est dominé par le développement de l'Internet, la naissance de Google en 1998 et des premiers réseaux sociaux, dont Facebook en 2004. Au plan juridique, l'an II se caractérise par l'adoption de la directive européenne de 1995 sur la protection des données personnelles¹⁷, obligeant les États membres de l'Union à harmoniser leur législation en la matière. Cependant, la portée de la législation est alors essentiellement régionale, puisque mise en œuvre au sein de l'Union européenne.

L'an III, qui, selon nous, couvre la période 2004 à 2016, correspond au processus de numérisation de la société. Cet âge n'est pas seulement celui du développement des GAFA, il

¹⁴ 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.

¹⁵ OCDE, *Recommandation du Conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, 23 octobre 1980.

¹⁶ Conseil de l'Europe, Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981.

¹⁷ 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.

correspond surtout au déploiement de la révolution numérique dans l'ensemble des domaines d'activité humaine, avec le développement de nouvelles notions telles que l'ubérisation de la société. Les législateurs des différents pays prennent conscience à cette époque de la nécessité de repenser nos législations pour mieux face au poids des géants de l'Internet et à la dérégulation qui en résulte, par exemple, mais pas uniquement en matière fiscale. Cette époque est ainsi celle de la réflexion puis de la mise en œuvre par l'OCDE et le G20 du projet sur l'érosion de la base d'imposition et les transferts de bénéfice (BEPS)¹⁸.

L'an III est également l'âge de l'ouverture des données¹⁹. Dans cette perspective, l'Union européenne a modifié en 2013²⁰, la directive qu'elle avait adoptée en 2003, afin d'harmoniser les législations des États membres en matière de réutilisation des données publiques. Pour y répondre, la France a dû reconnaître, par l'ordonnance du 6 juin 2005²¹, un droit à la réutilisation des données publiques, la seconde directive ayant été transposée par la loi du 28 décembre 2015²².

Sur le plan de la protection des données, c'est aussi le temps de la jurisprudence européenne de 2014 Google Spain²³, qui reconnaît l'existence d'un droit au déréférencement, amorçant ainsi l'encadrement des géants de l'Internet. Cette jurisprudence a préparé la voie à un mouvement plus vaste de régulation des données, qui aboutit, le 27 avril 2016, à l'adoption du règlement général sur la protection des données²⁴, entré en vigueur le 25 mai 2018, auquel il faut ajouter la directive 2016/680²⁵.

¹⁸ Le projet BEPS a été lancé en 2013 et a abouti OCDE à la définition de 15 actions en 2015.

Cf. OCDE, *Lutter contre l'érosion de la base d'imposition et le transfert de Bénéfices*, 2013, accessible à : <http://www.oecd.org/fr/fiscalite/lutter-contre-l-erosion-de-la-base-d-imposition-et-le-transfert-de-benefices-9789264192904-fr.htm>.

Voir aussi OCDE, Exposé des actions 2015, Projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices, 2015, accessible à : <http://www.oecd.org/fr/ctp/beps-expose-des-actions-2015.pdf>.

¹⁹ Voir W. Gilles, « Libre réflexion sur le droit dit "de l'open data". Origine, contours et évolution dans le cadre du droit de l'Union européenne », *La semaine juridique. Édition générale*, supplément au n° 9, 27 février 2017, p. 13.

²⁰ Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public.

²¹ Ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques.

²² Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public (1).

²³ Arrêt de la Cour (grande chambre) du 13 mai 2014, Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, accessible à :

<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62012CJ0131>.

²⁴ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

²⁵ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Cette nouvelle législation a conduit les pays européens à modifier leur législation, la France l'ayant fait avec la loi 20 juin 2018²⁶, qui a complété une première évolution juridique apportée par la loi pour une République numérique de 2016²⁷.

Les conséquences de ces évolutions issues de la régulation des données sont aussi internationales puisque, par exemple, le Conseil de l'Europe a lui-même modifié le 18 mai 2018 sa convention 108²⁸ pour tenir compte de l'adoption du règlement général sur la protection des données. De même, il faut noter que d'autres pays, comme le Brésil, viennent aussi d'adopter une législation en matière de protection des données. Il est possible de penser que l'influence européenne n'y est pas étrangère.

Aux États-Unis, l'affaire Cambridge Analytica/Facebook²⁹ de 2018 a permis de faire ressortir les inconvénients issus de l'absence de régulation de la protection des données personnelles à l'heure où se profilait l'entrée en vigueur du règlement général sur la protection des données au sein de l'Union européenne.

Ces évolutions technologiques et juridiques nous ont fait entrer de plain-pied dans ce que nous appelons l'an IV de la Révolution numérique. Cet âge qui correspond à l'émergence d'une société des données est matérialisé par le développement de technologies disruptives comme la blockchain et l'intelligence artificielle qui nous conduisent à repenser la place de l'homme et la régulation de la société. Ce sera l'objet de la conclusion des 3^e journées universitaires sur les enjeux des gouvernements ouverts et du numérique, qui aura lieu demain à partir de 17 heures en Sorbonne, en amphithéâtre Richelieu.

