LA TRANSPARENCE A L'EXCLUSION DES USAGES ALGORITHMIQUES

900. La reconnaissance d'un principe de transparence des traitements algorithmiques est indispensable en ce qu'il permet d'observer le positionnement des puissances œuvrant dans le cyberespace et leurs incidences sur les libertés. Cette problématique ne saurait toutefois dissimuler la question de l'usage algorithmique et de ses risques. En effet, quand bien même la transparence de ces outils serait totale d'un point de vue juridique et technique, ce qui au regard de l'informatique est une illusion, cela ne saurait légitimer l'immixtion d'une technologie dans un domaine.

901. Comme le souligne Dominique Cardon, avant les récents débats de la société civile au sujet de la transparence des traitements, certains mouvements militaient pour le recours à des algorithmes neutres, ce qui relève d'une méconnaissance technique[1810]. Puis, Frank Pasquale note à cet égard deux vagues[1811] : la première vague n'est pas contre le recours aux traitements algorithmiques, mais est en quête de responsabilisation des acteurs et d'une plus grande transparence des systèmes déployés. Quant à la seconde, intervenue plus récemment, elle est davantage réfractaire à l'immixtion des algorithmes et tend à freiner leurs déploiements, voire à les exclure. Bien que Frank Pasquale craigne que ces deux vagues ne s'affrontent, ces deux mouvements ne nous semblent pas irréconciliables.

902. C'est la raison pour laquelle le droit est aussi un outil de protection de la société et des personnes qui la composent, ce qui nous pousse nécessairement à étudier l'établissement d'un nouveau régime juridique à un niveau législatif et réglementaire relatif à la transparence appliquant le principe de transparence étudié (Section I). Il convient donc précisément de s'intéresser aux domaines nécessitant une transparence accrue. La récente proposition de règlement de la Commission européenne[1812] esquisse notamment à cet égard un régime juridique spécifique à la transparence de l'IA qui servira notre démonstration tout au long de ce chapitre.

[1810] « *Il est en effet vain de demander aux algorithmes d'être « neutres » alors qu'ils sont généralement conçus pour choisir, trier, filtrer ou ordonner les informations selon certains principes* », CARDON D., « Le pouvoir des algorithmes », *op. cit.*

[1811] PASQUALE F., The Second Wave of Algorithmic Accountability, *LMP Project.org* [en ligne]. 25 novembre 2019 [Consulté le 12 avril 2021]. Disponible à l'adresse : https://lpeproject.org/blog/the-second-wave-of-algorithmic-accountability

[1812] Proposition n° 2021/0106 (COD) de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, du 21 avril 2021.

903. Toutefois, la transparence ne peut pas tout et pose nécessairement, au-delà d'obligations de transparence, d'autres exigences au déploiement de ces systèmes. Cela implique même parfois l'exclusion de certaines techniques algorithmiques ou d'usages lorsque la technologie n'est plus au service des citoyens (Section II).

SECTION I - DE L'ETABLISSEMENT D'UN NOUVEAU REGIME JURIDIQUE LEGISLATIF ET REGLEMENTAIRE RELATIF A LA TRANSPARENCE

904. La mise en œuvre de la transparence des traitements algorithmiques implique de recourir à des techniques juridiques particulières dont l'étendue, la nature et le degré doivent être précisés. Certaines de ces techniques ont déjà été abordées tout au long de ces travaux, et s'appliquent déjà. Le droit européen, par l'intermédiaire de nouvelles propositions, s'intéresse toutefois à de nouvelles obligations. Enfin, il convient que les débiteurs de ces obligations soient correctement identifiés, ainsi que les personnes envers qui la levée de l'opacité s'effectuera (Paragraphe 1).

905. Pour ce faire, il est nécessaire de se fonder sur les risques algorithmiques ainsi que la légitimité de l'acteur en cause. Parmi les opérateurs économiques, tous ne représentent pas un risque systémique sur les personnes et la société. La puissance publique mérite également une attention toute particulière du fait de sa plus grande force (Paragraphe 2).

PARAGRAPHE 1 - Choix des techniques juridiques concourant à la transparence

906. Il convient de s'intéresser à la fois aux outils juridiques ainsi qu'aux approches prospectives et concrètes les plus adéquates à retenir dans les régimes juridiques œuvrant en faveur du principe de transparence étudié. Il est important de considérer que plusieurs approches peuvent être retenues par le droit pour réguler les traitements algorithmiques. Ainsi, la neutralité technique apparaît comme une force dans les régimes juridiques généraux (A) tandis qu'un panorama des différentes techniques juridiques nous enseigne sur ce qu'il est nécessaire de réaliser (B).

A - De la nécessaire neutralité technique des régimes juridiques généraux

907. La « neutralité technique » constitue une approche qui nous semble vertueuse en ce sens qu'elle est suffisamment englobante pour ne pas exclure certaines technologies du giron d'une règlementation qui se voudrait générale. Cela n'empêche nullement un régime juridique sectoriel précis en fonction de l'évolution de la technique.

908. A ce titre, la LIL de 1978[1813], à l'instar des réglementations nationales des autres Etats à cette époque, a institué une vision généraliste en visant les traitements de données personnelles pour préserver la vie privée des personnes physiques et les éventuelles discriminations qui en découleraient[1814]. Quel que soit le procédé utilisé en informatique, c'est la manipulation de données personnelles qui rend applicable ce régime juridique. L'objet saisi, les données personnelles, doit donc être protégé indépendamment de la technologie numérique mise en œuvre. C'est aussi cette philosophie qui est reprise par le RGPD ou la convention 108[1815].

909. Mais la vie privée étant une liberté individuelle rattachée aux personnes physiques, les personnes morales ne bénéficiaient pas d'une quelconque protection alors que des traitements étaient tout aussi susceptibles de les affecter. Indépendamment des exceptions prévues par le texte, le responsable du traitement, qu'il soit public ou privé, est tenu de communiquer à la personne physique concernée des informations sur ce traitement.

910. Les règlementations sectorielles intervenues plus tardivement ont également fait le choix de la neutralité technologique. Ainsi, dans le cadre de la LRN, il n'a pas été fait l'erreur d'exclure certaines méthodes algorithmiques préférant saisir les décisions administratives individuelles prises sur le fondement d'un traitement algorithmique[1816]. A l'exception des secrets protégés par la loi, une certaine transparence s'appliquera donc à l'intéressé au sujet du traitement ayant fondé la décision, et ce quel que soit le logiciel utilisé. Il en est de même lorsque ladite loi désigne l'opérateur de plateforme en ligne soumis à des obligations particulières de loyauté, de clarté et de transparence, pour les personnes, physiques ou morales,

[1813] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[1814] A cette époque, cette législation vise le respect de la vie privée. Il n'existe pas à ce moment le début d'une autonomisation du respect des données personnelles. Voir en ce sens le rapport de la commission informatique et libertés, dit « Tricot », La Documentation Française, 1975, p. 49. Depuis, il est en effet intéressant de noter que le respect des données personnelles figure dans certains textes, comme c'est le cas pour la Charte des droits fondamentaux de l'Union européenne à l'article 8, détachée du respect de la vie privée et familiale, ce qui ouvre la voie à un régime juridique totalement différent de celui de la vie privée.
[1815] *Supra.*, n° 80 et s.
[1816] *Supra.*, n° 404 et s.

agissant à titre professionnel, opérant notamment « *le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ; »*[1817]. Le caractère générique, et donc neutre de la formulation, offre une adaptabilité de ces régimes juridiques dans le temps.

911. Arnaud Latil observait dans son panorama des déclarations des droits du numérique publiées lors de la dernière décennie que le principe de neutralité technique est présent dans une grande partie de ces textes[1818], ce qui signifie que « *les auteurs évitent le plus possible de se référer à une technologie particulière* » et que « *cet objectif rédactionnel vise à éviter l'obsolescence juridique et donc à lutter contre la réduction prématurée de leur domaine d'application due au développement, par nature imprévisible, de nouvelles techniques. Les textes étudiés se bornent à faire référence à Internet (rarement au web), aux données et aux processus de décisions automatisées* »[1819].

912. Tandis que l'informatique n'a pas attendu l'IA pour avoir des incidences sur les droits fondamentaux des personnes et sur la société, une nouvelle approche complémentaire semble se dessiner, notamment pour assurer une transparence de ces systèmes, à savoir par les risques par domaine d'intervention[1820]. Mais le choix de la neutralité technique ne semble pas être celui privilégié par la Commission européenne, risquant une obsolescence prématurée et une insécurité juridique aussi bien pour les acteurs soumis à ces obligations que pour les personnes subissant ces systèmes.

913. Il aurait été ainsi préférable d'évoquer tout traitement de données à caractère personnel ou non, intervenant dans les domaines énoncés par la proposition. En effet, la dénomination de « *systèmes d'intelligence artificielle* » telle que retenue renvoie à une ou plusieurs catégories de techniques utilisées dans un logiciel[1821]. Dès lors, les techniques en question sont listées en annexe du projet et nous y retrouvons les « *approches d'apprentissage automatique, y compris d'apprentissage supervisé, non supervisé et par renforcement, utilisant une grande variété de*

[1817] *Supra.*, n° 269 et s.
[1818] FJELD J, ACHTEN N, HILLIGOSS H, NAGY A, SRIKUMAR M., *Principled Artifical Intelligence : Mapping Consensus in Ethical and Rights-Based Approches to Principles for AI*, *op. cit.*
[1819] LATIL A., « En attendant la Déclaration de droits fondamentaux du numérique », *op. cit*.
[1820] Proposition n° 2021/0106 (COD) de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, du 21 avril 2021. Il convient toutefois de noter que ce projet n'est pas si général en ce qu'il ne régule pas par exemple les réseaux sociaux, la commission ayant préférée le compléter par l'adoption d'une règlementation particulière. En ce sens, *Supra.*, n° 260 et s.
[1821] Art. 3, § 1 du projet.

méthodes, y compris l'apprentissage profond »[1822]. Les systèmes logiques sont également pris en considération par la présente proposition[1823]. Enfin, les dernières techniques saisies par la nouvelle réglementation en cours d'élaboration sont les systèmes statistiques qui comportent les « *approches* statistiques, *estimation bayésienne, méthodes de recherche et d'optimisation* »[1824]. Paradoxalement, bien qu'il s'agisse en apparence d'une certaine neutralité technique, car la proposition ne fait aucunement référence à une marque ou à un logiciel particulier, il s'agit d'une approche excluant de fait certaines techniques même si l'annexe utilise sans plus de précisions le terme « incluant » ces méthodes. Cela sera donc à l'appréciation des tribunaux, ce qui n'est pas sans provoquer une certaine insécurité juridique. Il est difficile pour l'heure de savoir si ces trois grandes catégories de techniques sont suffisamment exhaustives ou si elles sont lacunaires au point d'engendrer un contournement du régime juridique, puisque la Commission estime qu'elles sont à elles seules responsables d'un risque, notamment pour les droits fondamentaux. En effet, dans l'hypothèse où une technique n'est pas abordée par le règlement, le régime juridique en construction ne s'appliquerait pas, y compris en cas d'effets sur les personnes ou la société, à l'exception naturellement des réglementations généralistes déjà en application comme le RGPD (mais uniquement parce que son champ d'application porte sur les données à caractère personnel). Ainsi, même si les concepts utilisés par la Commission sont larges, tous les systèmes d'IA ne sont pas concernés par cette proposition[1825]. Quand bien même cette approche pourrait être considérée de neutre d'un point de vue technique, elle n'est pas si englobante et ne peut valoir la dénomination générale de « traitement algorithmique » ou « de traitement de données ». Il serait effectivement dommageable qu'en essayant de réglementer l'IA, plus précisément lesdits systèmes, nous excluions de fait des techniques futures ou non anticipées au moment de la rédaction du texte. L'adaptabilité de ce nouveau régime juridique à des nouvelles techniques pouvant émaner par exemple de l'ordinateur quantique, amenées à potentiellement révolutionner l'informatique interroge tout autant. Bien que la Commission ait voulu s'émanciper des définitions littéraires ou encore informatiques de l'IA, n'est-ce pas une erreur d'avoir voulu donner une définition juridique à un concept aussi discuté par les sciences informatiques ?

