La sauvegarde des libertés individuelles face à l'utilisation croissante de l'intelligence artificielle

Jim LAPIN

Édition électronique

URL : <http://journals.openedition.org/ctd/3192>

DOI : 10.4000/ctd.3192

ISSN : 2491-1437

Éditeur

Chaire Unesco Pratiques émergentes en technologies et communication pour le développement

Édition imprimée

ISBN : 2491-1437

Référence électronique

Jim LAPIN, « La sauvegarde des libertés individuelles face à l'utilisation croissante de l'intelligence artificielle », *Communication, technologies et développement* [En ligne], 8 | 2020, mis en ligne le 30 juin 2020, consulté le 28 mars 2021. URL : <http://journals.openedition.org/ctd/3192> ; DOI : <https://doi.org/10.4000/ctd.3192>

Ce document a été généré automatiquement le 28 mars 2021.

Communication, technologies et développement

La sauvegarde des libertés individuelles face à l'utilisation croissante de l'intelligence artificielle

Jim LAPIN

- 1 L'intelligence artificielle correspond aux technologies capables de traiter des sources hybrides et notamment des données non structurées. Elle a connu un réel essor ces dernières années. Pour la première fois peut-être, une activité immatérielle devient indépendante de l'Homme. Il ne s'agit plus de la mise en œuvre d'un programme par la volonté et sous le contrôle de l'être humain, mais du développement d'une forme de pensée qui, bien que conçue par l'Homme, tend dans une certaine mesure à s'en émanciper. Ainsi, des tâches complexes sont déléguées à des procédés technologiques de plus en plus autonomes. Elle est cependant susceptible de porter atteinte aux libertés individuelles. Au rang de ces libertés définies par les textes fondamentaux et par les hautes juridictions, on trouve la liberté de circulation, la liberté d'opinion, la liberté de culte, la liberté de conscience, la liberté économique, la liberté contractuelle¹, qui reposent sur l'autonomie de la volonté, et le droit à la vie privée². Cette dernière est étroitement liée au domicile, à la correspondance, aux relations intimes, dont il faut préserver le secret.
- 2 L'irruption dans nos vies de l'intelligence artificielle et son expansion font l'objet d'une attention particulière de la part des pouvoirs publics depuis que nous avons connu des exemples d'utilisation qui ont attiré l'attention et inquiété les citoyens. En effet ces pratiques ont porté au pilori les volontés individuelles et mis en cause un principe fondamental de notre ordre juridique : la garantie des libertés individuelles. N'ouvre-t-on pas les portes trop grandes à une confiance excessive dans la machine, poussant l'individu à abandonner ses capacités de jugement ? Il s'agirait d'adapter la réglementation en vigueur en définissant une nouvelle génération de garanties et de droits fondamentaux spécifique au numérique.

- 3 Ainsi, les pouvoirs publics se trouvent dans l'obligation d'adopter des règles juridiques qui permettent l'épanouissement des libertés individuelles face aux risques que représente l'intelligence artificielle. Le droit se devait d'évoluer vers un cadre juridique approprié qui permet à l'être humain de conserver sa capacité de jugement et son autonomie. Cependant, la régulation des algorithmes³ reste difficile en raison de l'évolutivité de la technologie et du caractère confidentiel et concurrentiel des développements.
- 4 Ensuite, afin de renforcer la protection juridique des utilisateurs, un certain nombre de réflexions ont été menées, notamment par la Commission nationale de l'informatique et des libertés (Cnil), dont le but est de faire en sorte que la technologie soit véritablement au service de l'Homme. Cependant, ne perdons pas de vue que si la France a raté le coche avec les moteurs de recherches (sous emprises des États-Unis et de la Chine), c'est peut-être parce qu'elle est culturellement rétive à toute invention mettant en jeu les droits fondamentaux de citoyens.
- 5 Le cadre réglementaire actuel est composé essentiellement de la loi du n° 2016-1321 du 7 octobre 2016 pour une République numérique⁴ et de la loi relative à la protection des données personnelles du 20 juin 2018 qui adapte la loi "Informatique et libertés" du 6 janvier 1978 au "paquet européen de protection des données". Ce paquet comprend le règlement général sur la protection des données (RGPD) du 27 avril 2016⁵ directement applicable dans tous les pays européens au 25 mai 2018 ainsi qu'une directive datée du même jour sur les fichiers en matière pénale, dite directive "police"⁶. Le non-respect de ces textes est assorti de sanctions infligées par la Cnil. Enfin, deux lois du 22 décembre 2018 relatives à la lutte contre la manipulation de l'information⁷ définissent un dispositif de protection de la liberté d'opinion face aux fausses informations diffusées sur Internet.
- 6 Il s'agira pour nous dans un premier temps d'analyser les enjeux de la protection des libertés individuelles face à l'intelligence artificielle (I) avant de constater que la réglementation française actuelle reste insuffisante pour protéger les libertés individuelles (II).

I/ Les enjeux de la protection des libertés individuelles face à l'intelligence artificielle

- 7 Les enjeux de la protection des libertés individuelles se mesurent avant tout au travers de la valeur juridique de ces principes (A). En effet, les libertés individuelles sont des libertés fondamentales garanties par la Constitution française et par la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. Ensuite ces enjeux se mesurent au regard des risques de perte de l'autonomie de la volonté (B) et de failles dans le respect de la vie privée (C).

A/ Les libertés individuelles : des libertés fondamentales

- 8 Une des conceptions des libertés individuelles trouve sa source dans l'individualisme libéral qui caractérise aujourd'hui notre société. Il repose sur deux principes : d'une part la « liberté individuelle » proprement dite, ou le droit de se préoccuper en premier lieu de la condition des individus de la société avant la condition de la société elle-

même et d'autre part l'autonomie morale qui exige que chaque individu mène une réflexion individuelle sans que ses opinions soient dictées par un quelconque groupe social.