§ 2 – LES QUESTIONNEMENTS DE LA REVOLUTION NUMERIQUE DE L'AN IV : LES DEFIS JURIDIQUES DU MONDE CONNECTE

A) L'avènement de l'âge de raison : la complexité des réponses aux interrogations juridiques nées de l'an IV de la révolution numérique

Après les évolutions juridiques et institutionnelles de ces 40 dernières années, il est possible de se demander si l'an IV marque enfin le début de l'âge de raison.

²⁶ Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, accessible à :

https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=980CF4A599209F423164522AF7057F23.tplgfr31s_3?cidTexte=JORFTEXT000037085952&categorieLien=id.

²⁷ Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, accessible à : <https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=14>.

²⁸ Cf. Council of Europe, Decision of the Committee of Ministers, 128th session of the Committee of Ministers, Elsinore, 18 May 2018.

Voir aussi : Council of Europe, Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data, 2018, accessible à : <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>.

²⁹ CNIL, Affaire Cambridge Analytica/Facebook, 12 avril 2018, accessible à : <https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook>.

Une première réponse pourrait être positive si l'on considère que l'époque contemporaine est aussi celle qui se défait de l'approche du numérique opposant ses partisans qui n'y voient que des avantages et ses opposants qui n'y voient que des inconvénients. Il semble exister une prise de conscience que cette binarité ne permet plus de prendre en compte la complexité de la matière.

Sans être exhaustif, une illustration de l'appréhension de la complexité du droit du numérique par le juge peut être apportée à travers l'exemple du droit au déréférencement. En effet, après l'arrêt Google Spain de 2014³⁰ et la consécration du droit au déréférencement, se pose la question de l'effectivité de sa mise en œuvre. Autrement dit, les premières questions pratiques apparaissent. Ainsi, comment articuler le droit à l'oubli et le droit à l'information ? C'est tout le sens de la question posée par l'arrêt Manni du 9 mars 2017³¹.

Toujours pour analyser l'effectivité du droit au déréférencement, le Conseil d'État a rendu deux décisions en 2017 destinées à poser des questions préjudicielles à la Cour de Justice de l'Union européenne pour savoir quelle est la portée territoriale du droit au déréférencement³² et quelles sont les obligations qui pèsent sur les moteurs de recherche lorsque le déréférencement concerne des données sensibles³³.

1) La question de la portée territoriale du droit au déréférencement : la décision du Conseil d'État du 19 juillet 2017

Dans sa décision du 19 juillet 2017, le Conseil d'État demande en premier lieu à la Cour de justice de l'Union européenne si le « droit au déréférencement » tel que consacré par son arrêt Google Spain du 13 mai 2014 doit être interprété comme signifiant que l'exploitant d'un moteur de recherche est tenu, en cas d'exercice du droit au déréférencement, « d'opérer ce déréférencement sur l'ensemble des noms de domaine de son moteur de telle sorte que les liens litigieux n'apparaissent plus, quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée, y compris hors du champ d'application territorial de la directive du 24 octobre 1995. »³⁴ Le Conseil d'État interroge ensuite la Cour de Justice de l'Union européenne sur les conséquences d'une réponse négative à la première question. Dans le cas où il n'existe pas d'obligation de mettre en œuvre le déréférencement sur l'ensemble des noms de domaine du moteur de recherche, c'est-à-dire, y

³⁰ Arrêt de la Cour (grande chambre) du 13 mai 2014, Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González

³¹ Arrêt de la Cour (deuxième chambre) du 9 mars 2017, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contre Salvatore Manni, Affaire C-398/15.

³² CE, 19 juillet 2017, Google Inc. Affaire pendante, référencée « C-507/17 – Google (Portée territoriale du déréférencement) » auprès de la CJUE.

³³ CE, 24 février 2017, 391 000, Publié au recueil Lebon. Affaire pendante, référencée « Affaire C-136/17 - G. C. e. a. (Déréférencement de données sensibles) » auprès de la CJUE.

³⁴ CE, 19 juillet 2017, Google Inc.

compris pour les extensions non européennes, le droit au déréférencement a-t-il à l'inverse une portée uniquement nationale. Autrement dit, le droit au déréférencement signifie-t-il que l'exploitant d'un moteur de recherche est seulement tenu, « lorsqu'il fait droit à une demande de déréférencement, de supprimer les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur sur le nom de domaine correspondant à l'État où la demande est réputée avoir été effectuée ou, plus généralement, sur les noms de domaine du moteur de recherche qui correspondent aux extensions nationales de ce moteur pour l'ensemble des États membres de l'Union européenne ? »³⁵ Enfin, le Conseil d'État demande, en complément de la deuxième question, à la Cour de Justice de l'Union européenne si le droit au déréférencement doit être interprété comme signifiant que « l'exploitant d'un moteur de recherche faisant droit à une demande de déréférencement est tenu de supprimer, par la technique dite du "géoblocage", depuis une adresse IP réputée localisée dans l'État de résidence du bénéficiaire du "droit au déréférencement", les résultats litigieux des recherches effectuées à partir de son nom, ou même, plus généralement, depuis une adresse IP réputée localisée dans l'un des États membres soumis à la directive du 24 octobre 1995, ce indépendamment du nom de domaine utilisé par l'internaute qui effectue la recherche ? »³⁶. Autrement dit, il s'agit pour le Conseil d'État, de savoir si l'exercice du droit au déréférencement implique pour un moteur de recherche de recourir à la technique du « géoblocage » pour empêcher l'accès aux résultats litigieux du moteur de recherche.