[1822] Annexe I a) du projet.
[1823] Annexe I b) : les systèmes logiques sont les *« approches fondées sur la logique et les connaissances, y compris la représentation des connaissances, la programmation inductive (logique), les bases de connaissances, les moteurs d'inférence et de déduction, le raisonnement (symbolique) et les systèmes experts* ».
[1824] Annexe I c).
[1825] CRICHTON C., « Projet de règlement sur l'IA (I), des concepts larges retenus par la Commission », *Dalloz IP/IT*, 2021.

914. Au-delà des techniques saisies par le projet, un système d'IA est qualifié comme tel par le règlement uniquement s'il « *peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit* »[1826]. L'association des techniques étudiées à des fins spécifiques rend donc ce régime juridique plus restrictif. Comme le note Cécile Crichton, il est troublant que la Commission ait fait par exemple le choix de préciser que les objectifs soient définis par une intervention humaine, ce qui n'est déjà plus toujours le cas[1827]. Et *a contrario*, un système d'IA ne générant pas du contenu, des prédictions ou des décisions produisant des effets avec son environnement, ne serait pas concerné par ces nouvelles obligations, y compris de transparence, alors même qu'il pourrait exercer une incidence indirecte sur la société et les personnes. Les concepts utilisés demeurent en l'état relativement flous juridiquement. La difficulté serait un contournement aisé du régime juridique par les acteurs, rendant inopérant la volonté initiale de la Commission.

B - Panorama des techniques juridiques concourant à la transparence des traitements algorithmiques

1 - Les débiteurs et destinataires des obligations de transparence

915. Souhaiter la transparence des traitements algorithmiques impose nécessairement de désigner le ou les débiteur(s) de ces obligations ainsi que leurs destinataires. En d'autres termes, quel sera l'acteur qui devra expliquer le traitement, et à qui.

916. L'étude du droit positif sur ces thématiques[1828] démontre que les acteurs sont actuellement parfaitement ciblés, notamment car les régimes juridiques abordés sont en réaction à des faits juridiques particuliers. Ainsi, ces réglementations sont apparues de manière chronologique au fur et à mesure que les effets de l'informatique ont été démontrés, dans une approche libérale. Tel est le cas en matière de données personnelles en mettant en œuvre un principe de transparence et un droit d'accès aux données par les personnes physiques auprès des responsables du traitement[1829]. De la même manière, lorsque les plateformes en ligne sont accusées de manipulation par l'intermédiaire de recommandations, le législateur leur impose

[1826] Art. 3 § 1 du projet.
[1827] CRICHTON C., « Projet de règlement sur l'IA (I), des concepts larges retenus par la Commission », *op. cit.*
[1828] Il s'agit de la première partie de ces travaux, *Supra*., n° 72 et s.
[1829] *Supra*., n° 80 et s.

des obligations vis-à-vis des consommateurs[1830]. Dans ce cas de figure il s'agit surtout d'une transparence conditionnant le consentement des individus.

917. Plus généralement, les décisions administratives individuelles prises sur le fondement d'un traitement algorithmique impliquent que l'administration soit en mesure d'expliquer les principales caractéristiques du traitement dès lors que l'intéressé en fait la demande[1831]. L'objectif poursuivi est ici de réduire le risque d'arbitraire de la part de l'administration.

918. Puis, parmi les régimes juridiques sectoriels étudiés, nous avons également constaté que la personne faisant l'objet d'un traitement de données n'était pas toujours au cœur de la transparence. C'est particulièrement le cas dans les régimes juridiques faisant intervenir des obligations d'informations de la part du concepteur du logiciel à son utilisateur (comme c'est le cas pour les outils d'aide à la prise de décision en matière médicale). Il en est de même concernant les constructeurs de véhicule à délégation de conduite ou de leurs mandataires auprès de l'autorité de contrôle chargée d'assurer leur conformité[1832]. Le constructeur se voit bénéficier d'un droit d'accès aux données du véhicule quand celui-ci est en fonctionnement afin de constater qu'il fonctionne correctement, et le cas échéant améliorer la sécurité[1833]. Cela s'explique car cette transparence conditionne essentiellement la sécurité des personnes et la mise en jeu de la responsabilité.

919. Plus récemment, la proposition de règlement européen général au sujet de l'IA évoque quant à elle plusieurs acteurs de la chaîne algorithmique, ce qui n'est pas sans complexifier, pour les personnes subissant ces systèmes, l'identification des débiteurs des nouvelles obligations de transparence. Son ambition est de proposer d'uniformiser de nombreux régimes juridiques existants essentiellement au nom de la protection des droits fondamentaux. En cela, elle participe à une autonomisation de la transparence des traitements algorithmiques dans un but de respect des droits et libertés. Le projet concerne les opérateurs[1834], tels que les

[1830] *Supra.*, n° 260 et s.
[1831] *Supra.*, n° 404 et s.
[1832] *Supra.*, n°372 et s.
[1833] *Ibid.*
[1834] Art. 3 (8) du projet.

fournisseurs[1835], l'utilisateur[1836], le mandataire[1837], l'importateur[1838], et le distributeur[1839], ce qui n'est pas sans rappeler les acteurs traditionnels appréhendés par le droit de l'Union comme par exemple sur la réglementation relative à l'intermédiation entre professionnels[1840]. A ce titre, certains auteurs reprochent déjà la complexité de la distinction entre le fournisseur et l'utilisateur dans la mesure où elle empêcherait de saisir certaines réalités techniques comme en matière d'agent conversationnel[1841]. Ces logiciels sont notamment configurables et personnalisables par l'utilisateur. Ainsi, imposer des obligations d'information aux professionnels au sens large comme cela est le cas en droit de la consommation semblerait plus adapté pour le consommateur. Cela rappelle à quel point il convient d'être le plus général possible, puisqu'à défaut, la désignation d'une pluralité de débiteurs est contreproductive à l'effectivité d'une règlementation générale relative à la transparence de l'environnement numérique.

920. L'ambition du projet est pourtant de prendre en considération le plus d'acteurs possibles de façon à ce que les nouvelles obligations de transparence renforcent la confiance aussi bien des entreprises envers leurs clients que des administrations à l'encontre de leurs administrés[1842]. Toutefois, ces obligations que nous verrons ultérieurement ne s'appliquent pas à tous les systèmes d'IA[1843], mais surtout à ceux considérés comme étant à « *haut risque* »[1844].

921. Toutefois, les personnes subissant ces systèmes ne sont aucunement définies par le règlement, ce qui est dommageable. En effet, ne convient-il pas, par exemple, de considérer qu'un utilisateur, à qui pourtant s'appliquent de nouvelles obligations, est en situation de vulnérabilité vis-à-vis d'un outil dont le traitement lui échapperait, notamment car il ne peut

[1835] Selon l'article 3 (2) du projet, le fournisseur est « *une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit* ».
[1836] Art. 3 (3), l'utilisateur est défini comme « *toute personne physique ou morale, autorité publique, agence ou autre organisme utilisant sous sa propre autorité un système d'IA, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel* ».
[1837] Art. 3 (5), le mandataire est « *toute personne physique ou morale établie dans l'Union ayant reçu mandat écrit d'un fournisseur de système d'IA pour s'acquitter en son nom des obligations et des procédures établies par le présent règlement* ».
[1838] Art. 3 (6), l'importateur est « *toute personne physique ou morale établie dans l'Union qui met sur le marché ou met en service un système d'IA qui porte le nom ou la marque d'une personne physique ou morale établie en dehors de l'Union* ».
[1839] Art. 3 (7), le distributeur est « *toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fournisseur ou l'importateur, qui met un système d'IA à disposition sur le marché de l'Union sans altérer ses propriétés* ».
[1840] Règlement UE 2019/1150 du Parlement Européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne. *Supra.*, n° 304 et s.
[1841] VEALE M., ZUIDERVEEN BORGESIUS F., « Demystifying the Draft EU Artificial Intellingence Act », *Computer Law Review International*, 2021, p. 97.
[1842] Proposition n° 2021/0106 (COD) de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, du 21 avril 2021, p. 10.
[1843] *Ibid.*, p. 9.
[1844] *Infra.*, n° 946 et s.

vérifier lui-même que les informations du fournisseur sont véridiques[1845] ? De la même manière, l'Etat ne doit-il pas également être considéré, dans certaines situations, comme une personne vulnérable vis-à-vis de ces systèmes ? Tel est par exemple le cas des traitements par l'exploration de données qui sont amenés à orienter les politiques publiques[1846].

922. La règlementation prévoit parfois qu'une transparence doit s'opérer auprès des régulateurs et non des personnes ou de la société. Il s'agit donc dans ce cas d'une transparence indirecte, mais cela ne veut pas dire pour autant que l'autorité de contrôle a la nécessité de communiquer ensuite dessus, quand bien même les secrets seraient protégés. Le projet précise à cet égard que le contrôleur qui devra être désigné est soumis à des obligations renforcées de confidentialité[1847]. Il ne faudrait pas que la levée des opacités des algorithmes se heurte de nouveau à une autre opacité : celle du contrôleur. Concernant la problématique de la symétrie informationnelle, c'est-à-dire s'assurer que l'information révélée par le débiteur à l'intéressé est véridique, elle devrait relever de fait de notre instance de contrôle unique que nous proposons dans l'immense majorité des cas[1848] en raison des secrets protégés par la loi. Et parfois, nous avons même proposé que pour certaines matières sensibles, ladite instance ait la charge d'effectuer cette transparence mais de manière indirecte, en tant que tiers de confiance. Cela implique, dans cette hypothèse, que pour exercer une transparence indirecte, les acteurs concernés aient également des obligations de transparence totale vis-à-vis de cette instance de contrôle au même titre que la réglementation sur le *trading algorithmique*[1849], et que cette dernière communique ensuite sous une forme intelligible à propos de ces systèmes.