- 9 Aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : « *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* ».
- 10 Aussi, l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales⁸ dispose que

« toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».
- 11 La Cour européenne des droits de l'Homme pousse très loin la protection de la sphère individuelle en lui donnant une portée maximale à travers la notion d'autonomie personnelle. Elle considère ainsi que « la faculté par chacun de mener sa vie comme il l'entend peut également inclure la possibilité de s'adonner à des activités perçues comme étant d'une nature physiquement ou moralement dommageable ou dangereuse pour sa personne. En d'autres termes, la notion d'autonomie personnelle peut s'entendre au sens du droit d'opérer des choix concernant son propre corps »⁹. Les juges constitutionnels européens et les organes de la Convention européenne des droits de l'homme ont ainsi fait émerger la notion d'autonomie personnelle au sein de l'ordre juridique, et fait de lui progressivement un droit fondamental¹⁰. Toute personne peut non seulement décider sans entrave de ses propres choix pour la construction de sa personnalité, mais aussi de revendiquer ces choix afin qu'ils soient reconnus et protégés juridiquement dans le cadre de ses relations à autrui.
- 12 Cependant, des motifs d'intérêt général peuvent justifier la restriction par les pouvoirs publics d'un certain nombre de libertés. Il incombe au législateur de concilier le respect des libertés individuelles avec d'autres exigences, comme la sauvegarde de l'ordre public, la recherche des auteurs d'infractions et la préservation du bien-être économique et social. Ainsi, le Conseil constitutionnel a souvent déclaré des dispositions législatives restreignant des libertés comme conformes sans réserve ou comme conformes avec réserves en raison de garanties qu'il suppose en adéquation avec l'objectif poursuivi¹¹. Il procède ainsi à un contrôle de proportionnalité¹². La mesure doit ainsi répondre aux exigences d'adéquation, de nécessité et de proportionnalité au sens strict¹³.
- 13 Aussi, « conformément à la théorie générale des libertés, la limitation du pouvoir ne consiste pas seulement à l'abstention de porter atteinte à une liberté ; elle se traduit aussi par l'obligation pour le pouvoir de protéger cette liberté et de la rendre effective notamment pour ce qui concerne les droits de créances »¹⁴. Le pouvoir doit ainsi protéger les libertés y compris dans les relations entre personnes. De la même manière, le Conseil constitutionnel considère que le législateur ne saurait modifier ou abroger des dispositions législatives touchant une liberté comme la liberté de communication qu'« en vue d'en rendre l'exercice plus effectif »¹⁵.

- 14 En matière plus spécifiquement de traitement des données à caractère personnel, la jurisprudence du Conseil constitutionnel laisse au législateur une grande liberté d'appréciation tout en protégeant les libertés individuelles. Le Conseil constitutionnel a jugé qu'il appartient au législateur de fixer les règles générales applicables aux fichiers nominatifs et aux traitements de données personnelles. Celles-ci doivent s'attacher à respecter la vie privée qui constitue un droit constitutionnel¹⁶. Le Conseil a par exemple imposé que soit observée une particulière vigilance dans la collecte et le traitement de données à caractère personnel de nature médicale¹⁷. Ainsi, le Conseil admet sous certaines réserves, les utilisations multiples d'un fichier. Dans sa décision n° 2003-467 DC du 13 mars 2003 sur la loi pour la sécurité intérieure, il a considéré qu'aucune norme constitutionnelle ne s'opposait par principe à l'utilisation à des fins administratives de données nominatives automatisées recueillies dans le cadre d'activités de police judiciaire. Toutefois, elle « méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées »¹⁸. C'est aux conditions dans lesquelles il est procédé à la double utilisation d'un fichier que le Conseil constitutionnel et, par voie de conséquence, le législateur ou le pouvoir réglementaire doivent être attentifs. Par ailleurs, le Conseil n'admet l'interconnexion de fichiers ayant à l'origine des finalités distinctes que dans un but de bonne administration et de contrôle.
- 15 Enfin, le Conseil de l'Europe a estimé que l'article 8 de la Convention européenne des droits de l'Homme précité, contenait un certain nombre de limites et d'inconvénients au regard du développement nouveau de l'informatique et des technologies de l'information. La portée du terme « vie privée » est insuffisamment définie et la prise en considération de la protection contre l'ingérence de personnes qui ne sont pas une autorité publique est inexistante. C'est ainsi qu'a été adoptée en 1981 une convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, appelée convention 108¹⁹, qui a été ratifiée par 31 États membres du Conseil de l'Europe, dont tous les États membres de l'Union européenne. Aux termes de son article 1^{er}, la convention a pour objectif d'assurer la protection du respect des droits et des libertés fondamentaux de toute personne physique, et notamment de son droit à la vie privée, à l'égard du traitement des données à caractère personnel la concernant.
- 16 La convention 108 ne pouvait pas être appliquée directement par les États contractants dont l'effectivité passait par l'adoption par les États signataires de dispositions de droit interne conformes à ses principes fondamentaux. La Cour européenne des droits de l'homme a estimé dans un avis de 1997 (affaire Z c. Finlande) que la protection des données à caractère personnel jouait un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la CEDH et précisé par la convention 108 à laquelle elle s'est référée. Ainsi, le comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a mené une réflexion sur l'application de la convention 108 au mécanisme de profilage par le biais du *Data Mining*²⁰ qui est une composante essentielle des technologies *Big Data*²¹.
- 17 La valeur juridique des libertés individuelles et leur portée étant ainsi exposées, il convient d'étudier le risque de perte de l'autonomie de la volonté que le développement de l'intelligence artificielle fait courir aux individus.

B/ La perte de l'autonomie de la volonté

- 18 L'intelligence artificielle fait courir le risque d'une profonde transformation sociétale où la société humaine serait remplacée par une société mécanisée. Il n'y aurait ainsi, plus de place pour l'émotivité, pour la réflexion et pour l'intimité²². On laisse l'individu penser qu'on le décharge d'un poids : celui de réfléchir à un choix. Il n'y aurait plus de liberté de réfléchir, ce qui est l'essence même de l'Homme. On pourrait ainsi compléter cette citation de René Descartes sur la conscience : « Je pense donc je suis »²³, *je ne pense pas, donc je ne suis pas ?*
- 19 La spécificité de l'être humain dans sa capacité de réflexion et de détermination de ses choix est questionnée par l'autonomie grandissante des machines ainsi que par l'apparition de formes d'hybridation entre humains et machines. En effet, les machines « permettent une analyse de plus en plus complète et intime de nos modes de vie, de nos besoins, de nos aspirations. Alors que la finalité de la machine était initialement de gérer des tâches, les systèmes d'intelligence artificielle assurent désormais une fonction de « rétroaction ». Cette fonction développe tout d'abord des capacités interprétatives permettant aux systèmes d'interpréter les situations à haute vitesse. Elle développe ensuite des capacités suggestives permettant aux machines de suggérer des actes. Le modèle de l'économie de la donnée se nourrit par conséquent de la collecte d'informations sur nos vies, ce qui aboutit à leur marchandisation intégrale. Les capacités interprétatives et suggestives génèrent un « accompagnement algorithmique de la vie à des fins prioritairement commerciales »²⁴. Enfin, la « rétroaction » permet une capacité autodécisionnelle en permettant à des artefacts²⁵ de prendre des décisions à la place de l'homme, comme pour le *trading* à haute fréquence qui décide d'achats ou de ventes à des vitesses très supérieures à celles des capacités cognitives humaines »²⁶.
- 20 L'intelligence artificielle censée guider l'action de l'Homme peut au final lui dicter ses choix. On se retrouve face à une tendance à punir et à juger avant même que les individus n'aient agi, sur la base de la simple présomption de ce qu'ils auraient pu faire²⁷. Celui-ci se retrouve ainsi bafoué dans son intégrité et sa dignité. Ceux qui exploitent les données du *Big Data* peuvent aussi avoir tendance à se focaliser sur les résultats attendus de cette exploitation, sans tenir compte de leurs limites. L'autonomie humaine serait en train de s'amoinrir face à l'intelligence artificielle, avec la délégation croissante de tâches, de raisonnements ou de décisions de plus en plus critiques à des machines. C'est la raison pour laquelle l'utilisation de l'intelligence artificielle doit être encadrée et accompagnée.
- 21 En effet, le choix final dans un processus décisionnel faisant appel soit à la réflexion, soit aux réflexes, ou aux deux à la fois, doit revenir à l'individu. Les entreprises sont visées, mais aussi les États qui sont eux aussi susceptibles de commettre des abus dans l'utilisation de l'intelligence artificielle..
- 22 Il convient cependant de relativiser ces risques. En effet, l'être humain étant libéré d'une partie des tâches qui le mobilisaient pourra se concentrer sur d'autres activités et tâches que l'intelligence artificielle ne pourra pas faire pour lui. Car l'être humain n'est pas réduit uniquement à son intelligence, mais fait preuve aussi de sensibilité, d'émotion, et de passions qui le font. Ce sont ces qualités qui lui permettent d'explorer son univers²⁸.