2) La question de la mise en œuvre du droit au déréférencement des données sensibles : la décision du Conseil d'État du 24 février 2017

Dans sa décision du 24 février 2017, le Conseil d'État interroge la Cour de justice de l'Union européenne sur l'applicabilité ou non aux moteurs de recherche de l'interdiction énoncée aux paragraphes 1 et 5 de l'article 8 de la directive du 24 octobre 1995. L'article 8 de ce texte est relatif aux traitements portant sur des catégories particulières de données. Le premier alinéa pose le principe d'interdiction de traiter les données à caractère personnel portant sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle. Cependant, les alinéas 2 et 3 posent aussitôt des exceptions à cette interdiction, par exemple, en cas de consentement explicite de la personne concernée par le traitement, lorsque les données sont traitées pour défendre les intérêts vitaux de la personne concernée ou encore lorsque le traitement des

³⁵ CE, 19 juillet 2017, Google Inc.

³⁶ CE, 19 juillet 2017, Google Inc.

données répond à une finalité de médecine préventive ou de diagnostic médical. Le 4^e alinéa permet, quant à lui, aux États membres de prévoir une exception à l'interdiction de traitement des données sensibles pour un motif d'intérêt public important. Enfin, le 5^e alinéa porte sur le traitement des données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté. Il est prévu que le traitement de ces données « ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. | Les États membres peuvent prévoir que les données relatives aux sanctions administratives ou aux jugements civils sont également traitées sous le contrôle de l'autorité publique. »³⁷

S'il est admis que les moteurs de recherche constituent des responsables de traitement, le Conseil d'État s'interroge en premier lieu sur la portée des interdictions énoncées à l'article 8 de la directive du 24 octobre 1995 pour les moteurs de recherche du fait de la nature spécifique de leur activité qui est de faire apparaître sur leur page Internet les résultats des recherches faites par les internautes. Le Conseil d'État demande donc dans un premier temps à la Cour de Justice de l'Union européenne si « 1^o Eu égard aux responsabilités, aux compétences et aux possibilités spécifiques de l'exploitant d'un moteur de recherche, l'interdiction faite aux autres responsables de traitement de traiter des données relevant des paragraphes 1 et 5 de l'article 8 de la directive du 24 octobre 1995, sous réserve des exceptions prévues par ce texte, est [...] également applicable à cet exploitant en tant que responsable du traitement que constitue ce moteur ».

En deuxième lieu, le Conseil d'État envisage le cas d'une réponse positive à la première question, c'est-à-dire, l'hypothèse où l'interdiction de traiter des données sensibles énoncée à l'article 8 de la directive du 24 octobre 1995 s'appliquerait aux moteurs de recherche. Une réponse positive signifierait-elle que le moteur de recherche ne pourrait pas faire droit à une demande de déréférencement. En effet, le fait de déréférencer ces données sensibles s'analyserait dans une telle hypothèse comme un traitement de données interdit au titre de l'article 8. Cependant, comme le deuxième alinéa prévoit aussi que l'interdiction de traiter ces données sensibles cesse en cas de consentement explicite de la personne concernée par le traitement, il est possible de penser que le fait pour la personne concernée d'exercer un droit au déréférencement équivaut à donner son accord explicite à traiter ces données. Toutefois, le même article 8 prévoit aussi que les États

³⁷ Article 8 de 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.

membres peuvent adopter une législation interdisant dans certains cas que l'interdiction au traitement des données sensibles soit levée, même en cas de consentement explicite de la personne concernée³⁸. Ces différentes hypothèses correspondent à autant de questions posées par le Conseil d'État à la Cour de justice de l'Union européenne qui sont examinées ci-après.

Dans un premier temps, le juge français demande au juge européen si les paragraphes 1 et 5 de l'article 8 de la directive du 24 octobre 1995 doivent être interprétés comme signifiant que « que l'interdiction ainsi faite, sous réserve des exceptions prévues par cette directive, à l'exploitant d'un moteur de recherche de traiter des données relevant de ces dispositions l'obligerait à faire systématiquement droit aux demandes de déréférencement portant sur des liens menant vers des pages web qui traitent de telles données ». Autrement dit, le fait qu'un moteur de recherche ne soit pas soumis à l'interdiction de traiter des données signifie-t-il qu'il a l'obligation de systématiquement déréférencer les données sensibles prévues à l'article 8 de la directive du 24 octobre 1995 lorsqu'un internaute invoque le droit au déréférencement ?

Ensuite, le Conseil d'État s'interroge plus spécifiquement sur la portée de l'interdiction de traitement de données sensibles énoncée à l'article 8 paragraphe 2, a) et e), de la directive du 24 octobre 1995. Le premier cas autorise le traitement des données sensibles lorsque la personne concernée a explicitement donné son accord, dès lors que l'État membre n'a pas adopté une législation interdisant de lever l'interdiction par consentement de la personne concernée. Le second cas permet de traiter les données sensibles lorsque ces données ont été manifestement rendues publiques par la personne concernée ou sont nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice. Le Conseil d'État interroge la Cour de justice de l'Union européenne sur la portée de ces deux exceptions à l'égard des exploitants d'un moteur de recherche du fait des responsabilités, compétences et possibilités spécifiques liées à la nature de leur activité. Plus précisément, il est demandé à la Cour de Justice de l'Union européenne si l'exploitant d'un moteur de recherche peut « refuser de faire droit à une demande de déréférencement lorsqu'il constate que les liens en cause mènent vers des contenus qui, s'ils comportent des données relevant des catégories énumérées au paragraphe 1 de l'article 8, entrent également dans le champ des exceptions prévues par le paragraphe 2 de ce même article, notamment le a) et le e). »³⁹