2 - La nature et le degré de transparence

923. Comme nous l'avons vu, il existe des techniques juridiques plus traditionnelles participant à la transparence des traitements algorithmiques sans pour autant avoir été pensées pour cela initialement. Tel est le cas par exemple de l'allègement de la charge de la preuve, voire, le cas échéant, de son renversement[1850], qui peuvent être efficaces pour obtenir d'un

[1845] Il est par ailleurs à noter que l'utilisateur qui va enrichir un système d'apprentissage avec des données peut pervertir le système volontairement ou non.
[1846] *Supra.*, n° 484 et s.
[1847] Proposition n° 2021/0106 (COD) de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, du 21 avril 2021, *op. cit.*, p. 11.
[1848] *Supra.*, n° 717 et s.
[1849] *Supra.*, n° 316 et s.
[1850] *Supra.*, n° 287 et 371.

acteur des informations sur le fonctionnement des traitements, tout comme le juge judiciaire bénéficie au titre de pouvoirs d'instruction prévus par l'article 145 du Code de procédure civile de la faculté d'obtenir la communication de documents techniques sur ces systèmes[1851]. L'obligation de publication de rapports réguliers et d'analyses d'impact est aussi une méthode pouvant éclairer les citoyens ou le pouvoir politique sur le comportement et les incidences des outils algorithmiques, ce qui n'a malheureusement pas été suffisamment le cas en matière de renseignement[1852] ou lors de la crise de la Covid-19[1853]. Mais il sera question ici de s'interroger sur les techniques propres à la compréhension des traitements.

924. La nature et le degré de transparence sont variables en fonction du déploiement du traitement. La transparence peut être préalable à la mise en œuvre du traitement, ou être *a posteriori* vis-à-vis des régulateurs ou des personnes subissant ces systèmes, ou intéressés au titre de leur qualité de justiciable.

925. Nous retrouvons toutefois parmi les régimes juridiques en vigueur ou en cours d'élaboration des approches communes même s'il convient de considérer que la transparence en tant que telle est un ensemble de techniques juridiques ne reposant pas sur une unité conceptuelle[1854]. Le même constat peut être effectué en matière de traitement algorithmique. Bien que les exceptions demeurent nombreuses, la communication du code source des logiciels utilisés par l'administration peut être sollicitée par les administrés, sans oublier la documentation afférente pour la comprendre. La LRN a également prévu une mention explicite informant l'intéressé qu'une décision administrative individuelle à son encontre est fondée sur un traitement algorithmique, ce qui permet ensuite le cas échéant de demander la communication des principales caractéristiques du traitement, que l'intéressé soit par ailleurs une personne physique ou morale[1855]. Et plus récemment, le RGPD, dans la continuité de la directive 95/46/CE et de la LIL de 1978, prévoit la communication d'un certain nombre d'informations lors de la collecte et du traitement des données personnelles. La nouvelle

---

[1851] *Supra*., n° 337.

[1852] En ce sens, comme l'indique la députée Paula Forteza il est à noter que les parlementaires ne bénéficient pas par exemple des informations suffisantes au sujet du déploiement des outils algorithmiques utilisés à titre expérimental dans le cadre de la loi renseignement. « *À ce jour, l'étude d'impact présentée par le gouvernement est très parcellaire du fait de la confidentialité de la technologie appliquée. Nous savons seulement que cette technologie a permis de générer 1739 alertes qui ont conduit à lever l'anonymat.* », FORTEZA P., L'utilisation des nouvelles technologies par les pouvoirs publics, *op. cit.*

[1853] Alors que le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommés « *Stopcovid* » prévoyait en son article 5 un rapport public du responsable de traitement sur le fonctionnement de l'application dans les trente jours suivant sa mise en œuvre, et au plus tard le 30 janvier 2021, le décret 2021-157 du 12 février 2021 est venu substituer à cette obligation une publication « *dans les trente jours suivant le terme de la mise en œuvre de l'application* », ce qui dénature la prétention initiale et cette forme de transparence.

[1854] KERLEO J-F., *La transparence en droit, Recherche sur la formation d'une culture juridique*, *op. cit.*

[1855] *Supra*., n° 407 et s.

règlementation sur les données personnelles prévoit même un droit à l'explicabilité des décisions automatisées portant sur ces données[1856]. Quant aux plateformes en ligne, les obligations de transparence sont plutôt générales, à travers la communication d'informations précontractuelles, voire contractuelles au titre de la loyauté, de la clarté et de la transparence « *sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder* » [1857] notamment.

926. Les techniques juridiques précitées et abordées tout au long de ces travaux ont pour objectif de concourir à une plus grande transparence de ces systèmes même si l'objectif poursuivi n'est pas forcément la compréhension du numérique dans un but de protection des droits et libertés. Elles peinent de plus à répondre aux nouveaux enjeux comme en matière d'IA.

927. C'est la raison pour laquelle la proposition de règlement européen sur l'IA prévoit des nouvelles techniques juridiques se superposant aux régimes juridiques existants et aux objectifs déjà poursuivis pour parvenir à l'intelligibilité de ces systèmes à des fins de respect des droits fondamentaux, de la santé, mais aussi pour assurer la sécurité juridique nécessaire au développement de ces outils[1858].

928. La transparence mise en œuvre par le règlement possède de plus des degrés divers en fonction du domaine d'intervention de la technologie. Cette nouvelle règlementation prévoit aussi que pour certains systèmes d'IA[1859], « *les fournisseurs veillent à ce que les systèmes d'IA destinés à interagir avec des personnes physiques soient conçus et développés de manière à ce que les personnes physiques soient informées qu'elles interagissent avec un système d'IA* »[1860]. Il serait également nécessaire de garder une trace de cette interaction pour démontrer par exemple le choix de l'utilisateur en cas de litige, et ce en vue de lutter contre les systèmes inéquitables numériques[1861]. Cette approche est primordiale puisqu'elle conditionne la connaissance de l'intervention d'un traitement, ouvrant ensuite la voie à des demandes d'information, voire à sa contestation devant une juridiction. Elle prévoit également pour

[1856] *Supra.*, n° 80 et s.
[1857] Supra., n° 266 et s.
[1858] Parmi les objectifs visés par cette proposition de règlement (hors annexe), nous retrouvons le respect des droits fondamentaux et des valeurs de l'Union. Cette volonté est affirmée par la Commission et le terme de « droits fondamentaux » est utilisé 78 fois dans le texte. La santé et la sécurité sont également associées à l'approche fondée sur les risques. La santé est utilisée 50 fois, tandis que la sécurité l'est 143 fois. Enfin, la sécurité juridique est également une priorité de l'Union pour assurer le développement de ces technologies, raison pour laquelle elle est citée 17 fois. Tel est donc le fondement de ce projet.
[1859] *Infra*., n° 946 et s.
[1860] Art. 52 du projet.
[1861] DANET A., ENGUEHARD C., « De la preuve et de l'utilisation des Systèmes Inéquitables Numériques », Les convergences du droit et du numérique, septembre 2017, Bordeaux, *INRIA* [en ligne]. [Consulté le 22 juin 2020]. Disponible à l'adresse : https://hal.inria.fr/hal-01730375/document

certains systèmes[1862] à haut risque leur inscription dans un registre[1863] géré par *« la Commission pour accroître la transparence, améliorer le contrôle public et renforcer le contrôle ex post par les autorités compétentes »*[1864], alors que le RGPD avait donné une place moins importante que la LIL de 1978 sur ce point[1865]. Cela permettrait, comme l'indique le CEPD, de fournir des informations au grand public sur les failles et incidents connus[1866].

929. Le projet de règlement européen inaugure une approche fondée sur les risques[1867] avec le déploiement de nouvelles techniques juridiques concourant directement ou indirectement à la transparence des traitements algorithmiques. Plus l'usage est risqué eu égard à son domaine d'intervention, plus les obligations de transparence sont renforcées. Ainsi, lorsque l'usage est à haut risque, il convient de s'assurer de la conformité au droit *ex ante*, c'est-à-dire avant son déploiement[1868], et ce conformément à une procédure d'évaluation[1869]. Plusieurs obligations doivent alors être respectées par le fournisseur[1870], telles que la mise en œuvre d'un système de gestion des risques incluant la tenue d'une documentation précise par ce dernier[1871]. Dans l'hypothèse où le système d'IA ferait appel à des données, il est également prévu l'élaboration d'une surveillance des modèles, des données, de la méthodologie, et ce afin d'assurer la détection des éventuels biais[1872]. A cela s'ajoute la confection d'une documentation technique standardisée[1873] qui devra être mise à jour[1874] ainsi que la conservation de la journalisation du traitement[1875]. Ces obligations permettent aussi bien à l'acteur du marché qu'au régulateur de donner des indications sur le fonctionnement du traitement et sa traçabilité.

930. D'autres obligations prévues par le projet portent davantage sur la communication d'informations aux personnes subissant ces systèmes[1876]. Dès lors, ces derniers seraient conçus et développés pour permettre aux utilisateurs d'interpréter les résultats du système et de les

[1862] *Infra.*, n° 946 et s.
[1863] Art. 60 du projet. En ce sens, nous avions déjà abordé la manière dont la tenue des registres concourait à une meilleure transparence auprès des autorités publiques.
[1864] *Ibid.*, p.16 du projet.
[1865] *Supra.*, n° 232 et s.
[1866] EDPB-EDPS, Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p. 19, *EDPB.europa.eu* [en ligne]. 18 juin 2021. [Consulté le 22 juillet 2021]. Disponible à l'adresse : https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf
[1867] Nous développerons ultérieurement, *Infra.*, n° 946 et s.
[1868] Art. 8 § 2 du projet.
[1869] *Ibid.*, Art. 19 et 43.
[1870] *Ibid.*, Art. 16 a.
[1871] *Ibid.*, Art. 9 et art. 17.
[1872] *Ibid.*, Art. 10.
[1873] *Ibid.*, Ces éléments sont précisés en annexe 4 du projet.
[1874] *Ibid.*, Art. 11 et art. 18.
[1875] *Ibid.*, Art. 12. Voir également art. 20.
[1876] *Ibid.*, Art. 13.

utiliser de manière appropriée[1877]. Un mode d'emploi comportant des informations concises, complètes, correctes, claires et intelligibles sur le traitement est à délivrer à l'utilisateur[1878].

931. Le fournisseur est tenu de déployer un système de surveillance humaine de celui-ci[1879]. Cette supervision a pour objectif de réduire la durée d'une éventuelle violation des droits et libertés[1880]. Nous considérons notamment que les obligations prévues à l'article 15 relatives à l'exactitude du système concourent à la transparence en ce qu'elles permettent de prévenir les erreurs, les défaillances et les biais du système[1881].

932. Il est intéressant de noter que certaines obligations du fournisseur sont à tenir vis-à-vis du régulateur, comme la notification d'un dysfonctionnement[1882]. Il est également question d'une coopération avec l'autorité de contrôle[1883]. Des documents doivent aussi être tenus à disposition d'une autorité de contrôle pour une durée de dix ans[1884], ainsi qu'une surveillance postérieure à la commercialisation du système, et ce toute sa vie[1885].

933. Certains systèmes d'IA, qui sont parfois des algorithmes auto-apprenants, font l'objet d'obligations particulières auprès de l'utilisateur professionnel qui dispose d'un devoir de pertinence et de qualité des données qu'il utilise. En effet, la qualité de ces données a une incidence sur les calculs opérés par le système, raison pour laquelle il est tenu de stocker les journaux d'événements générés automatiquement par le système[1886].