- 23 Il convient malgré tout d'anticiper le fait que seule l'intelligence artificielle sera à même de lutter contre les abus de l'intelligence artificielle. Le cadre réglementaire actuel, bien qu'encourageant, ne permet pas suffisamment de garantir la pleine expression de l'autonomie de la volonté, ni d'ailleurs de protéger le respect de la vie privée qui constitue un autre risque que nous pouvons identifier.

C/ Les risques de failles dans le respect de la vie privée

- 24 L'individu doit pouvoir s'épanouir dans la sphère intime, à l'abri du regard de l'État et de la société. Le développement des techniques, de la science, de l'informatique, de la presse, de l'Internet et des moyens de communication menace chaque jour davantage cet épanouissement.
- 25 La protection des données personnelles cristallise des enjeux importants et ambivalents, qui trouvent à s'illustrer dans des questions concrètes et d'actualité, tant sur le plan interne qu'international. Cette question est très sensible dans le contexte actuel du développement sans limites de la capacité de traiter des données personnelles en toujours plus grand nombre, qui touche l'intimité de la personne. On assiste par ailleurs à un affaiblissement de l'État dans le traitement de cette question. Cette tendance à l'accroissement quantitatif et qualitatif des possibilités techniques de traitement des données personnelles a atteint un seuil considéré comme critique.
- 26 Elle trouve tout d'abord à s'illustrer dans les progrès constants de la biométrie qui a permis une intrusion croissante dans les corps des individus, et aujourd'hui s'apprête à investir le champ de la psyché²⁹ avec le scanner et l'IRM³⁰. Les débats autour de la création d'un titre d'identité électronique, éventuellement obligatoire, ont fait ressurgir les craintes à propos de la constitution d'un fichier des Français. La création d'une base de données biométriques reliée à une base de données d'identité pour assurer l'unicité de la délivrance et du renouvellement des titres d'identité exige des précautions importantes. Les fonctions d'identification d'un tel fichier permettent l'utilisation des données pour d'autres fins que celle pour laquelle elles ont été collectées. En somme, créer un fichier reviendrait à mettre le doigt dans un engrenage³¹.
- 27 Ensuite, l'utilisation d'Internet implique nécessairement qu'il y ait de l'échange et des traitements de données personnelles. Ce processus ne se réalise pas à l'initiative d'une personne physique ou morale. Il implique nécessairement la bonne marche technique du service³². Il en va ainsi notamment des moteurs de recherche³³, de l'adresse IP (*Internet Protocol*) des ordinateurs, des *cookies* et des fichiers *logs*³⁴. Ainsi, les nécessités techniques aboutissent à la mise en place par principe des traitements de données personnelles plus ou moins visibles par l'internaute pour toute opération effectuée sur Internet. Une telle opération sur ce réseau se trouve ainsi faire l'objet de traces identifiantes. Ce procédé de traçabilité et de renseignement est, dans le monde réel, caractéristique d'un régime totalitaire selon André Lucas, Jean Deveze et Jean Frayssinet³⁵.
- 28 La prochaine étape technologique de diffusion d'outils miniaturisés informatisés de traitement et de communication de données jusque dans notre quotidien, connue comme l'« internet des objets »³⁶, ne va faire qu'amplifier cette tendance en étendant ce qui existe aujourd'hui dans la sphère du virtuel à la sphère du réel. En effet, comme le fait remarquer à juste titre Guillaume Desgens-Pasanau, celui qui souhaiterait se

soustraire de la sphère virtuelle pour protéger les éléments de son intimité, se placerait en dehors de la vie sociale³⁷. Or on est bien obligé de constater que ces évolutions technologiques augmentent par principe, fortement les risques d'atteintes à la vie privée. Ces risques sont donc inhérents à l'usage de telles technologies qui envahissent notre quotidien. Se pose alors la question de l'efficacité des instruments relatifs aux données personnelles pour protéger la vie privée de la personne fichée³⁸. Ce qui nous conduit à explorer le cadre réglementaire permettant de protéger les libertés individuelles face à l'intelligence artificielle.

II/ Le cadre réglementaire pour protéger les libertés individuelles face à l'intelligence artificielle et ses limites

- 29 La réglementation de la protection des Libertés individuelles face à l'utilisation des technologies de communication n'est pas tout à fait nouvelle, car la loi informatique et libertés du 6 janvier 1978 imposait déjà un certain nombre de principes qui ont nécessité un renforcement (A). Il a fallu également renforcer la protection de la liberté d'opinion (B). Par ailleurs, cette utilisation croissante de l'intelligence artificielle a nécessité la consécration d'un principe de vigilance dont l'efficacité reste à prouver (C).