En outre, le Conseil d'État s'interroge sur l'articulation entre droit au déréférencement d'une part, et droit à la liberté d'expression d'autre part. Ainsi, il évoque le cas où l'exercice du droit au déréférencement pourrait se heurter au droit de savoir ou de s'exprimer. Sont ainsi concernées les données à caractère personnel

³⁸ Cf. article 8, 2, a.

³⁹ CE, 24 février 2017, 391 000, Publié au recueil Lebon. Affaire pendante, référencée « Affaire C-136/17 - G. C. e. a. (Déréférencement de données sensibles) » auprès de la CJUE.

dont le traitement est nécessaire aux *seules fins de journalisme ou d'expression artistique ou littéraire*. Autrement dit, est en jeu la question de l'articulation entre l'article 8 de la directive du 24 octobre 1995 et l'article 9 de ce texte qui demande aux États membres de prévoir notamment pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations à l'interdiction de traiter des données sensibles lorsqu'il s'agit uniquement de concilier le droit à la vie privée avec les règles relatives à la liberté d'expression⁴⁰. Or, l'articulation entre ces deux dispositions peut s'avérer difficile.

Si le moteur de recherche devait répondre favorablement au droit au déréférencement, il en résulterait une difficulté pour les journalistes ou les auteurs de traiter les données en question puisque celles-ci, une fois déréférencées, ne seraient plus accessibles à partir du moteur de recherche concerné. Il est à noter cependant que la jurisprudence Google Spain, rendue dans le cadre de la directive du 24 octobre 1995, a prévu un droit au déréférencement et non un droit à l'effacement. Les données en question seraient donc toujours accessibles sur le site Internet sur lequel elles figurent. En revanche, il est à rappeler que le règlement général sur la protection des données a une portée plus large puisqu'il prévoit un droit à l'effacement des données⁴¹. Les conséquences de l'exercice d'un droit à l'effacement des données sur le droit à l'information seront donc plus importantes dans le cadre de la mise en œuvre du RGPD, et il sera intéressant d'étudier les premières décisions de justice lorsqu'elles interviendront sur ce sujet.

Dans cette attente, le Conseil d'État demande à la Cour de justice de l'Union européenne de se prononcer sur l'interprétation à donner à la directive du 24 octobre 1995 qui prévoit que « lorsque les liens dont le déréférencement est demandé mènent vers des traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire qui, à ce titre, en vertu de l'article 9 de la directive du 24 octobre 1995, peuvent collecter et traiter des données relevant des catégories mentionnées à l'article 8, paragraphes 1 et 5, de cette directive, l'exploitant d'un moteur de recherche peut, pour ce motif, refuser de faire droit à une demande de déréférencement »⁴².

⁴⁰ L'article 9 de la directive du 24 octobre 1995 prévoit que :

« Article 9 - Traitements de données à caractère personnel et liberté d'expression

Les États membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression. »

⁴¹ Cf. l'article 17 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

⁴² CE, 24 février 2017, 391 000, Publié au recueil Lebon. Affaire pendante, référencée « Affaire C-136/17 – G. C. e. a. (Déréférencement de données sensibles) » auprès de la CJUE.

En troisième lieu, le Conseil d'État envisage le cas d'une réponse négative à la première question, c'est-à-dire, l'hypothèse où l'interdiction de traiter des données sensibles énoncée à l'article 8 de la directive du 24 octobre 1995 ne s'appliquerait pas aux moteurs de recherche. Dans cette perspective, le Conseil d'État est amené à poser trois sous-questions à la Cour de justice de l'Union européenne.

La première sous-question invite à se demander quelles sont les exigences spécifiques applicables à l'exploitant d'un moteur de recherche dans l'hypothèse où il n'est pas soumis à l'interdiction de traiter les données sensibles prévue par l'article 8 de la directive du 24 octobre 1995. En effet, comme expliqué précédemment, les exploitants des moteurs de recherches sont considérés comme des responsables de traitement de données à caractère personnel. Si la Cour de Justice de l'Union européenne devait considérer que les exploitants des moteurs de recherche ne sont pas soumis, contrairement aux autres responsables de traitement de données à caractère personnel, à l'interdiction de traiter les données sensibles prévue par l'article 8 de la directive du 24 octobre 1995, ce régime spécifique résulterait des responsabilités, des compétences et des possibilités liées à la nature spécifique de leur activité. Cependant, l'absence de soumission à l'interdiction prévue à l'article 8 de la directive du fait de la nature particulière de leur activité ne doit pas signifier qu'aucune obligation ne pèse sur eux en matière de traitement des données, d'autant plus lorsque celles-ci sont sensibles. C'est à cette question qu'est invitée à répondre la Cour de justice de l'Union européenne lorsque le Conseil d'État lui demande « à quelles exigences spécifiques de la directive du 24 octobre 1995 l'exploitant d'un moteur de recherche, compte tenu de ses responsabilités, de ses compétences et de ses possibilités, doit-il satisfaire ».