934. Concernant les algorithmes non régis par ces nouvelles obligations, car jugés à faible risque, ils seraient conditionnés à une transparence minimale, notamment par l'adoption de normes volontaires tels que les codes de conduite[1887].

935. Néanmoins, la communication d'une information générale ne permet pas pour la personne subissant ces systèmes de rejouer le traitement. C'est pour cette raison qu'il est parfois préférable de transmettre plus d'éléments directement à la personne concernée ou bien à l'autorité de contrôle qui devra ensuite effectuer un rôle de tiers de confiance. Le renforcement

[1877] *Ibid*., Art. 13 § 1.
[1878] *Ibid*., Art. 13 § 2. Ces mentions doivent comporter certaines précisions minimales telles que celles prévues à l'article 13 § 3.
[1879] *Ibid*., Art. 14.
[1880] *Ibid*., Art. 14 § 2.
[1881] *Ibid*., Art. 15.
[1882] *Ibid*., Art. 22 et art. 62.
[1883] *Ibid*., Art. 23.
[1884] *Ibid*., Art. 50, y compris ceux mentionnés à l'article 11 et 17.
[1885] *Ibid*., Art. 61.
[1886] *Ibid*., Art. 29.
[1887] Art. 69 du projet.

des audits et des certifications[1888] sont par ailleurs des techniques juridiques nécessaires à prendre en considération pour amoindrir le risque.

936. Des outils juridiques ont donc été pensés spécifiquement pour concourir à la transparence des traitements, mais encore faut-il les déployer correctement de manière la plus adéquate possible.

PARAGRAPHE 2 - Etude des différentes approches permettant d'appréhender les obligations de transparence

937. Après avoir dressé la nécessité de la neutralité technique des régimes juridiques généraux et les différentes techniques juridiques concourant à une meilleure transparence qu'il est souhaitable de retenir, deux principales approches nous semblent être pertinentes dans l'appréciation du degré et de la nature de la transparence et elles doivent donc nécessairement être combinées afin que la régulation de ces algorithmes ne soit pas lacunaire. Il s'agit de l'approche par la légitimité (A) et fondée sur les risques (B).

A - L'approche fondée sur la légitimité

938. Pour l'heure, et dans l'esprit du libéralisme politique, la puissance de l'Etat ne peut être appréhendée de la même manière que celles des entités privées puisque même lorsqu'il semble être affaibli, l'Etat sait faire ressurgir sa force, notamment par la voie de son exorbitance du droit commun. La mission d'intérêt général dévolue à l'administration et aux représentants du peuple souverain implique toutefois un contrôle conséquent de leur action, ne serait-ce que pour s'assurer que la plus grande force de l'Etat ne soit pas accaparée par des intérêts particuliers[1889]. Les secrets inhérents aux intérêts de la nation sont autant de menaces planant sur les droits et libertés, ce qui nécessite un contrôle renforcé de l'action publique, car il est dans certain cas un prétexte illégitime à l'opacité.

[1888] Art. 42 du RGPD et Art. 44 du projet de règlement sur l'IA.

[1889] Guy Héraud considère par exemple qu'il « *arrive pourtant qu'une conjuration de personnes et d'intérêts accumule une force qui menace l'Etat ou le régime. Cette force peut imposer aux pouvoirs établis des décisions qui, valant officiellement comme décisions de l'Etat, seront en fait l'expression de volontés particulières. Il se peut que l'Etat devienne, comme on l'a dit, la simple résultante des féodalités modernes* », HERAUD G., « La validité juridique », *op. cit.*, p. 481.

939. Quand bien même il est d'ores et déjà possible de constater que certains géants du numérique rivalisent à certains égards avec certaines prérogatives étatiques[1890], ce pouvoir n'est pas de même nature. En effet, lorsqu'une surveillance est opérée à des fins commerciales, même si elle est problématique vis-à-vis de la vie privée, la puissance publique bénéficie d'une exorbitance légitime puisqu'elle est l'outil permettant l'autonomie des citoyens en démocratie[1891]. Mais nous imaginons mal Facebook, sur la base des renseignements dont il dispose, déployer des forces de police et sa justice pour ensuite incarcérer un individu qui contreviendrait à ses conditions générales d'utilisation. Il ne s'agit pas de nier que les acteurs privés ont, par la voie des algorithmes, des effets sur la société, mais de reconnaitre que les incidences sur les individus ne sont pas à l'heure actuelle identiques entre ces deux entités. A moins qu'ils ne soient amenés à collaborer entre eux, voire à converger, car leurs intérêts seraient communs. Il n'est donc pas possible que le droit saisisse le marché de la même façon qu'il appréhenderait l'Etat.

940. Nous avions indiqué que la constitutionnalisation du principe de transparence des traitements se devait d'être générale en ciblant aussi bien les acteurs publics que privés, car d'une part les administrations sont amenées à recourir à des algorithmes privés, ce qui implique de les contrôler, et d'autre part car l'incidence de cette source est qu'elle effectue une hiérarchisation entre différentes libertés, droits et principes, puisque nous estimons qu'ils ne peuvent tous être considérés à égalité. Cela ne veut nullement dire pour autant que la transparence applicable à l'administration serait de même nature et du même degré qu'à l'encontre des acteurs du marché. Certaines valeurs doivent effectivement primer sur d'autres, en particulier dans l'environnement numérique, et lorsque la transparence est une clé de voûte de l'ordre juridique, il convient que le secret ne puisse pas par exemple être opposé à l'Etat, justement parce qu'il est l'entité la plus légitime. Cela ne peut s'opérer qu'à la condition que suffisamment de garanties soient mises en œuvre pour que les gouvernants ne neutralisent pas le délicat équilibre institutionnel nécessaire à mettre en place[1892].

941. L'approche par la légitimité pose donc la question de la nature du contrôle. Dans le cadre de l'Etat, les personnes juridiques sont davantage susceptibles de demander des comptes à leur administration par l'intermédiaire d'un contrôle direct. La LRN a œuvré en ce sens, mais les exceptions demeurent nombreuses et ont même été accentuées au regard de l'action

[1890] PASQUALE F., From territorial to functional Sovereignty: The case of Amazon, *op. cit.*
[1891] *Supra.*, n° 634 et s.
[1892] Supra., n° 690 et s.

publique[1893]. En revanche, une transparence indirecte des opérateurs économiques effectuée par une autorité de contrôle semble plus opportune dès lors que ce travail est correctement opéré. C'est pour cela que dans le respect du droit des tiers, l'instance unique de contrôle des traitements algorithmiques que nous proposons pourra œuvrer à son effectivité, et ce en toute indépendance, notamment vis-à-vis des gouvernants.

942. Ce n'est donc pas seulement en fonction du risque d'une technique particulière ou d'un usage que l'on appréhende la nécessité de transparence, mais parce dans l'esprit de la DDHC l'administration doit rendre compte[1894], notamment car l'exercice d'une telle force implique un contrôle renforcé pour qu'elle ne soit pas le cas échéant usurpée. Quelle que soit la technique utilisée, systèmes d'IA ou non, les algorithmes doivent être expliqués à chaque personne intéressée y compris en vue de pouvoir rejouer le traitement. Et lorsqu'interviennent certains secrets protégés, dont on comprend par ailleurs l'existence, c'est à l'instance de contrôle, avec du personnel habilité, qu'il conviendra d'effectuer ce contrôle et de transmettre ensuite au public les éléments communicables. Le problème est qu'aujourd'hui la multiplication des instances de contrôle nuit à l'effectivité des réglementations. Quoi qu'il arrive, la transparence sera réalisée, même si elle n'intervient que par la voie de cette instance qui pourra attester que les grandes caractéristiques communiquées par l'administration sont véridiques, et que la situation de l'intéressé a bien été calculée. En matière de renseignement, il existe naturellement des cas où le droit d'accès à certains fichiers de données personnelles est indirect pour les intéressés également[1895], ce qui limite par ailleurs l'exercice d'autres droits, comme celui de rectification des données collectées ou traitées. Dans cette hypothèse, un recours doit permettre que l'instance vérifie ensuite la véracité des informations détenues par l'administration, que les données soient personnelles ou non. Dans l'immense majorité de cas, la transparence devra donc être directe, tandis que dans quelques rares circonstances, comme dans le domaine de la défense nationale, les traitements seront vérifiés par des spécialistes en toute indépendance pour assurer leur conformité au droit, même si elle ne pourra être effectuée par tous les acteurs de la société civile que nous avons abordés[1896]. Ce contrôle est d'autant plus nécessaire qu'il est une garantie pour l'Etat, à savoir le souverain, que l'administration et les gouvernants respectent bien le droit édicté.

[1893] Voir par exemple en ce sens les exceptions aux dispositions du CRPA dans le code de l'éducation au sujet de l'explicabilité de « *Parcoursup* » au regard des algorithmes locaux. *Supra.*, n° 468.
[1894] Art. 15 DDHC de 1789.
[1895] Certains fichiers jugés sensibles par l'Etat empêchent une consultation directe par l'intéressé. Tel est par exemple le cas des fichiers de renseignement dont la vérification va être opérée par un tiers de confiance étatique, en l'occurrence un magistrat de la CNIL. Voir en ce sens, art. 118 de la LIL de 1978 modifiée et *Supra*., n° 139 et s.
[1896] *Supra.*, n° 795 et s.

943. Toutefois, certains algorithmes privés sont également des outils utilisés pour obtenir un comportement particulier des masses, qu'il s'agisse du corps social ou des individus, le plus souvent à des fins marchandes[1897]. Dans cette approche, il n'est donc pas inenvisageable d'imposer également des obligations de transparence renforcées à certains acteurs, car les décisions prises par ces plateformes en ligne sont systémiques en ce qu'elles exercent une influence significative en matière de recommandation par exemple. Certaines règlementations s'y sont attelées, mais il convient d'aller plus loin, notamment par l'intermédiaire d'une transparence indirecte opérée par notre instance de contrôle de ces traitements et dont le secret ne lui serait pas opposable. Cela implique par conséquent que ces acteurs mettent à disposition toute la documentation permettant de comprendre le fonctionnement de ces traitements, ainsi que l'accès à ces derniers pour s'assurer de la véracité des déclarations, naturellement avec des précautions prises telles que l'intervention de médecins s'il est question de données de santé par exemple.