A/ Le renforcement des principes de transparence et de loyauté

- 30 Les problèmes que génèrent l'utilisation du *big data* sont renforcés par le fait que les États eux-mêmes utilisent l'intelligence artificielle pour la mise en place de politiques publiques. Les principes contenus dans la loi informatique et libertés ont été précisés au niveau européen par le règlement général sur la protection des données (RGPD) adopté le 14 avril 2016. Cette réglementation impose entre autres, des obligations de transparence et de loyauté.
- 31 L'exigence de transparence s'est emparée de ce procédé opaque pour toute personne dépourvue de connaissances informatiques : les algorithmes. Ils sont en effet de plus en plus utilisés par l'administration et les entreprises. C'est ainsi que ce procédé permet déterminer si les étudiants peuvent entrer à l'Université à travers de l'Admission post-bac puis de *Parcoursup*. C'est aussi un algorithme qui attribue les postes de maîtres de conférences à partir des priorités qu'ils ont établies sur le site du ministère de l'Enseignement supérieur.
- 32 Tout d'abord, la loi du 7 octobre 2016 pour une République numérique impose une exigence de transparence aux administrations quant aux traitements algorithmiques servant de prendre des décisions individuelles. La loi insère au code des relations entre le public et l'administration (CRPA) une nouvelle disposition aux termes de laquelle une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite informant l'intéressé. Aux termes des nouveaux articles L. 312-1-1 à L. 312-1-4 du CRPA, insérés par la loi précitée, doivent être formés à l'éthique tous les acteurs-maillons de la « chaîne algorithmique » (concepteurs, professionnels, citoyens). Ce principe d'alphabétisation au numérique doit permettre à chaque humain de comprendre les ressorts de la machine. Ainsi, d'une part, les administrations ont l'obligation de publier en ligne les règles définissant les principaux traitements

algorithmiques utilisés dans la réalisation de leurs missions lorsque ces traitements fondent des décisions individuelles. D'autre part, aux termes de l'article L. 311-2-1 du CRPA, elles ont obligation de rendre accessibles les données traitées par les algorithmes fondant une décision individuelle.

- 33 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 demande³⁹. Cependant, la loi pour une République numérique ne précise pas que les algorithmes sont des documents administratifs. On en déduit que l'algorithme ne pourra pas être communiqué sous sa forme brute. Seules pourront être communiquées les caractéristiques du traitement, notamment les objectifs, les finalités et les contraintes du système ainsi qu'un exposé des paramètres, des principales caractéristiques, et des règles générales de l'algorithme. Ceci peut sembler être un obstacle au principe de transparence et donc la préservation de l'opacité. Cependant à notre sens il n'en est rien. La préoccupation du législateur était aussi de préserver les secrets de conception des algorithmes. Ceci principalement lorsque l'algorithme a été élaboré par une entreprise, dans le cadre d'un contrat qui ne transfère pas à l'administration les droits de propriété intellectuelle. Il faut certes faire vivre les principes de transparence, mais non au détriment de la propriété intellectuelle qu'il convient de protéger face à la concurrence internationale⁴⁰.
- 34 Ensuite, au-delà des exigences imposées à l'administration, de manière générale, le RGPD a mis l'accent sur la finalité de la collecte des données, qui est à notre sens, un principe qui vient renforcer l'exigence de transparence. Avant toute collecte et utilisation de données personnelles, le responsable de traitement doit précisément annoncer aux personnes concernées les objectifs de cette collecte des données ou autrement dit ce à quoi elles vont lui servir.
- 35 Ces dispositions législatives répondent ainsi aux préoccupations de Viktor Mayer-Schönberger et de Kenneth Cukier⁴¹ qui ont estimé que « les précisions permises par le traitement des *big data* ne doivent pas être des boîtes noires, elles doivent pouvoir être expliquées ». Il faut donc imposer la transparence face à l'utilisation de ces nombreuses et diverses données. La solution donc à ces préoccupations passe par la formation permettant de déchiffrer et d'expliquer ce qui se passe derrière ces *big data*. Ce rôle pourrait être assuré par des *algorithmistes*, des auditeurs de *big data* en quelque sorte. Schönberger et Cukier s'appuient ainsi sur ce qui s'est produit au début du siècle suite à l'explosion des données financières où les auditeurs et comptables ont été chargés de mettre en place un système de valorisation garantissant un reflet juste et transparent du prix des portefeuilles boursiers, mais moins structurant sur l'économie réelle⁴².
- 36 Afin de veiller au respect du principe de transparence, le législateur a par la même occasion, renforcé le pouvoir de sanction de la Cnil⁴³. C'est ainsi que cette dernière a infligé le 21 janvier 2019, une amende record de 50 millions d'euros à Google, reprochant au géant américain de ne pas informer suffisamment clairement ses utilisateurs sur l'exploitation de leurs données personnelles. Selon la Cnil,
- « Les manquements constatés privent les utilisateurs de garanties fondamentales concernant des traitements pouvant révéler des pans entiers de leur vie privée, car reposant sur un volume considérable de données, une grande variété de services et des possibilités de combinaison de données quasi-illimitées »⁴⁴.
- 37 Face à tous ces enjeux, il était également nécessaire de renforcer le principe de loyauté et de licéité. Ainsi, les données personnelles collectées ne pourront pas être réutilisées

pour une autre finalité que celle prévue initialement. La loi Informatique et Libertés précitée, modifiée par la loi n° 2004-801 du 6 août 2004 transposant la directive 98/46 CE du 24 octobre 1995 disposait déjà que les informations collectées par un système de traitement automatisé de données personnelles, ne pouvaient être utilisées à une autre fin que celle figurant dans la déclaration préalable faite auprès de la Commission nationale de l'informatique et des libertés (Cnil). Ainsi, la Cour de cassation a eu à juger qu'un système de traitement automatisé de données à caractère nominatif qui n'a pas fait l'objet d'une déclaration à la Cnil⁴⁵ ou dont la finalité a été détournée⁴⁶ ne peut pas être opposé aux salariés et constitue un dispositif illicite. Plus, récemment, suite à une requête de l'association UFC-Que Choisir déposée en 2014 contre Google⁴⁷, le Tribunal de Grande Instance de Paris par un jugement du 12 février 2019⁴⁸, déclare abusives et illicites 38 clauses des « conditions d'utilisation » et des « règles de confidentialité » du géant américain. Il a été fait interdiction à ce dernier de collecter et partager les données personnelles de ses utilisateurs sans les avoir informés clairement, de géolocaliser en permanence ses utilisateurs et de modifier volontairement les données personnelles collectées ou les diffuser librement dans des annonces commerciales. Aussi, Google ne peut plus dissuader les utilisateurs de s'opposer aux dépôts systématiques de cookies ni de laisser croire que l'utilisation de ses services entraîne l'acceptation des conditions d'utilisation et règles de confidentialité.