La deuxième sous-question porte sur l'exercice d'un droit au déréférencement renvoyant à des pages web contenant des données dont la publication est illicite. Dans une telle hypothèse, le Conseil d'État s'interroge sur les conséquences de cette situation à l'égard de l'exploitant du moteur de recherche. Trois situations peuvent être envisagées.

Dans la *première situation*, il s'agit de savoir si la directive du 24 octobre 1995 impose à l'exploitant d'un moteur de recherche de supprimer ces liens de la liste des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur ». Cette première interrogation met donc en lumière le fait de savoir s'il existe ou non une obligation pour l'exploitant du moteur de recherche, de répondre à la demande de déréférencement lorsqu'elle porte sur des données dont la publication est illicite.

La *deuxième situation* envisagée consiste à se demander si la directive du 24 octobre 1995 implique uniquement que l'exploitant du moteur de recherche tienne compte du fait que les pages web contiennent des données dont la publication est illicite « pour apprécier le bien-fondé de la demande de déréférencement ». Dans cette deuxième situation, la mise en œuvre du droit au déréférencement dépend de l'exploitant du moteur de

recherche qui apprécie le bien-fondé de la demande, celui-ci ayant comme seule obligation de prendre en considération, lorsque la demande lui est soumise, le fait que les pages web contiennent des données dont la publication est illicite.

La troisième situation présente l'hypothèse où le fait que les pages web contiennent des données dont la publication est illicite est sans incidence sur l'appréciation que l'exploitant du moteur de recherche porte à la demande de déréférencement.

Autrement dit, dans le premier cas, l'existence de données dont la publication est illicite constitue une obligation liant l'exploitant du moteur de recherche ; dans le deuxième cas, elle est une circonstance à prendre en compte au moment où l'exploitant du moteur de recherche examine la demande de déréférencement ; la dernière hypothèse prévoyant le cas où le moteur de recherche n'a pas à tenir compte du fait que la demande de déréférencement porte sur des données dont la publication est illicite.

La troisième sous-question concerne l'hypothèse de la publication sur des pages web de données litigieuses dont le traitement n'entre pas dans le champ d'application territorial de la directive du 24 octobre 1995, et donc dans les lois de transposition de cette directive. Une telle hypothèse peut poser des difficultés de mise en œuvre lorsque, conformément aux deux premiers cas susmentionnés, l'exploitant du moteur de recherche doit ou peut tenir compte, lors de l'examen du droit au déréférencement, du fait que la publication est issue d'un traitement de données exclu du champ d'application territorial de la directive du 24 octobre 1995. Cela revient à se demander comment les exploitants des moteurs de recherche pourraient-ils apprécier la licéité de la publication des données litigieuses issue d'un traitement de données ne relevant pas du champ d'application de la directive de 1995. Cette situation vise par exemple le cas de résultats de moteurs de recherche obtenus à partir de publication figurant sur des sites Internet non européens, par exemple sur des journaux dont les pages web sont hébergées sur les continents américain, asiatique, africain ou en Océanie, mais aussi en Europe en dehors de l'Union européenne. Dans une telle hypothèse, le Conseil d'État se pose la question de l'appréciation de la licéité de la publication des données litigieuses. En effet, les législations étant différentes, une même information peut être considérée comme illicite par le droit de l'Union européenne, mais licite en dehors. Par exemple, une publication d'informations qualifiée d'illicite par le droit de l'Union peut être considérée comme une information licite par le droit des États-Unis, car relevant du droit à la liberté d'expression et du premier amendement. Aussi, le Conseil d'État demande-t-il à la Cour de Justice de l'Union européenne « comment apprécier la licéité de la publication des données litigieuses sur des pages web qui proviennent de traitements n'entrant pas dans le champ d'application territorial de la directive du 24 octobre 1995 et, par suite, des législations nationales la mettant en œuvre ».

En quatrième lieu, le Conseil d'État s'intéresse aux obligations pesant sur les exploitants des moteurs de recherche à l'égard des demandes de déréférencement portant sur des données à caractère personnel devenues « incomplètes », « inexactes » ou « non actualisées ».

Il s'agit de savoir si dans de telles circonstances, la directive du 24 octobre 1995 impose à l'exploitant du moteur de recherche d'accéder à la demande de déréférencement. L'exercice d'un droit au déréférencement dans une telle hypothèse est d'une manière générale compréhensible, car une publication de données à caractère personnel incomplète, inexacte ou non actualisée est susceptible de porter préjudice à la personne concernée. Les enjeux sont encore plus importants lorsque les informations en question sont relatives à des procédures judiciaires, des infractions ou des condamnations pénales. Aussi, le Conseil d'État formule-t-il une question plus spécifique dans ces trois hypothèses.

D'une part, il s'agit de savoir si un exploitant de moteur de recherche est tenu de déréférencer des liens menant vers des informations portant sur une procédure judiciaire dont le demandeur a démontré qu'elles ne correspondent plus à la réalité de sa situation.