944. Ainsi, peu importe le concepteur ou le fournisseur du logiciel, c'est parce que le programme est utilisé par l'administration qu'il implique la transparence. C'est donc dans la définition des besoins lors des marchés publics que l'administration devra exiger des prestataires la transparence, et que toute clause contraire serait illégale. S'il s'agit d'un développement interne, le logiciel devra d'autant plus respecter ces obligations. Si la transparence ne peut être effectuée, elle le sera par le tiers de confiance public indépendant étudié[1898]. Comme nous l'avons vu[1899], il convient de considérer le logiciel comme un acte d'interprétation du droit, dont il faut assurer la publicité. La transparence a vocation à s'appliquer, et ce quand bien même il s'agit d'une aide à la prise de décision, c'est-à-dire lorsque la décision n'est pas fondée uniquement sur un algorithme. C'est pour cela que, comme nous le préconisons, une exigence de publication de rapports sur le comportement de l'administration devrait être respectée pour savoir si l'administration suit systématiquement ces recommandations[1900]. En effet, les raisonnements humains sont opaques, raison pour laquelle il existe des obligations de motivation dans certains cas, comme pour les décisions administratives individuelles. Mais dès lors qu'un outil informatique exerce des effets juridiques sur une personne ou un groupe, il est impératif qu'il soit explicité, et ce même s'il s'agit d'une aide à la prise de décision. La transparence apparaît alors comme une contrepartie

[1897] ZUBOFF S., *L'âge du capitalisme de surveillance. Le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, *op. cit.*
[1898] *Supra.*, n° 694 et s.
[1899] *Supra.*, n° 477 et s.
[1900] *Ibid.*

à la substitution d'un raisonnement humain à un calcul informatique, ne serait-ce que pour en garder le contrôle.

945. Tandis que pour l'approche privée, c'est davantage le caractère systémique, tel que le déclenchement d'un seuil, qui nous semble opportun, ce qui rejoint l'approche fondée sur les risques.

B - L'approche fondée sur les risques

946. L'approche fondée sur les risques revêt plusieurs dimensions. Cette démarche a pour objectif de faire appliquer des obligations de transparence, voire l'exclusion d'usages algorithmiques, en fonction d'une échelle de risque préalablement évaluée. L'application d'un régime juridique en fonction du risque n'est pas nouvelle puisqu'elle était déjà par exemple préconisée dans des rapports canadiens[1901] et allemands[1902], et plus récemment dans le livre blanc de la Commission européenne[1903]. Cette logique est celle retenue par le projet de règlement européen visant les « *systèmes d'intelligence artificielle* ».

947. Comme le note Cécile Crichton « *réguler une technologie dont les applications sont hétérogènes suscite une difficulté fondamentale, qui réside dans l'approche à retenir. Alors que cette approche aurait pu être sectorielle (en fonction du secteur industriel concerné) ou juridique (en fonction de la branche du droit concernée), la Commission a privilégié une troisième option déjà pressentie par ses précédents écrits : une approche fondée sur les risques* »[1904].

948. Dans le cadre de cette proposition, que nous avons fait le choix d'étudier pour mieux illustrer ce propos, car il s'agit de la plus aboutie à ce jour, les niveaux de risques sont principalement établis au regard des incidences sur les droits fondamentaux et la sécurité[1905].

[1901] GOUVERNEMENT DU CANADA, Directive on Automated Decision-Making, *tbs-sct.gc.ca* [en ligne]. 01 avril 2021 [Consulté le 22 juin 2021]. Disponible à l'adresse : https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

[1902] DATEN ETHIK KOMMISSION, Opinion of the Data Ethics Commission, *datenethikkommission.de* [en ligne]. [Consulté le 2 juin 2021]. Disponible à l'adresse : https://datenethikkommission.de/wp-content/uploads/191023_DEK_Kurzfassung_en_bf.pdf

[1903] « *Les États membres font observer l'absence actuelle d'un cadre européen commun. La commission fédérale allemande pour l'éthique des données a préconisé un système de réglementation fondé sur cinq niveaux de risque, allant d'une absence de réglementation pour les systèmes d'IA les plus inoffensifs à une interdiction totale pour les plus dangereux.* », COMMISSION EUROPEENNE, Livre blanc. Intelligence Artificielle. Une approche européenne axée sur l'excellence et la confiance, *op. cit.*, p. 12.

[1904] CRICHTON C., « Projet de règlement sur l'IA (II), une approche fondée sur les risques », *Dalloz IP/IT*, 2021.

[1905] « *La proposition s'appuie sur les cadres juridiques existants et est proportionnée et nécessaire pour atteindre ses objectifs, car elle suit une approche fondée sur les risques et n'impose des charges réglementaires que lorsqu'un système d'IA est susceptible de présenter des risques élevés pour les droits fondamentaux et la sécurité* », p. 8 du projet.

C'est donc en plus des objectifs que nous avons abordés tout au long de cette thèse par la règlementation et les techniques juridiques mises en œuvre pour y parvenir, que des nouvelles obligations de transparence vont non pas se substituer, mais s'ajouter pour poursuivre l'objectif de protection spécifique des droits et libertés, et le cas échéant de la conformité de ces systèmes à l'ordre juridique.

949. Cela nécessite donc une excellente cartographie de l'environnement numérique puisqu'à défaut aucune obligation ne s'appliquera aux acteurs[1906]. Une liste d'usage est alors établie afin de faire la distinction parmi les niveaux de cette échelle de risque. Le déclenchement de ces niveaux permettra notamment l'application particulière d'obligations relative à la transparence, et ce conformément aux outils juridiques de transparence précédemment étudiés[1907].

950. L'approche retenue peut être résumée sous forme de pyramide : à la base de cet édifice nous retrouvons les systèmes qui ne sont pas considérés comme étant à haut risque. Ils ne sont que très peu concernés par ces nouvelles obligations[1908]. Puis, plus nous nous rapprochons du sommet de cette dernière, plus le risque identifié est significatif et les obligations de transparence se renforcent[1909], voire l'usage y est strictement interdit[1910].

951. L'article 6 §1 du projet renvoie à une annexe[1911], divisée en sections, le soin de lister les domaines harmonisés au sein de l'Union et considérés comme étant à haut risque en cas de recours à une IA, mais sous conditions. Ce n'est donc pas la simple intervention d'une IA dans l'un des domaines évoqués qui justifie qu'il soit qualifié de haut risque. Sont jugés à haut risque les systèmes d'IA ayant vocation à être utilisés comme système de sécurité d'un produit ou est le produit lui-même conformément aux règlementations évoquées[1912]. Il en est de même si « *le produit dont le composant de sécurité est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une évaluation de la conformité par un tiers en vue de la mise sur le marché ou de la mise en service de ce produit conformément aux actes législatifs*

[1906] Les acteurs listés sont ceux vu précédemment, *Supra.*, n° 919.
[1907] *Supra.*, n° 961 et s.
[1908] « *Pour les systèmes d'IA qui ne sont pas à haut risque, seules des obligations de transparence très limitées sont imposées, par exemple en ce qui concerne la fourniture d'informations signalant l'utilisation d'un système d'IA lorsque celui-ci interagit avec des humains* », p. 8 du projet.
[1909] « *Pour les systèmes d'IA à haut risque, les exigences en matière de données de haute qualité, de documentation, de traçabilité, de transparence, de contrôle humain, d'exactitude et de robustesse se limitent au strict nécessaire pour atténuer les risques pour les droits fondamentaux et la sécurité qui sont associés à l'IA et qui ne sont pas couverts par d'autres cadres juridiques existants », ibid.*
[1910] Nous aborderons en détail l'interdiction stricte des usages plus tardivement. *Infra.*, n° 953 et s.
[1911] Annexe II du projet.
[1912] *Ibid.*, (a).

d'harmonisation de l'Union énumérés à l'annexe II »[1913]. Sont concernés ceux qui relèvent du champ d'application de la règlementation « *machines* », de la sécurité des jouets, des bateaux de plaisance et des véhicules nautiques à moteur, des ascenseurs ainsi que leurs composants de sécurité, les appareils et systèmes utilisés en atmosphères explosibles, la mise sur le marché d'équipement radioélectrique et d'équipement sous pression, les installations à câbles, les équipements de protection individuelle, les appareils à gaz, les dispositifs médicaux et de diagnostic *in vitro* (Section A). Quant à la section B de l'annexe, elle renvoie à l'aviation civile avec notamment la conception des aéronefs, y compris ceux sans pilote, les véhicules terrestres deux, trois roues ainsi que les quadricycles, les véhicules terrestres agricoles et forestiers, les équipements marins, le système ferroviaire, les véhicules terrestres à moteurs et les systèmes afférents.

952. Quant à l'article 6 § 2, il renvoie à une annexe énumérant des domaines dans lesquels le simple usage d'un système d'IA est suffisant à le qualifier de « à haut risque », est donc indifférent que ces algorithmes interviennent dans un composant de sécurité par exemple. Ces domaines sont si sensibles que le fournisseur ou son mandataire a pour obligation d'enregistrer le système d'IA dans une base de données prévue par l'Union européenne[1914]. Nous y retrouvons les systèmes biométriques et la catégorisation des personnes, tels que la reconnaissance faciale, que le traitement ait par ailleurs lieu en temps réel ou *a posteriori*[1915] ; La gestion et l'exploitation des infrastructure critiques[1916] ; l'éducation et la formation professionnelle[1917] ; les relations entre l'employeur et les salariés ainsi que l'accès au travail indépendant[1918] ; l'accès et l'utilisation des services publics et privés considérés comme essentiels[1919] et ce qui se réfère à l'application de la loi[1920] ; mais aussi à la gestion de l'immigration, de l'asile et du contrôle aux frontières[1921]. Pour finir, l'administration de la justice et des processus démocratiques figurent également dans cette liste, toutefois seuls les systèmes assistant l'autorité judiciaire aussi bien dans la recherche que dans l'application du droit aux faits[1922] sont pour l'heure visés par des obligations de transparence. La commission

[1913] *Ibid*., (b).
[1914] Art. 51 du projet.
[1915] Annexe III § 1.
[1916] *Ibid*., § 2.
[1917] *Ibid*., § 3.
[1918] *Ibid*., § 4.
[1919] *Ibid*., § 5.
[1920] *Ibid*., § 6.
[1921] *Ibid*., § 7.
[1922] *Ibid*., § 8.

se réserve néanmoins la possibilité de modifier spécifiquement cette annexe par des actes délégués[1923].

953. La proposition aborde également pour l'heure quatre cas d'usages en matière d'IA faisant l'objet d'une stricte interdiction[1924]. Tel est le cas des systèmes qui mettraient en œuvre des techniques subliminales ayant pour conséquence de modifier le comportement d'une personne physique qui cause ou est susceptible de causer, y compris à un tiers, un préjudice physique ou psychologique[1925]. Il en est de même si le système utilise les vulnérabilités d'un groupe de personnes en raison de leur âge ou de leur handicap, « *pour altérer substantiellement le comportement d'un membre de ce groupe d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique* »[1926]. Est également exclu de la mise sur le marché ou pour le compte d'un Etat, un système de crédit social, comme instauré en République Populaire de Chine[1927]. Le dernier usage évoqué est toutefois soumis à des exceptions puisque sont prohibés par principe les traitements d'identification biométriques effectués au sein de l'espace public[1928], sauf s'ils permettent de rechercher des potentielles victimes de la criminalité ou des enfants disparus[1929], de prévenir des menaces substantielles et imminentes pour la vie ou la sécurité des personnes, y compris en matière d'attaque terroriste[1930], ainsi que la détection, la localisation ou la poursuite d'auteurs ou de suspects de certaines infractions pénales[1931]. Ces exceptions ne peuvent toutefois être mises en œuvre, sauf urgence, que sous certaines conditions telle que l'autorisation d'une autorité administrative indépendante ou de l'autorité judiciaire[1932] dans les modalités définies par le droit national[1933].