- 38 Cependant, en raison de l'évolution technologique et de l'utilisation d'algorithmes de plus en plus complexe par les entreprises du net, les pouvoirs publics ont dû procéder à l'adaptation du principe de loyauté. Ainsi, les algorithmes utilisés en intelligence artificielle ne doivent trahir ni l'utilisateur ni la communauté. Il s'agit de favoriser une utilisation qui permet à l'algorithme « de dire ce qu'il fait et de faire ce qu'il dit »⁴⁹. Le RGPD adopté rappelons-le en avril 2016, après donc la plainte déposée contre Google, dispose que le responsable de traitement doit informer la personne concernée de « l'existence d'une prise de décision automatisée, y compris un profilage (...) et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée » (art. 13-2-f). À partir de cette information est offert à la personne concernée un droit d'opposition. Deux exceptions sont néanmoins prévues à cette faculté : lorsque cela est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ou si le consentement explicite de la personne a été recueilli. Ce texte impose aux grandes forces économiques du *big data* des obligations qui consistent à éviter qu'ils n'interfèrent de manière excessive dans la vie privée des citoyens.
- 39 Le principe de loyauté peut s'appliquer par exemple dans le cadre du débat démocratique afin de lutter contre la segmentation du corps politique par le ciblage de l'information. Il peut également trouver à s'appliquer à l'utilisation d'algorithmes de police prédictive⁵⁰ sur des communautés ou quartiers entiers⁵¹.
- 40 Enfin, la loi du 7 octobre 2016 pour une République numérique précitée élargit l'exigence de loyauté des plateformes en ligne⁵² et l'information des consommateurs, au-delà des seules plateformes de mise en relation⁵³. Tout opérateur de plateforme en ligne est tenu désormais de délivrer au consommateur une information loyale, claire et transparente sur les conditions générales d'utilisation du service d'intermédiation qu'il propose, et « sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder ». Par ailleurs, les opérateurs de plateformes en ligne dont l'activité dépasse un seuil de cinq

millions de visiteurs uniques par mois, par plateforme, calculé sur la base de la dernière année civile, devront élaborer et diffuser aux consommateurs des bonnes pratiques visant à renforcer les obligations de clarté, de transparence et de loyauté. Il convient désormais de garantir que les masses de données collectées ne doit pas être utilisées scrupuleusement au profit d'intérêts économiques et au préjudice des intérêts particuliers⁵⁴.

- 41 L'autorité administrative compétente peut procéder à des enquêtes afin d'évaluer et de comparer les pratiques des opérateurs de plateforme en ligne. La liste des plateformes qui ne respectent pas leurs obligations est rendue publique. Cette publicité constitue une forme de sanction, car elle permet de rompre la confiance des internautes vis-à-vis de ces plateformes et donc par voie de conséquence la baisse de leur utilisation générant la baisse du chiffre d'affaires des opérateurs de ces plateformes.
- 42 Enfin, la loi précitée fait obligation à 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 de délivrer aux utilisateurs une information loyale, claire et transparente sur les modalités de publication et de traitement des avis mis en ligne (Article L111-7-2 du code de consommation). Cette question touche par ailleurs la liberté d'opinion dont la protection a été également renforcée.

B/ Le renforcement de la protection de la liberté d'opinion

- 43 Les *fake news*⁵⁵, les tentatives de falsification des élections et la propagande à outrance ont largement occupé les médias, notamment lors des dernières élections présidentielles américaine et française⁵⁶. Ces faits ont par ailleurs fortement remis en cause l'idée d'une mondialisation positive où chacun pouvait en tirer des avantages. En raison de ces événements la tentation est grande d'instaurer un contrôle renforcé du Web et une censure accrue de l'information, constituant de nouvelles restrictions à la liberté d'expression. La question est de savoir cependant si l'on doit pour corriger un excès adopter des solutions qui sont tout autant excessives.
- 44 Il faut rappeler à cet égard que les contenus d'origine américaine sont présents de manière écrasante sur les réseaux participant ainsi à imposer l'impérialisme des États-Unis. À côté de cette omniprésence américaine, la propagande chinoise, russe ou islamiste sont minimes, mais il ne faut pas pour autant être moins vigilants à leur égard.
- 45 Si les responsabilités civiles et pénales des auteurs de ces fausses informations peuvent être recherchées sur le fondement des lois existantes, celles-ci sont toutefois insuffisantes pour permettre le retrait rapide des contenus en ligne afin d'éviter leur propagation ou leur réapparition. Cependant, les mesures à prendre doivent être conciliées avec la préservation de la liberté d'expression. Cet enjeu majeur se pose avec beaucoup d'acuité dans le cadre du débat électoral au cours duquel s'expriment par nature des opinions ou arguments que les adversaires des candidats peuvent estimer insincères.
- 46 Afin de contrecarrer d'éventuelles opérations de déstabilisation qui pourraient survenir lors des prochaines échéances électorales, le législateur français a décidé de faire évoluer la législation par l'adoption le 22 décembre 2018 des deux lois relatives à la lutte contre les fausses informations⁵⁷.

- 47 Tout d'abord, de nouveaux outils permettront de mieux lutter contre la diffusion de fausses informations durant la période électorale. Il s'agit d'une part, d'imposer en amont aux plateformes, des obligations de transparence renforcées en vue de permettre, aux autorités publiques de détecter d'éventuelles campagnes de déstabilisation des institutions par la diffusion de fausses informations et aux internautes de connaître notamment l'annonceur des contenus sponsorisés. D'autre part il s'agit en aval de permettre que soit rendue une décision judiciaire à bref délai visant à faire cesser leur diffusion.
- 48 Ensuite, la loi renforce le devoir de coopération des intermédiaires techniques en ajoutant la lutte contre les fausses informations aux obligations de coopération imposées aux intermédiaires techniques. Au-delà de l'obligation de retirer promptement tout contenu illicite porté à leur connaissance, les prestataires visés sont soumis à l'obligation de mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance des contenus constitutifs de fausses informations, d'une part, et de relayer promptement auprès des autorités publiques compétentes les signalements relatifs à ces contenus transmis par les internautes, d'autre part.
- 49 Ils doivent enfin, rendre publics les moyens qu'ils consacrent à la lutte contre la diffusion de fausses informations. Cette troisième obligation est transversale et impose une transparence dans la mise en place des deux premières obligations.
- 50 Cependant, il n'est pas sûr que ces nouvelles mesures soient efficaces et produisent les résultats escomptés. En effet, elles seront confrontées à l'absence de culture ou du sentiment national des internautes, car ceux-ci dépourvus de sens critique qui permet de démêler le vrai du faux. Le contrôle des autorités publiques peut très vite se retourner contre elles les internautes estimant que ce contrôle vise à instaurer et imposer un discours officiel, portant ainsi atteinte à leur liberté d'opinion. La meilleure arme contre la volonté hégémonique de certains par le biais d'Internet, est certainement la pédagogie et l'instruction permettant le développement l'esprit critique et par conséquent l'épanouissement de la liberté d'opinion.
- 51 Les pouvoirs publics ont dû par ailleurs innover en consacrant un nouveau principe de vigilance.

52

C/ L'adoption d'un principe de vigilance

- 53 Le Conseil constitutionnel avait déjà auparavant, imposé que soit observée une particulière vigilance dans la collecte et le traitement de données à caractère personnel de nature médicale⁵⁸. Mais on ne pouvait pas dire qu'il avait dégagé un principe général de vigilance. Le principe a été consacré comme nouveau principe par le RGPD.
- 54 Ce principe doit permettre d'aboutir à une remise en question continue de l'algorithme, car il est extrêmement complexe et en perpétuelle mutation. Ce principe recouvre tout d'abord la règle de la pertinence ou de minimisation. Cette règle exige que les données traitées soient pertinentes, adéquates et limitées au regard de la finalité poursuivie. Ainsi seules les données strictement nécessaires à la réalisation de l'objectif déterminé doivent être collectées : c'est le principe de minimisation. Autrement dit le responsable de traitement ne doit pas collecter plus de données que ce dont il a vraiment besoin⁵⁹.