D'autre part, le Conseil d'État demande à la Cour de justice de l'Union européenne si les données relatives à la mise en examen d'un individu ou relatant un procès entrent dans le champ d'application des données relatives aux infractions et condamnations pénales dont le traitement est en strictement encadré par le paragraphe 5 de l'article 8 de la directive puisque le traitement ne peut. Cette disposition prévoit en effet que :

« Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. »⁴³

Dans le prolongement de cette question, le juge français demande au juge de l'Union européenne si les pages web contenant des données faisant état des condamnations ou des procédures judiciaires visant une personne physique entrent dans le champ d'application du paragraphe 5 de l'article 8 de la directive du 24 octobre 1995.

À travers ces questions, il s'agit de savoir si l'exploitant d'un moteur de recherche est autorisé à accéder au droit de déréférencement concernant les données relatives à la mise en examen, aux infractions et condamnations ou encore aux procédures judiciaires d'une personne concernée. En effet, une personne ayant fait l'objet

⁴³ Cf. Article 8, § 5, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995

d'une condamnation peut avoir intérêt à ce que cette information ne soit plus accessible aux internautes. Déréférencer les liens renvoyant vers des publications faisant état de ces condamnations ne supprime certes pas l'information sur le site Internet du journal ayant publié l'information, mais il rend plus difficile l'accès à cette information puisque l'internaute ne pourra pas exercer une recherche générale à partir d'un moteur de recherche, mais devra spécifiquement se rendre sur le site Internet de chaque journal pour avoir accès à l'information. On comprend donc l'intérêt de la question posée par le Conseil d'État.

B) L'avènement de l'âge de raison : la complexité des défis issus de l'an IV de la révolution numérique

L'an IV de la révolution numérique fait naître de nouveaux défis juridiques, parmi lesquels figurent ceux liés à la mise en œuvre de la blockchain et de l'intelligence artificielle. Cependant, avant de traiter de ces deux sujets, il convient de mentionner la mise en œuvre du droit à la libre détermination de ses données personnelles, nouveau droit créé en France en 2016.

En effet, la loi du 6 janvier 1978 avait posé dès l'origine comme principe celui de mettre l'informatique au service du citoyen, ajoutant qu'elle ne doit porter atteinte « ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »⁴⁴. Plus de 40 ans après, l'affirmation de cette exigence demeure et n'a pas été remise en cause et a même été renforcée en 2016 lorsque le législateur a ajouté le droit à la libre détermination de ses données personnelles, c'est-à-dire, le droit de toute personne à disposer du droit de décider et de contrôler les usages faits de ses données à caractère personnel dans les conditions fixées par la loi du 6 janvier 1978⁴⁵.

Tout laisse à penser cependant que la mise en œuvre de ce nouveau droit ne sera pas sans poser des interrogations quant à l'interprétation et/ou la mise en œuvre des nouveaux droits, dont figure celui du droit de disposer de ses données à caractère personnel après sa mort⁴⁶. Ce droit permet à une personne physique d'arrêter des directives concernant la conservation, l'effacement et à la communication de ses données à caractère personnel après son décès. Le législateur a établi une distinction entre les directives qualifiées de générales et celles qui sont particulières. Les directives générales portent sur l'ensemble des données à caractère personnel et constituent des instructions générales enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés. Au contraire, les directives particulières sont destinées aux

⁴⁴ Cf. la version initiale de l'article 1^{er} de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⁴⁵ Cf. le second alinéa de l'article 1^{er} de la loi du 6 janvier 1978, ajouté par l'article 54 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

⁴⁶ Cf. l'article 40-1 de la loi du 6 janvier 1978. Voir aussi le 6) de l'article 32 de la loi du 6 janvier 1988 s'agissant du droit à l'information relatif à ce droit.

responsables de traitement qui sont amenés à suivre les instructions communiquées de son vivant par la personne concernée pour la mise en œuvre du traitement de ses données à caractère personnel après sa mort. Or, qu'en sera-t-il de l'effectivité de ce droit lorsqu'il s'agira de mettre en œuvre des directives spécifiques, par exemple pour une personne n'ayant pas d'héritier ou encore en cas de désaccord entre héritiers, hypothèse explicitement prévue par la loi du 6 janvier 1978 qui prévoit que de tels désaccords sont portés devant le tribunal de grande instance compétent⁴⁷?

Un deuxième défi juridique à venir est celui de la régulation de la blockchain, même si les premières bases commencent à être posées avec l'adoption des premières législations, mais aussi à travers les premières décisions de justice rendues en la matière.

En ce sens, il faut mentionner par exemple, en France, la décision du Conseil d'État du 26 avril 2018 concernant la fiscalité des cryptoactifs⁴⁸. Le juge administratif français a posé le principe que les produits que les particuliers tirent de la cession de « bitcoins » doivent être imposés en principe dans la catégorie des plus-values de bien meubles.

Cependant, il a également considéré que certaines circonstances propres à l'opération de cession peuvent impliquer d'imposer les gains issus de la cession de bitcoins dans d'autres catégories de revenus.

Tel est le cas lorsqu'un particulier a obtenu des bitcoins dans le cadre d'un minage. Dans une telle hypothèse, le gain issu de la cession des bitcoins s'analyse comme la contrepartie de la participation du contribuable à la création ou au fonctionnement de ce système d'unité de compte virtuelle. Les gains ne résultant pas d'une opération de placement, mais d'un véritable travail, celui du minage des bitcoins, ils doivent être imposés dans la catégorie des bénéfices non commerciaux.