954. Il est à noter que certaines technologies peuvent notamment faire l'objet d'un régime juridique spécifique. Telle est aussi l'approche du projet de règlement européen[1934], mais à la marge de sa logique générale précédemment abordée. C'est donc parce qu'une technologie en particulier est jugée sensible qu'un régime juridique de transparence renforcée va s'appliquer en supplément des obligations déjà prévues au titre III du règlement[1935], et ce quand bien même

[1923] Dans les conditions prévues à l'art. 7 du projet.
[1924] Art. 5 du projet.
[1925] *Ibid*., § 1 (a).
[1926] *Ibid*., (b).
[1927] *Ibid*., (c).
[1928] *Ibid*., (d).
[1929] *Ibid*., i.
[1930] *Ibid*., ii.
[1931] *Ibid*., iii.
[1932] Art. 5 § 3.
[1933] Art. 5 § 4.
[1934] Art. 52.
[1935] *Supra.*, n° 951 et s.

le domaine est à faible risque. En ce sens, l'article 52 évoque précisément une transparence spécifique sauf exception[1936] pour certaines méthodes d'IA, à savoir les systèmes interagissant avec les personnes physiques (bot)[1937], les dispositifs de reconnaissance biométrique comportant la reconnaissance d'émotions[1938] ou portant sur « *des images ou des contenus audio ou vidéo présentant une ressemblance avec des personnes, des objets, des lieux ou d'autres entités ou événements existants et pouvant être perçus à tort comme authentiques ou véridiques (« hypertrucage »)* »[1939]. Néanmoins, de nombreuses exceptions sont à relever. Dans l'hypothèse de la reconnaissance biométrique, si elle est utilisée « *à des fins de prévention et de détection des infractions pénales et d'enquêtes* », l'obligation d'information du fonctionnement dudit systèmes aux personnes exposées n'est pas applicable[1940]. Dans son avis, le CEPD considère à cet égard que de telles exceptions pour des systèmes à haut risque sont trop larges en plus de constituer une incitation à l'usage[1941]. Le Comité se prononce par ailleurs pour l'interdiction de la reconnaissance d'émotions qu'elle juge trop intrusive sauf à des fins de santé ou de recherche[1942].

955. Il s'agit donc finalement d'une régulation du marché qui ne prend pas en considération de nombreux domaines très sensibles comme la défense ou la sécurité nationale puisqu'ils demeurent de la compétence des Etats, ce qui démontre par ailleurs que l'Union européenne, sous sa forme actuelle, ne pourra convenablement réguler de tels usages, alors que, par exemple, les droits et libertés pourraient être fortement impactés par de tels systèmes.

956. De plus, à l'instar des règlementations européennes étudiées dans le cadre de ces travaux comme le RGPD, les exceptions demeurent nombreuses[1943], notamment car le libéralisme économique prime dans certains cas sur les obligations de transparence[1944]. Or, que la

[1936] En ce sens, voir art. 52.
[1937] *Ibid*., § 1.
[1938] *Ibid*., § 2 du projet.
[1939] Art. 52 § 3.
[1940] Art. 52 § 2.
[1941] EDPB-EDPS, Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *op. cit*., § 70.
[1942] *Ibid*., § 35.
[1943] *Ibid*.
[1944] « *Les obligations en matière de renforcement de la transparence ne porteront pas non plus atteinte de manière disproportionnée au droit à la protection de la propriété intellectuelle (article 17, paragraphe 2), puisqu'elles seront limitées aux informations strictement nécessaires pour permettre aux personnes d'exercer leur droit à un recours effectif et à la transparence requise de la part des autorités de contrôle et d'exécution, conformément à leurs mandats. Toute divulgation d'informations sera effectuée conformément à la législation en vigueur dans le domaine concerné, notamment la directive 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites. Lorsque les autorités publiques et les organismes notifiés doivent avoir accès à des informations confidentielles ou à un code source pour vérifier le respect d'obligations essentielles, ils sont soumis à des obligations de confidentialité contraignantes* », p. 13 du projet.

transparence soit effectuée directement vis-à-vis des personnes[1945] ou indirectement par l'intermédiaire d'un tiers de confiance, cela affecte ses chances de constater l'ampleur de la violation de ses droits. La proposition de règlement n'aborde pas la qualité ou la nature de l'information que les autorités de contrôle vont effectuer auprès du public[1946]. Quand bien même il existe une transparence minimale pour que les personnes puissent exercer leur droit à un recours effectif, il convient de reconnaître que nous aurions préféré que ce soit à l'autorité de contrôle d'établir ce qui est à considérer comme minimal, et non à l'acteur soumis à ces obligations de les apprécier. Il est en effet tentant pour le débiteur de ces obligations d'occulter certaines informations pour éviter d'éventuelles poursuites, même si l'autorité de contrôle pourra *a posteriori* confronter ces éléments et infliger le cas échéant des sanctions. Mais encore faut-il que ces autorités bénéficient des moyens suffisants pour y parvenir.

957. La transparence des traitements est la clé de voûte du respect des droits et libertés, et donc la condition *sine qua non* du déploiement sans risque de ces systèmes. Mais ce principe ne peut être une fin en soi car d'une part, quand bien même un usage est entièrement expliqué et contrôlé, le recours à la technologie n'en demeure pas moins problématique, ne serait-ce que parce que la transparence permet surtout de constater la nature du fait juridique afin de le soumettre ensuite au régime juridique adéquat. Et d'autre part, de manière paradoxale, un système opaque, utilisé dans un secteur dont l'usage n'a potentiellement que très peu d'incidences juridiques, ne nécessite pas d'exigence de clarté particulière.

958. Il s'agit donc d'une ambivalence à corriger. En ce sens, l'approche par le risque est intéressante sans être irréprochable. C'est pour cette raison qu'il convient d'interdire certains usages et de combiner les différentes approches étudiées, ce que ne parvient pas suffisamment à effectuer le projet de règlement à notre sens.

SECTION 2 - LES LIMITES AU PRINCIPE DE TRANSPARENCE DES TRAITEMENTS ALGORITHMIQUES

959. Bien que le principe de transparence des traitements algorithmiques soit essentiel pour les raisons évoquées tout au long de ces travaux, force est de reconnaître qu'il ne saurait

[1945] Art. 70 et art. 17 § 2 du projet.

[1946] En effet, le CEPD précise dans son avis sur la proposition de règlement que lorsque le secret s'oppose à une communication directe de certaines informations, ces systèmes doivent faire l'objet d'une inscription particulière dans un registre afin qu'ils puissent être surveillés par une autorité de contrôle compétente pour assurer sa transparence. Voir en ce sens, EDPB-EDPS, Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *op. cit.*, § 71.

résoudre toutes les difficultés inhérentes au numérique. L'objectif primaire de la transparence est l'observation des faits juridiques induits par le numérique en prenant connaissance du positionnement des puissances au sein de cyberespace, afin de saisir notamment l'étendue des violations des droits et libertés. Mais son accomplissement ne peut légitimer à lui seul le recours à des technologies. Ce n'est donc pas parce qu'une technologie serait à la fois transparente d'un point de vue juridique que technique qu'il devrait en légitimer l'usage.

960. Nous nous efforçons cependant de proposer une classification générale relative à la transparence des traitements et à l'exclusion des traitements (Paragraphe 1), sans négliger qu'au-delà de la réforme institutionnelle proposée censée restaurer l'équilibre des pouvoirs dans un monde de plus en plus numérique[1947], le principe de transparence se doit d'être complété par un principe de participation des citoyens aux décisions numériques (Paragraphe 2).

PARAGRAPHE 1 - Essai de classification générale relative à la transparence et l'exclusion des traitements

961. Comme nous l'avons vu, la régulation des traitements algorithmiques peut s'opérer par des approches relatives aux risques ou à la légitimité[1948]. Mais le projet de règlement européen, qui est par ailleurs la première règlementation à aborder l'approche par le risque en la matière, comporte une importante lacune ; à savoir la volonté de réguler avant tout le marché en se souciant assez peu des risques engendrés par les usages algorithmiques de la puissance publique. Cette ambition européenne ne peut donc en l'état être pleinement satisfaisante puisqu'elle fait fi de l'approche par la légitimité. En effet, la puissance de l'Etat ne peut être appréhendée de la même manière que les puissances privées[1949]. Nous ne reviendrons cependant pas en détail sur la régulation du marché, déjà longuement détaillée et opérée dans l'étude du projet de règlement européen.

962. La combinaison de l'approche par la légitimité et le risque nous impose par conséquent deux régimes juridiques distincts. D'une part, il convient donc de convenir d'une approche par le risque pour le marché, et d'autre part, pour la puissance publique. Dans cette hypothèse, il est opportun de se focaliser sur un régime spécifique de transparence pour l'action publique, ce que ne prend pas en compte le projet de règlement (A) et de l'autre une réflexion plus

[1947] *Supra.*, n° 690 et s.
[1948] *Supra.*, n° 937 et s.
[1949] *Supra.*, n° 613 et s.

approfondie au sujet de l'exclusion de certains usages (B), car quand bien même la transparence serait absolue, elle n'a pas vocation à légitimer des technologies liberticides.

A - De la nécessaire transparence spécifique à l'action publique

963. L'approche par le risque ne peut être générique. En effet, des exclusions ou des obligations de transparence accrues peuvent avoir lieu dans l'administration et non dans le secteur privé, ce que ne fait pas le règlement européen. Il conviendrait donc davantage de réaliser deux pyramides, c'est-à-dire un risque établi en fonction de la légitimité de la puissance de l'Etat qui de fait engendre un risque sur les individus et groupes, et une autre correspondant au marché telle que proposée par la Commission.

964. Il serait intéressant à notre sens de préciser davantage l'approche par le risque dans le cadre spécifique de l'action administrative puisque ce n'est pas celle explorée par le projet de règlement. Dans une approche sectorielle, contrairement au projet de règlement européen qui se veut général, un rapport de l'ENA avait déjà évoqué une démarche spécifique par le risque en matière d'« *éthique et de responsabilité des algorithmes publics* »[1950], proposition que nous souhaitons combiner par une approche par la légitimité. Et c'est aussi la raison pour laquelle certains auteurs, comme Jean-François Kerléo, se prononcent en faveur de la constitutionnalisation d'un principe de transparence de la vie publique[1951].