- 55 Ensuite le principe impose la règle de la limitation de la conservation des données. Elle signifie qu'une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de les conserver et elles doivent être supprimées. La durée de conservation des données doit ainsi être limitée au strict minimum. Cette durée de conservation doit être définie au préalable par le responsable du traitement, en tenant compte des éventuelles obligations à conserver certaines données qui peuvent être variables. Afin de vérifier le respect de ce principe dans la pratique, une procédure de conservation, d'archivage et de purge devra être mise en œuvre.⁶⁰
- 56 Enfin, il exige la sécurité des données personnelles. Le responsable de traitement doit prendre toutes précautions utiles pour garantir la sécurité des données qu'il a collectées, mais aussi leur confidentialité, c'est-à-dire s'assurer que seules les personnes autorisées y accèdent. Ces mesures pourront être déterminées en fonction des risques pesant sur ce fichier (par exemple sensibilité des données ou encore objectif du traitement)
- 57 Les exigences de ce principe sont toutefois moins évidentes que ceux du principe de loyauté. Il faut davantage l'alimenter afin de permettre l'atteinte des objectifs qu'il sous-tend ou d'inventer de nouvelles règles. Il convient ainsi de définir un principe de vigilance/réflexivité en organisant un questionnement régulier, méthodique et délibératif à l'égard de ces objets mouvants. Il permettra ainsi de répondre aux exigences qu'imposent les objets technologiques du fait de leur nature, du caractère très compartimenté des chaînes algorithmiques au sein desquels ils s'insèrent ; enfin, de corriger la confiance excessive à laquelle ils donnent souvent lieu et qui peut porter atteinte à l'autonomie de la volonté. C'est toute la chaîne algorithmique, à savoir concepteurs, entreprises et citoyens qui doivent être mobilisés pour alimenter ce principe, au moyen de procédures concrètes comme la mise en place de comités d'éthique assurant un dialogue systématique et continu entre les différentes parties-prenantes.
- 58 Par ailleurs, le principe de vigilance devra s'appuyer sur une certification. Il s'agit ici d'élaborer un processus de contrôle fondé sur la certification des différentes composantes des systèmes pilotés par l'intelligence artificielle. La certification veillera à ce que les composantes initiales ainsi que leur mutation ne soient pas en mesure de porter atteinte aux droits des tiers et aux principes fondamentaux touchant aux libertés individuelles. Elle doit s'assurer que les résultats ne soient pas détournés à des fins commerciales préjudiciables aux intérêts particuliers.
- 59 Ainsi, on estime qu'un véhicule autonome circulant pendant une heure et demie produit un volume de données exprimé en giga octets. En cas d'accident, il sera alors nécessaire de pouvoir les retraiter pour déterminer au mieux les circonstances exactes. Cette certification inclut l'évaluation des risques, et doit s'organiser au sein du secteur privé dans le respect de normes établies et sanctionnées par l'État. Sa bonne conceptualisation permettra de garantir au mieux le respect de la vie privée et notamment de la protection des données personnelles.
- 60 Cependant, la nécessité de protéger les libertés individuelles ne doit pas aboutir à l'adoption de règles qui constitueront un frein aux innovations technologiques. Un juste équilibre doit être trouvé entre le développement de ces dernières et la garantie des libertés individuelles.

61

NOTES

1. La liberté de circulation : dans la même optique que la précédente, elle reconnaît à l'homme le droit d'aller et venir librement sur le territoire national, ce qui inclut la possibilité d'y entrer ou d'en sortir. Cette liberté a été étendue en Europe grâce aux accords de Schengen, permettant la libre circulation des personnes dans l'espace de la Communauté européenne. La liberté de culte ainsi que la liberté de conscience : la liberté de culte permet à chaque individu de pratiquer la religion de son choix, la liberté de conscience permet de ne pas avoir de croyance religieuse. La Déclaration des droits de l'homme et du citoyen en fixe pour limite : l'absence de trouble à l'ordre public. La liberté d'opinion consiste en la liberté de pensée associée à la liberté d'expression : elle permet à chacun de penser et d'exprimer ses pensées sans censure *préalable*, mais non sans sanctions, si cette liberté porte préjudice à quelqu'un. Elle va de pair avec la liberté de la presse, qui est celle d'un propriétaire de journal de dire ce qu'il veut dans son journal. La liberté économique : elle permet à chacun de percevoir des revenus de son travail et de pouvoir affecter ces derniers librement : liberté de travailler et de consommer. Nul ne peut se voir refuser *par principe* un emploi pour des considérations autres que de qualification professionnelle (par exemple sexe, origine ethnique, âge ou religion). La liberté contractuelle : les individus doivent être libres de définir eux-mêmes les termes des contrats qu'ils passent entre eux.

2. Dans son acception originelle, il fournit d'abord une protection contre une intrusion dans l'intimité des personnes, qu'elle soit le fait de l'État ou des tiers. Ainsi conçue, la vie privée est étroitement liée au domicile, à la correspondance, aux relations intimes, dont il faut préserver le secret. C'est en 1995 que le Conseil constitutionnel admettra en pleine lumière le droit au respect de la vie privée. Appelé à se prononcer sur la constitutionnalité de dispositions encadrant l'installation de systèmes de vidéosurveillance, le Conseil constitutionnel jugera « *que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* ».

En 1995, appelé à se prononcer sur la constitutionnalité de dispositions encadrant l'installation de systèmes de vidéosurveillance, se fondant sur l'article 66 de la Constitution, le Conseil constitutionnel jugera « *que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* » (Cons. const., 18 janv. 1995, n° 94-352 DC, cons. 3 ; rapp. 22 avr. 1997, n° 97-389 DC, cons. 44). C'est en 1998 que le Conseil constitutionnel remet en cause pour la première fois l'architecture de l'article 66 de la Constitution telle que voulue par le constituant de 1958, en distinguant le respect de la vie privée de la liberté individuelle, la faisant ainsi entrer dans nombre de libertés garanties par les articles 2 et 4 de la Constitution. (Cons. Const., 29 déc. 1998 n°98-405 DC).

3. Il s'agit de l'ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur. www.larousse.fr. Voir not. Jean-Marc DELTORN, La protection des données personnelles face aux algorithmes prédictifs, *RDLF* 2017.

4. *JORF* n°0235 du 8 octobre 2016 – « "Droit à l'oubli", "mort numérique"...: les députés accordent de nouveaux pouvoirs aux internautes », *L'Express*, 22 janv.2016.