Au contraire, les gains « provenant de la cession, à titre habituel, d'unités de "bitcoin" acquises en vue de leur revente, y compris lorsque la cession prend la forme d'un échange contre un autre bien meuble, dans des conditions caractérisant l'exercice d'une profession commerciale, sont imposables dans la catégorie des bénéfices industriels et commerciaux. »⁴⁹

Si la décision rendue par le Conseil d'État peut se comprendre, elle n'en reste pas moins complexe et illustre la nature des interrogations à venir dans la mise en œuvre de la blockchain, la décision du 26 avril 2018 n'étant qu'un exemple parmi d'autres des interrogations juridiques que pose la mise en œuvre de la blockchain.

Enfin, la société est amenée à répondre à un troisième défi juridique à travers le déploiement de l'intelligence artificielle.

Depuis plusieurs siècles, l'homme est considéré comme l'espèce dominante sur terre comme le furent les dinosaures en leur temps

⁴⁷ Cf. le III de l'article 40-1 de la loi du 6 janvier 1978.

⁴⁸ CE, 26 AVRIL 2018, M. G... ET AUTRES, N^{os} 417809, 418030, 418031, 418032, 418033.

⁴⁹ CE, 26 avril 2018, M. G... et autres, n^{os} 417809, 418030, 418031, 418032, 418033.

avant leur extinction il y a 66 millions d'années⁵⁰. Cependant, au regard de l'évolution rapide que connaissent actuellement les nouvelles technologies et en particulier l'intelligence artificielle, certains se demandent si demain, et pour la première fois, l'homme ne pourrait pas être en concurrence avec une espèce dominante. Tel serait le cas si des chercheurs parvenaient à développer une intelligence artificielle auto-apprenante et auto-évolutive. Elon Musk a même déclaré en 2014 que l'intelligence artificielle était la plus grande menace qui pesait sur la survie de l'espèce humaine⁵¹ appelant par conséquent à sa régulation⁵², quand Stephen Hawking déclarait de son côté la même année à la BBC que le développement d'une intelligence artificielle intégrale pourrait sonner le glas de l'espèce humaine. Selon lui, les humains étant limités par la lenteur de l'évolution biologique, ils ne pourraient pas rivaliser avec cette nouvelle espèce et seraient donc remplacés par cette dernière⁵³.

Sans aller jusqu'à envisager cette hypothèse où l'homme disparaîtrait au profit d'une intelligence artificielle, il n'en demeure pas moins que le scénario d'une intelligence auto-apprenante et autonome paraît pour l'instant de la pure fiction. Cependant, il est possible de penser qu'en d'autres temps, par exemple à l'époque de Gutenberg, auraient paru tout aussi irréalistes les propos de celui qui aurait affirmé qu'un jour un être humain irait sur la lune ou sur Mars, qu'il serait possible d'envoyer des informations en moins d'une seconde à l'autre bout de la Terre ou que grâce à des hologrammes, il serait possible d'être présent à deux endroits différents de la terre en même temps.

Cette comparaison avec Gutenberg n'est pas anodine. En effet, certains considèrent que le développement de l'Internet et de l'intelligence artificielle est une révolution aussi importante que celle de l'invention de l'imprimerie. La difficulté à prévoir les évolutions futures rend plus que jamais nécessaire de réfléchir dès aujourd'hui à la régulation juridique de l'intelligence artificielle.

Certains pays comme la France ont déjà commencé à apporter des réponses à ce sujet, en ayant la volonté d'encadrer l'utilisation des algorithmes. Par exemple, la réforme de l'entrée dans l'enseignement supérieur français a été l'occasion d'apporter les premières réponses, en laissant ouvertes de nouvelles interrogations. Ainsi, la CADA a considéré dans une décision du 23 juin 2016 que les « fichiers informatiques constituant le code

⁵⁰ Cf. notamment F. Broswimmer (traduction de Thierry Vanès), *Écocide : Une brève histoire de l'extinction en masse des espèces*, Parangon, 2003.

⁵¹ Propos tenus en 2014 par Elon Musk au Massachusetts Institute of Technology (MIT) lors d'une interview au

AeroAstro Centennial Symposium, cités par S. Gibbs, « Elon Musk: artificial intelligence is our biggest existential threat », *The Guardian*, 27 octobre 2014, dernière modification le 21 février 2017, accessible à :

<https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat>.

⁵² Ibidem.

⁵³ R. CELLAN-JONES, « Stephen Hawking warns artificial intelligence could end mankind », BBC, 2 décembre 2014, accessible à : <https://www.bbc.com/news/technology-30290540>.

source ou algorithme sollicité» étaient des documents administratifs communicables⁵⁴, jurisprudence qui sera consacrée quelques mois plus tard au plan textuel par le code des relations entre le public et l'administration qui range les codes sources au sein des documents administratifs⁵⁵.

De son côté, la CNIL a rappelé dans une décision du 30 août 2017⁵⁶ que, conformément à l'article 10 de la loi du 6 janvier 1978, « 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. »⁵⁷

Mais ces décisions et consécutions textuelles ne suppriment cependant pas l'ensemble des interrogations qui peuvent naître des évolutions technologiques, d'autant que le droit n'est pas toujours stable. Ainsi, conscient des difficultés qu'il y aurait à faire respecter une disposition prévoyant qu'il ne serait pas possible de prendre une décision entraînant des effets juridiques à l'égard d'une personne sur le seul fondement d'un algorithme, le législateur a réécrit en 2018 l'article 10 de la loi du 6 janvier 1978 pour prévoir plusieurs exceptions à cette interdiction.