965. Nous considérons pour les raisons évoquées que la transparence directe doit être privilégiée vis-à-vis de l'Etat, et ce quel que soit le risque sur les droits et libertés ou la société en général, car son action est légitimée par la poursuite de l'intérêt général et parce qu'il est de ce fait susceptible de recourir à des décisions s'imposant aux administrés et directement exécutoires. Il convient donc que cette transparence soit du plus haut degré, surtout lorsqu'il y a usage de prérogatives de puissance publique, comme pour les collectes et les traitements de données obligatoires, mais ce dans le respect de la vie privée des tiers. A minima, le caractère indirect de la transparence implique que notre commission unique est tenue et habilitée à vérifier les informations déclarées par l'administration. C'est effectivement parce que la

[1950] RAPPORT ENA, Ethique et responsabilité des algorithmes publics, annexe 3, p. 30, *Etalab.gouv.fr* [en ligne]. Juin 2019. [Consulté le 12 décembre 2020]. Disponible à l'adresse : https://www.etalab.gouv.fr/wp-content/uploads/2020/01/Rapport-ENA-Ethique-et-responsabilit%C3%A9-des-algorithmes-publics.pdf
[1951] Voir en ce sens, KERLEO J-F., « La constitutionnalisation d'un principe de transparence de la vie publique », *ADJA*, 2020. *Supra.*, n° 675.

puissance de l'Etat légitime de tels traitements qu'il est impératif d'attendre en retour des garanties de transparence.

966. Dans les hypothèses où une transparence directe s'opérerait, les personnes concernées ou la société, par l'intermédiaire de la société civile, pourraient accéder au code source, à la documentation afférente, et pourraient solliciter l'autorité de contrôle pour qu'elle s'assure que le code source communiqué est par exemple conforme au logiciel utilisé par l'administration. Les systèmes les plus risqués exigeraient des autorisations pour leur déploiement, y compris dans certains cas une consultation démocratique voire un scrutin, des audits réguliers et la tenue de la conservation de registre pour une meilleure effectivité des contrôles.

967. Dans la continuité de la jurisprudence du Conseil constitutionnel[1952], lorsqu'une décision automatisée administrative individuelle fait intervenir des technologies auto-apprenantes et a des effets juridiques sur les personnes, est imposée l'explication de toutes les étapes du traitement, de façon à ce que le responsable du traitement soit en mesure de le vérifier. Il est par ailleurs impératif d'aller plus loin au sujet de la transparence des traitements ne faisant pas intervenir de données personnelles, ou des données anonymisées, puisqu'elles sont susceptibles d'exercer une influence sur la prise de décision. Le rapport Tricot déclarait dès 1975 lorsqu'il se penchait sur une réglementation des données personnelles *« que nous serons sans doute amenés à nous interroger sur la possibilité et l'intérêt de consacrer d'autres libertés, telles que celles pour l'homme et les groupements de connaître les informations enregistrées à leur sujet et de pouvoir les discuter* »[1953].

968. C'est pour cette raison que nous préconisions que l'administration communique obligatoirement, sous forme de rapport annuel, des statistiques sur ces outils de recommandation, qui certes ne prennent pas de décision, mais sont susceptibles d'influencer l'agent administratif dans son jugement. S'il s'avère que la recommandation est suivie dans l'immense majorité des cas, l'agent ne pourrait pas faire écran vis-à-vis de l'algorithme, ce qui permettrait également de contester l'algorithme, dans le cadre d'un contrôle de légalité par exemple.

969. De la même manière, lorsque l'Etat ou ses représentants utilisent des technologies ayant des incidences sur les libertés ou la société, et donc pouvant desservir les intérêts de la Nation,

[1952] CC, décision n° 2018-765 DC, 12 juin 2018, Loi relative à la protection des données personnelles, § 70 et § 71.
[1953] Rapport de la Commission informatique et libertés, la documentation française, 1975, p. 20.

ils doivent être dans l'obligation de solliciter une transparence vis-à-vis du fournisseur notamment pour pallier les potentielles vulnérabilités à leur encontre[1954]. En effet, ses services, et le cas échéant avec l'aide du tiers de confiance que nous avons souhaité instituer, seraient tenus d'évaluer les caractéristiques et les données utilisées par le système. Tel serait particulièrement le cas des logiciels utilisés en matière d'exploration des données lors de grandes consultations de nature politique, et qui ont ensuite des conséquences juridiques, ou celles qui relèveraient de prédictions comme dans le cadre d'une pandémie ou des outils de *trading* qui peuvent affecter l'économie d'une nation, voire de l'humanité[1955]. Il en est de même lorsque les algorithmes jouent un rôle en matière d'évaluation des politiques publiques, puisque s'ils sont erronés ou parcellaires dans les modélisations utilisées, ils sont susceptibles de mettre fin à tort à certaines politiques au nom d'une prétendue « scientificité ». En effet, en informatique, ce qui n'est pas dans le modèle algorithmique est hors modèle et ne pourra donc être pris en compte. Il convient de démontrer que certains outils présentés comme impartiaux ne sont autre que des impostures.

970. Concernant la participation à la vie démocratique, nous rejoignons la prise de position de Eric Buge et Camille Morio disposant que « (…) *La sincérité implique notamment, en matière de décision publique, la reconnaissance d'un principe de transparence. Cette dernière concerne les modalités de la consultation, qui doivent être publiquement explicitées. Elle doit aussi porter sur ses résultats, qui appartiennent tant au commanditaire de la consultation qu'au public qui y a participé. Un principe d'open data est donc à affirmer. Enfin, s'agissant spécifiquement des plateformes numériques utilisées par les pouvoirs publics, la garantie minimale voudrait que, dans un domaine qui touche à l'exercice de la démocratie, les algorithmes sous-jacents (codes source) soient accessibles et étudiables, c'est-à-dire publiés en open source* »[1956]. Il est aussi nécessaire que des missions de surveillance diligentées par notre autorité de contrôle indépendante soit chargée de vérifier leur analyse, y compris quand cette tâche est déléguée à des personnes privées comme cela a été cas dans le cadre du grand débat[1957]. Parallèlement, et à titre préventif, cette approche par les risques et sur le fondement de la légitimité devrait nous amener, comme le préconise le défenseur des droits, à « *réviser le seuil d'évaluation des marchés publics informatiques et d'intégrer à leur contrôle au-delà des*

[1954] DOUVILLE T., HERVOCHON C., NOEL E., PAQUIER Y., « Les vulnérabilités numériques », *op. cit.*, p. 117.
[1955] AÏT-KACIMI N., Trading : les « robots » rechignent à livrer leurs secrets au régulateur, *Les Echos* [en ligne]. 14 novembre 2019. [Consulté le 26 février 2020]. Disponible à l'adresse : https://www.lesechos.fr/finance-marches/marches-financiers/les-robots-rechignent-a-livrer-leurs-secrets-au-regulateur-1147749
[1956] Voir en ce sens, BUGE E., MORIO C., « Le Grand débat national, apports et limites pour la participation citoyenne », *op. cit.*, p. 1205.
[1957] *Supra.*, n° 487 et s.

seuls aspects budgétaires, une appréciation des risques de discrimination, et plus généralement d'atteinte aux libertés et droits fondamentaux »[1958].

971. Quant à la transparence des traitements du marché à laquelle il est moins question de s'étendre car le règlement européen y consacre un régime juridique complet, il convient davantage de la considérer de manière indirecte vis-à-vis des personnes, à la condition que le contrôle étatique soit suffisant. Cela n'empêche nullement, comme dans le cadre du règlement européen, qu'une transparence d'une autre nature, c'est-à-dire faisant référence davantage à l'intelligibilité, à l'explication des principales caractéristiques, soit opérée vis-à-vis des personnes, qu'elles soient physiques ou morales dès lors que ces informations sont vérifiées par ledit tiers de confiance. Dans le cadre de la régulation du marché, la nature et le degré de transparence en fonction des usages nous semblent être une assez bonne avancée, raison pour laquelle nous n'y reviendrons pas dès lors que le tiers de confiance institué est fiable et lui-même transparent sur les missions qu'il effectue[1959].

972. Mais la transparence ne saurait justifier pour autant tous les usages technologiques. Ce principe ne peut faire l'impasse sur l'acceptabilité, ne serait-ce que parce que sa raison d'être juridique est de pouvoir observer le positionnement des puissances. En ce sens, il est la clé de voûte de l'ordre juridique et participe notamment à assurer la publicité des normes étatiques et privées. La crainte est donc de constater que ce principe est utilisé à d'autres fins, dont celle de légitimation d'un usage attentatoire aux libertés. La transparence n'est là que pour s'efforcer à comprendre le fonctionnement de ces outils.

973. Ainsi, au-delà de la transparence, l'acceptation d'une technologie peut être subordonnée à des conditions particulières, ou à défaut à une stricte exclusion d'un usage.

B - Conditionnalité et exclusion ferme des traitements algorithmiques

974. Quand bien même la transparence de ces systèmes serait absolue, certains usages algorithmiques doivent soit faire l'objet de garanties particulières, soit d'une exclusion. Ce que

[1958] DEFENSEUR DES DROITS, Rapport, Technologies biométriques : l'impératif respect des droits fondamentaux, 2021, p.19.
[1959] *« Le ministre de l'Intérieur a tenté, fin 2020, d'échapper à une sanction de la Cnil qui enquêtait sur cette surveillance illégale. Il a surtout réclamé que cette sanction, une fois prononcée, soit dissimulée aux citoyens et aux parlementaires. »*, LE FOLL C., POURE C., Drones : comment Gérald Darmanin a voulu échapper à toute sanction, *Mediapart* [en ligne]. 8 mai 2021 [Consulté le 2 juin 2021]. Disponible à l'adresse : https://www.mediapart.fr/journal/france/080521/drones-comment-gerald-darmanin-voulu-echapper-toute-sanction

nous appelons conditionnalité est l'acceptation d'un usage sous réserve qu'il remplisse des garanties autres qu'en matière de transparence. Mais cela implique une excellente connaissance de la technologie utilisée afin de s'assurer que dans les faits, elle respecte les objectifs fixés en démocratie. A titre d'exemple, une architecture technique ou un design logiciel serait autorisé parce qu'il est plus respectueux de l'environnement qu'un autre[1960]. Il pourrait s'agir également d'autoriser le recours à des algorithmes dès lors qu'il existe un interlocuteur humain, comme en matière d'accès à un service public. En d'autres termes, il ne serait pas possible qu'une administration dématérialise exclusivement toutes ses procédures ou l'accueil du public. La conditionnalité peut aussi impliquer qu'un usage soit autorisé à la seule modalité qu'il s'agit d'une gestion purement publique, voire nécessitant le recours à des logiciels libres et ouverts. Tel serait le cas d'une plateforme publique offrant plus de garantie qu'une gestion privée comme cela est actuellement le cas avec le « *Health data hub* »[1961], car au-delà des impératifs de transparence, c'est prendre le risque que des données ne soient transmises à d'autres opérateurs à des fins commerciales, et ce même illicitement.

975. Il en est de même dans le cadre du renseignement où de nombreux logiciels privés américains sont utilisés et détournés en tant que cheval de Troie. Le logiciel libre utilisé par l'Etat, même s'il est parfois moins efficace, offre au moins une meilleure compréhension de ce dernier et il garantit qu'il ne sera pas détourné à d'autres fins, car rappelons-le, l'univers numérique n'est pas si facilement observable techniquement. Le logiciel est une partie importante en matière de souveraineté, mais il convient également de considérer que dans des domaines très particuliers, car sensibles, il est préférable de conditionner notamment un usage par le recours à un matériel informatique conçu et produit en France. Puisque comme nous l'avons déjà abordé[1962], le traitement algorithmique implique l'exécution d'un code source par un ordinateur qui lui-même est susceptible de contourner le logiciel, aussi transparent soit-il. En ce sens, certains usages doivent donc être subordonnés à des garanties de bout en bout, de la conception du logiciel à celle de l'ordinateur.