5. 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) ; Nils MONNERIE « Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement », *Revue internationale de droit économique*, 2018/4 (t. XXXII), p. 431-452.

6. 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, transposée par la n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et modifiant la loi Informatique et liberté, *JORF* n° 0141 du 21 juin 2018.

7. Loi organique n° 2018-1201 et loi n° 2018-1202 du 22 déc. 2018 relatives à la lutte contre la manipulation de l'information, *JORF* n° 0297 du 23 déc. 2018.

8. Louis Edmond PETTITI, Emmanuel. DECAUX, Paul Henry. IMBERT (Sous la dir.) *La Convention européenne des droits de l'homme, commentaire article par article*, Économica, 1999.

9. CEDH, K.A et A.D c/ Belgique du 17 fév. 2005, cf. *Revue Droits* (48, 2008 ; 49, 2009).

10. Voir Hélène HURPY, *Fonction de l'autonomie personnelle et protection des droits de la personne humaine dans les jurisprudences constitutionnelles et européenne*, Thèse sous la direction du Professeur Annabelle PENA, Université Aix-Marseille, RDLF 2014.

11. Par exemple : Cons. const., 2010-25 QPC, 16 sept. 2010, *JORF* 16 sept. 2010, p. 16847 à propos du Fichier national automatisé des empreintes génétiques ; Cons. const., 2011-625 DC, 10 mars 2011, *JORF* 15 mars 2011, à propos des dispositions organisant le blocage des adresses électroniques des sites qui diffusent des images à caractère pornographique mettant en scène des mineurs.

12. Cf. Ferdinand MÉLIN-SOUCRAMANIEN, « Le contrôle de proportionnalité exercé par le Conseil constitutionnel », *LPA* n° 45, mars 2009 - Valérie GOESEL-LE BIHAN, « Le contrôle exercé par le Conseil constitutionnel : défense et illustration d'une théorie générale », *Revue de droit constitutionnel* n° 45, 2001.

13. L'exigence d'adéquation signifie que la mesure adoptée doit être *a priori* susceptible de permettre ou de faciliter la réalisation du but visé ; l'exigence de nécessité a pour corollaire que la mesure ne doit pas être plus restrictive que ne l'exige le but poursuivi, ce qui suppose que le choix d'une mesure moins contraignante pour les personnes concernées ou pour la collectivité n'aurait pu permettre d'atteindre à l'identique l'objectif visé et enfin l'exigence de proportionnalité au sens strict signifie, à supposer que la mesure soit nécessaire, elle ne soit pas hors de proportion avec le résultat recherché, ce qui implique une mise en balance des charges créées et des avantages apportés par la réalisation de l'objectif poursuivi.

14. « La conception des libertés par le Conseil constitutionnel et par la Cour européenne des droits de l'Homme, *Les nouveaux cahiers du Conseil constitutionnel*, 2011/3 N°32, pp 19 à 28.

15. Cons. const., 84-181 DC, 10-11 octobre 1984, Rec. 73.

16. Cons. const., 99-416 DC du 23 juillet 1999 sur la loi portant création d'une couverture maladie universelle.

17. Cons. Const. 99-422 DC du 21 décembre 1999.

18. Cons. const., 2003-467 DC du 13 mars 2003 sur la loi pour la sécurité intérieure

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

20. Les logiciels *Data Mining* font partie des outils analytiques utilisés pour l'analyse de données. Ils permettent aux utilisateurs d'analyser des données sous différents angles, de les catégoriser, et de résumer les relations identifiées. Techniquement, le *Data Mining* est le procédé permettant de trouver des corrélations ou des patterns entre de nombreuses bases de données relationnelles.

21. La notion de *big data* est un concept s'étant popularisé dès 2012 pour traduire le fait que les entreprises sont confrontées à des volumes de données (data) à traiter de plus en plus considérables et présentant de forts enjeux commerciaux et marketing.
22. Viktor MAYER-SCHONBERGER et Kenneth CUKIER, *Big Data : la révolution des données est en marche*, traduction de Hayet DHIFALLAH, éd. Laffont, 2014.
23. René DESCARTES, citation sur la conscience.
24. *Intelligence artificielle : des libertés individuelles au discernement orienté*, EuroGroup Consulting, mars 2017.
25. Le terme d'artefact désigne à l'origine un phénomène créé de toutes pièces par les conditions expérimentales. En tant qu'objet fabriqué, l'artefact regroupe les ustensiles, les bâtiments et œuvres d'art.
26. *Intelligence artificielle : des libertés individuelles au discernement orienté*, EuroGroup Consulting, préc.
27. Viktor MAYER-SCHONBERGER et Kenneth CUKIER, *Big Data : la révolution des données est en marche*, traduction de Hayet DHIFALLAH, préc.
28. *Intelligence artificielle : des libertés individuelles au discernement orienté*, préc., p. 63.
29. La psyché est une théorie en psychologie analytique, qui désigne l'ensemble des manifestations conscientes et inconscientes de la personnalité d'un individu. Elle est composée de 4 parties distinctes : le mental, l'égo, l'inconscient et le conscient.
30. Nicolas OCHOA. *Le droit des données personnelles, une police administrative spéciale*. Droit. Université Paris 1 Panthéon-Sorbonne, 2014. Le sigle IRM désigne l'imagerie à résonance magnétique.
31. Le Décret n° 2016-1460 du 28 oct. 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité. C'est la deuxième tentative du gouvernement français pour développer une base de données biométriques massive et centralisée, suite aux efforts du gouvernement de droite de Nicolas Sarkozy en 2012 pour adopter une loi proposant une base de données similaire.
 Dans ce cas, le Conseil constitutionnel français a finalement mis fin à la loi pour des raisons que la portée de la base de données était trop large et que la police l'utiliserait finalement pour identifier des individus à partir de données biométriques. Le gouvernement français insiste sur le fait que la nouvelle base de données ne sera utilisée que pour authentifier des individus et non pour les identifier. En d'autres termes, la base de données sera utilisée pour vérifier que les gens sont ce qu'ils disent être, et non pour savoir la biométrie qui a été découverte sur les lieux d'un crime.
- L'autorité judiciaire, gardienne de la liberté individuelle en vertu de l'article 66 de la Constitution, doit seule permettre l'utilisation du fichier à des fins de police judiciaire. Cf. Rapport d'information n° 439 (2004-2005) de M. Jean-René LECERF, Mission d'information de la commission des lois du sénat, déposé le 29 juin 2005.
32. André LUCAS, Jean DEVEZE, Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, PUF, 2001, pp. 14-15 : « L'internet a mis en avant le problème majeur de la « traçabilité » : toute connexion pour obtenir un quelconque service, toute consultation d'un site laissent des traces électroniques. Celles-ci sont dans l'ordinateur de l'internaute, identifié par une adresse IP (*Internet Protocol*), stable ou dynamique du fournisseur d'accès, du serveur, du gestionnaire de l'infrastructure-réseau. Collectées, rassemblées, traitées, diffusées, elles « parlent » de l'internaute qui devient transparent, elles diminuent ou suppriment la confidentialité des échanges. L'internaute est un moderne Petit Poucet qui laisse derrière lui volontairement et involontairement des « données-traces » que d'autres se chargent de collecter, d'interpréter, d'utiliser, de diffuser ».