Désormais, l'article 10 de la loi du 6 janvier 1978 dans sa version modifiée par la loi du 20 juin 2018 dispose :

« 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.

Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception :

1° Des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, sous les réserves mentionnées au 3 du même article 22 et à condition que les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre soient communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande ;

2° Des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre Ier du titre Ier du livre IV du code des relations entre le public et l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 8 de la présente loi.

⁵⁴ CADA, Avis 20161989 – séance du 23 juin 2016.

⁵⁵ Cf. l'article 300-2 du code des relations entre le public et l'administration.

⁵⁶ 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.

⁵⁷ Deuxième alinéa de l'article 10 de la loi du 6 janvier 1978 dans sa version antérieure à la loi du 20 juin 2018.

Ces décisions comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du code des relations entre le public et l'administration. Pour ces décisions, 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.

Par dérogation au 2° du présent article, aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre Ier du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel. »⁵⁸

Les brèches ainsi ouvertes par la reconnaissance, certes encadrée, d'exceptions à l'impossibilité de prendre une décision produisant des effets juridiques à l'égard d'une personne sur le seul fondement d'un traitement automatisé des données à caractère personnel suscitent des interrogations quant aux relations qui peuvent s'établir entre l'individu et la machine. En effet, il s'agit de se demander si une décision doit toujours résulter d'une volonté humaine ou si elle peut être le fruit d'un processus entièrement automatisé. Dans cette hypothèse, dans quels cas acceptons-nous de nous en remettre à une décision de la machine plutôt qu'à une décision humaine ?

Ces interrogations conduisent à réfléchir plus largement à l'avènement de l'interaction homme-machine théorisée par Joseph Licklider dans son article « *Man-Computer Symbiosis* »⁵⁹ publié en 1960.

Les progrès technologiques que nous connaissons actuellement rendent plus que jamais nécessaire de réfléchir au régime de responsabilité de l'intelligence artificielle. Aujourd'hui, se pose déjà la question de savoir qui est responsable en cas de litige d'un véhicule autonome piloté par une intelligence artificielle. Demain, la défaillance pourrait être plus difficile à établir s'il ne s'agit pas de juger de la responsabilité d'une intelligence artificielle autonome, comme celle d'un véhicule autonome, mais plutôt de celle d'un homme augmenté. Par exemple, si à l'avenir la recherche permettait à des personnes non voyantes de retrouver la vue grâce à des « yeux numériques », et que cette personne commettait un accident après avoir brûlé un feu rouge, il ne sera pas évident de trancher le litige si le conducteur avance comme argument que son « œil numérique » a été défectueux alors que dans le même temps, le fabricant de « l'œil numérique » rejette la faute sur le programmeur, qui lui-même considère que le conducteur aurait dû s'arrêter de conduire immédiatement après avoir constaté une

⁵⁸ Article 10 de la loi du 6 janvier 1978 dans sa version modifiée par la loi du 20 juin 2018.

⁵⁹ J. Licklider, *Man-Computer Symbiosis*, 1RE Transactions on Human Factors in Electronics, volume HFE-1, mars 1960, pp. 4-11.

défaillance de son œil, et non continuer à conduire pendant 2 minutes, provoquant ainsi l'accident.

Les mêmes personnes pourront aussi reprocher au fabricant de la voiture autonome, mais aussi au programmeur de l'intelligence artificielle, de ne pas avoir su anticiper la perte de contrôle du véhicule. Si en outre «l'œil numérique» est connecté à la voiture autonome et que des informations ont mal été transmises entre l'œil et la voiture en raison de la défaillance du réseau wifi ou d'un problème de fracture numérique qui n'avait pas été mentionné, il est alors possible d'entrevoir toute la difficulté qu'il y aurait à juger de tels litiges. En effet, dans une telle hypothèse, il conviendra d'articuler à la fois la question des objets connectés, celle de la fracture numérique, celle de la responsabilité du constructeur et du programmeur de «l'œil numérique», celle de la responsabilité du constructeur et du programmeur du véhicule autonome, celle de la responsabilité du conducteur équipé de l'œil numérique, et le cas échéant, celle de la responsabilité d'un piéton imprudent, etc.

Pour mieux réguler juridiquement les risques liés au développement de l'intelligence artificielle, il est donc nécessaire d'entamer une réflexion d'ensemble portant sur le régime de responsabilité qui peut en résulter. Il importe d'y procéder dans un langage clair afin de tenter de mettre ces évolutions et leurs conséquences juridiques à la portée de tous. Une telle démarche permettrait de tenter d'atténuer la complexité inhérente à la régulation juridique des avancées engendrées par les nouvelles technologies.

Cet enjeu revêt une importance déterminante, car appréhender la complexité de la régulation juridique des avancées technologiques permettrait par exemple de trancher les litiges correspondants et donc de contribuer au bon fonctionnement de la justice. Il reste cependant qu'une telle complexité se développe à une vitesse croissante.