33. LAMY *Droit du numérique*, Lamy, 2012, p. 1978 : « Système d'exploitation de banque de données et, par extension, serveur spécialisé permettant d'accéder sur la toile à des ressources (pages, sites, etc.) à partir de mots clés ».
34. En informatique, le *logging* désigne l'enregistrement séquentiel dans un fichier ou une base de données de tous les événements affectant un processus particulier (application, activité d'un réseau informatique...). « Le journal (en anglais *log file* ou plus simplement *log*), désigne alors le fichier contenant ces enregistrements. Généralement datés et classés par ordre chronologique, ces derniers permettent d'analyser pas à pas l'activité internet du processus et ses interactions avec son environnement ».
35. André LUCAS, Jean DEVEZE, Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, op. cit, p. 16 : « mais consulter des sites pornographiques du Web relevé aussi de la liberté personnelle, de la vie privée : on ne demande pas la carte d'identité à l'acheteur d'une revue « X » en kiosque. Cependant le fournisseur d'accès possède cette information personnelle ».
36. Et ce notamment par les technologies de la RFID (Radio Frequency Identification, en français « identification par radiofréquence ») dans un premier temps, des nanotechnologies dans un second.
37. Guillaume DESGENS-PASANAU, « Informatique et libertés, une équation à plusieurs inconnues », in GIROT Jean- Luc (dir.), *Le harcèlement numérique*, Dalloz, 2005, p. 97.
38. Nicolas OCHOA. *Le droit des données personnelles, une police administrative spéciale*. Droit. Université Paris 1 Panthéon-Sorbonne, 2014, op. cit.
39. Cette obligation de communication ne concerne pas les documents administratifs dont la consultation ou la communication porterait 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 sûreté de l'État, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations, à la monnaie et 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 et aux autres secrets protégés par la loi
40. Voir l'étude d'impact dur le projet de loi pour une République numérique, p. 11.
41. Viktor MAYER-SCHONBERGER, et Kenneth CUKER, *Big Data : la révolution des données est en marche*, traduction de Hayet DHIFALLAH, éd. Laffont, 2014, op. cit.
42. Voir lettre de Mission du Ministre de l'Économie, de l'Industrie et de l'Emploi en date du 31 juil. 2009 à ESCP Europe.
43. La Cnil peut prononcer des amendes administratives qui peuvent atteindre jusqu'à 20 millions d'euros, ou dans le cadre d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent.
44. <https://www.cnil.fr>
45. Cour de Cassation, ch. soc., 6 avr. 2004, n° 01-45.227, D. 2004. 2736, note R. de Quenaudon.
46. Cour de Cassation, ch. soc., 3 nov. 2011, n° 10-18.036, Dalloz actualité, 4 nov. 2011, obs. A. Astaix.
47. En 2014, l'UFC-Que choisir a aussi assigné en justice pour les mêmes raisons Twitter et Facebook. Le premier a été condamné en août 2018 également à 30 000 €.
48. TGI de Paris, 12 fév. 2019, UFC-Que Choisir c/ Google Inc. V. not. Luc-Marie AUGAGNEUR, « Les clauses abusives des conditions de Google », *AJ contrat* 2019, p. 175, 17 avr. 2019 – Cécile CRICHETON, « Clauses abusives et Google : une classification du régime attendue », *Dalloz IP/IT* 2019, 15 mars 2019.
49. Isabelle FALQUE PIERROTIN, Présidente de la Cnil, in *Algorithmes* : « Ce sont les individus qu'il faut responsabiliser », www.lepoint.fr, 29 janv. 2018.

50. La police prédictive permet d'anticiper les faits en utilisant notamment des données ouvertes et des données produites par les services de sécurité. V. not. : Nathalie PERRIER, « La police prédictive est un outil d'aide à la décision en matière de sécurité », *www.lagazettedescommunes.com* - Xavier LATOUR « Sécurité intérieure : un droit « augmenté ? », *AJDA* 2018. 431, 5 mars 2018.

51. Cnil, *Comment permettre à l'Homme de garder la main ?* Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, déc. 2017.

52. Aux termes de l'article L111-7 du code de la consommation, « 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 ».

53. Il s'agit de l'intermédiation proposée entre deux groupes d'utilisateurs. Elle permet la mise en relation de plusieurs types d'agents au sein d'un même espace.

54. Aux termes de l'article D111-15 du code de la consommation, « Le seuil du nombre de connexions au-delà duquel les opérateurs de plateformes en ligne sont soumis aux obligations de l'article L. 111-7-1 est fixé à cinq millions de visiteurs uniques par mois, par plateforme, calculé sur la base de la dernière année civile. Un opérateur de plateforme en ligne dont le nombre de connexions dépasse le seuil mentionné au premier alinéa dispose d'un délai de six mois pour se mettre en conformité avec l'article L. 111-7-1 ».

55. On peut traduire *fake news* par intox, informations fallacieuses ou fausses nouvelles. Il s'agit d'informations mensongères délivrées dans le but de manipuler ou tromper les individus. Voir à ce sujet notamment, « Les fake news menacent-elles le débat public ? », *www.vie-publique.fr*, 18 oct. 2018.

56. Voir notamment Philippe MOURON, « De la rumeur aux fausses informations », *Légicom*, 10 janv. 2018.

57. Voir not. : « La loi *Fake news* publiée après sa validation par le Conseil constitutionnel » *Légipresse*, 25 janv. 2019 – Pierre JANUEL et Marine BABONNEAU, « Loi *Fake news* : première application du référé », *Dalloz actualité*, *www.dalloz.fr*, 21 mai 2019 – Patrick SERGEANT, « Lutte contre les *fake news* et rémunération du droit voisin à la table des discussions entre éditeurs de presse et GAFA », *Légipresse*, 29 mai 2019 – Diane DE BELLESCIZE, « *Fake news* : une loi polémique, qui pose plus de questions qu'elle n'en résout », *Constitutions*, 25 mars 2019.

58. Cons. Const. 99-422 DC du 21 décembre 1999, op. cit.

59. Exemple de données non pertinentes : un site marchand qui propose de tester son produit à domicile n'a pas besoin de collecter.

60. Exemples de limitation de données : Les coordonnées d'un prospect qui ne répond à aucune sollicitation pendant 3 ans doivent être supprimées.

AUTEUR

JIM LAPIN

Maître de conférences associé à l'Université des Antilles

Membre du CREDDI-Université des Antilles

Membre associé de l'IDETCOM-Université Toulouse Capitole