976. Quant à l'exclusion, elle doit parfois être stricte du fait du domaine d'intervention ou en fonction de la technologie utilisée, car l'usage ne peut, du fait de sa nature, offrir des garanties suffisantes et engendre un risque trop important sur la société et les libertés. L'exclusion des usages algorithmiques n'est pas une approche nouvelle. L'étude des premiers régimes

[1960] MATHIS B., « Faut-il réglementer les crypto-actifs en fonction de leur consommation d'électricité », *Revue internationale des services financiers*, 2020, p. 59 à 62.
[1961] Pour plus de précisions au sujet du « *Health data hub* », *Supra.*, n° 631 et s.
[1962] *Supra.*, n° 13.

juridiques nous apprend, comme dans de nombreux domaines, que la LIL de 1978 prévoyait, qu'au-delà de la transparence des traitements tel que le droit d'accès à ses données nominatives, certains usages devaient toutefois être prohibés. L'article 2 de la LIL[1963] disposait dès 1978 qu'« *aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir lieu pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité* ».

977. Il en était de même concernant les décisions administratives ou privées prises sur le fondement d'un profilage opéré par un traitement automatisé[1964]. Mais la tentation du recours à l'informatique, y compris pour combler la faiblesse de moyens matériels et humains, a conduit à ce que des systèmes automatisés privés ou publics puissent s'y substituer, sous réserve d'une certaine transparence[1965], comme si cette dernière légitimait à elle seule l'usage autrefois interdit pour des motifs de préservation des droits et libertés.

978. Il apparait donc, que compte tenu des nouvelles technologies pourtant parfois séduisantes, il faille recourir davantage à l'interdiction de certains usages. Le projet de règlement européen esquisse cette éventualité, mais manque à notre sens d'ambition, surtout concernant l'exclusion des usages relatifs à la vie démocratique ou à l'action administrative, sans doute car l'approche par la légitimité n'a pas été combinée avec celle par les risques. Et comme nous l'avons abordé, l'approche fondée sur les risques nécessite une excellente cartographie des domaines d'intervention des traitements algorithmiques, ce qui peine à être satisfaisant dans le projet de la Commission. L'avis du CEPD sur ladite proposition évoque de plus à juste titre que l'information est difficile à apporter quant aux systèmes d'IA et qu'il conviendrait davantage de « *promouvoir de nouvelles manières plus proactives et opportunes d'informer les utilisateurs des systèmes d'IA du statut (de décision) dans lequel se trouve le système à tout moment, en les avertissant rapidement des conséquences potentiellement néfastes, de sorte que les personnes dont les droits et libertés peuvent être altérés par les décisions autonomes de la machine peuvent réagir, ou redresser la décision* »[1966]. La transparence n'est toutefois pas uniquement qu'une question de volonté, mais aussi de

[1963] Art. 47 modifié et art. 2 ancien de la LIL de 1978.
[1964] Art. 2 ancien de la LIL de 1978.
[1965] Art. 42 al. 2 de la LIL de 1978 modifiée. Voir également en ce sens, CC, décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*, § 70 et § 71. Pour plus de précisions, *Supra.*, n° 435 et s.
[1966] Traduit de l'anglais, « *The Regulation should promote new, more proactive and timely ways to inform users of AI systems on the (decision-making) status where the system lays at any time, providing early warning of potential harmful outcomes, so that individuals whose right and freedoms may be impaired by machine's autonomous decisions may react, or redress the decision* », EDPB-EDPS, Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *op. cit.*, § 72.

faisabilité technique. A l'évidence puisque l'immixtion de ces technologies dans des usages trop sensibles ne saurait offrir des garanties suffisantes de transparence et de respect des exigences démocratiques en général, leur exclusion est nécessaire dans de nombreux domaines.

979. Il est également possible de trouver trace dans le code pénal de pratiques répréhensibles, car fondées sur la collecte de données non seulement personnelles mais pluripersonnelles tels que les tests génétiques récréatifs[1967]. C'est la dimension collective de la collecte et du traitement qui est dangereuse et justifie son interdiction. En effet, la collecte d'un ADN n'engage pas seulement la personne concernée, puisqu'elle permet notamment l'identification de plusieurs individus, voire d'un groupe ethnique, sans que ces derniers n'aient à donner leur consentement[1968]. De plus, le traitement illicite d'une telle information serait irréversible en ce que nous ne pouvons modifier notre ADN contrairement à des données d'une autre nature tels qu'un numéro de téléphone ou une adresse postale.

980. L'immixtion des algorithmes dans le cadre de la prévention des atteintes à l'ordre public ou à la recherche des auteurs d'infractions est par ailleurs un domaine très sensible. A titre d'exemple, le caractère systémique de la surveillance des télécommunications opérée par ces nouveaux outils laisse à penser que le glissement d'une surveillance de masse vers une surveillance généralisée relève davantage d'une simple différence de degré que de nature. Sans surprise, la Cour EDH ne s'oppose pas à une telle surveillance de masse au motif qu'il y aurait une prolifération des menaces, notamment permis par l'environnement numérique[1969]. Au nom des marges d'appréciation des Etats, l'absence de contrôle de nécessité ouvre la voie à des usages liberticides, et ce quand bien même des garanties seraient posées par l'intermédiaire d'un contrôle de proportionnalité[1970]. Or, c'est la nature de ces techniques qui les rend intrusives, ces outils n'étant pas neutres, puisqu'ils sont conçus pour détecter un très grand nombre de données sans le moindre discernement. Certes, il est possible de penser des garanties

[1967] L'article L. 226-28-1 du Code pénal dispose que « *Le fait, pour une personne, de solliciter l'examen de ses caractéristiques génétiques ou de celles d'un tiers ou l'identification d'une personne par ses empreintes génétiques en dehors des conditions prévues par la loi est puni de 3 750 € d'amende* ».

[1968] CHATELLLIER R., Des tests génétiques dits récréatifs, mais pas inoffensifs, *Linc.cnil.fr* [en ligne]. 13 septembre 2018. [Consulté le 2 octobre 2020]. Disponible à l'adresse : https://linc.cnil.fr/fr/des-tests-genetiques-dits-recreatifs-mais-pas-inoffensifs#:~:text=En%20France%2C%20ce%20type%20de,'un%20tiers%2C%20ou%20l'

[1969] Cour EDH, Big brother watch Ru, et Centrum för rättvisa c. Suède, 25 mai 2021. Point 347 *« Certes, l'article 8 de la Convention n'interdit pas de recourir à l'interception en masse afin de protéger la sécurité nationale ou d' autres intérêts nationaux essentiels contre des menaces extérieures graves, et les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de régime d'interception ils ont besoin à cet effet, cependant la latitude qui leur est accordée pour la mise en œuvre de ce régime doit être plus restreinte et un certain nombre de garanties doivent être mises en place.* ». Voir également au plan national, CE, Ass, 21 avril 2021 req. n° 393099, 394922, 397844, 397851, 424717, 424718 ; DUBOUT E., « Le Conseil d'Etat, gardien de la sécurité », *RDLF*, 2021, chron. n° 18, *Revuedlf.com* [en ligne] [Consulté le 23 avril 2021]. Disponible à l'adresse : http://www.revuedlf.com/droit-ue/le-conseil-detat-gardien-de-la-securite/

[1970] SIZAIRE V., « L'art du trompe l'œil », *La Revue des Droits de l'Homme*, [en ligne]. Septembre 2021 [Consulté le 22 septembre 2021]. Disponible à l'adresse : https://journals.openedition.org/revdh/12968#abstract.

sur la procédure de déploiement de ces outils, mais nullement sur le traitement lui-même, dans la mesure où ils progressent sans la connaissance de notre tradition juridique.

981. Ce risque de généralisation de la surveillance même au-delà de circonstances exceptionnelles a également été soulevé lors de l'urgence sanitaire par la CNIL, craignant un effet cliquet[1971]. D'une part concernant le déploiement de « vidéos intelligentes »[1972] pour mesurer le port du masque dans les transports, et d'autre part au sujet du recours au « passe sanitaire » [1973]. Elle a en ce sens indiqué pour la vidéo intelligente que « *même s'il est limité au cadre de l'état d'urgence sanitaire, un tel déploiement présente le risque réel de généraliser un sentiment de surveillance chez les citoyens, de créer un phénomène d'accoutumance et de banalisation de technologies intrusives et, en définitive, d'engendrer une surveillance accrue* », tandis que pour le « passe sanitaire », l'accoutumance et une banalisation pourraient aboutir à ce que de plus en plus de lieux, tels que l'accès au cinéma, seraient conditionnés à sa présentation, ce qui a finalement été le cas[1974]. Par ailleurs, la modification de la finalité d'un traitement à des fins liberticides apparaît aisée avec le temps.

982. D'autres techniques, telle que la reconnaissance faciale, traitent les données biométriques des personnes comme si elles étaient suspectes, parfois sur de simples émotions[1975] et ce sans le moindre soupçon raisonnable. Le fait de scanner des visages rend chaque individu présumé suspect, en plus de la collecte et du traitement d'un gabarit biométrique intrusif sans leur consentement. Il s'agit d'une automatisation de la suspicion, ayant par ailleurs des incidences sur l'exercice des autres libertés comme la liberté d'expression ou de manifestation[1976]. On a donc du mal à comprendre que la reconnaissance faciale soit interdite par principe sur le fondement du risque dans le projet de la Commission européenne alors qu'elle est autorisée par voie d'exception pour les usages les plus intrusifs tels que le maintien de l'ordre public[1977]. Les lignes directrices du Conseil de l'Europe sont à cet égard

[1971] Ce terme ne doit pas être appréhendé conformément à la jurisprudence du conseil constitutionnel, mais dans l'acception qu'une technologie, une fois déployée, a tendance à se pérenniser.
[1972] CNIL, Délibération n° 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports
[1973] CNIL, Délibération n° 2021-024 du 12 mai 2021 portant avis sur le projet de mise en place d'un passe sanitaire conditionnant l'accès à certains lieux, évènements ou établissements impliquant de grands rassemblements de personnes. Voir également en ce sens, délibération n° 2021-097 du 6 août 2021 portant avis sur un projet de décret modifiant le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire et le décret n° 2021-901 du 6 juillet 2021 relatif au traitement automatisé de données à caractère personnel dénommé « Convertisseur de certificats ».
[1974] Loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire, art. 1.
[1975] SIRINELLI P., PREVOST S., « Reconnaissance émotionnelle, connaissance irrationnelle ? », *Dalloz IP/IT*, 2021, p. 237.
[1976] Un sondage a révélé au Royaume-Uni que parmi les 16-24 ans interrogés, 38% ont déclaré « qu'ils éviteraient de participer à une manifestation si la police y utilisait la reconnaissance faciale. », DUCOURTIEUX C., « Le Royaume-Uni, champion de la reconnaissance faciale », *Le Monde*, 4 septembre 2019.
[1977] Art. 5 du projet de règlement.

bien plus protectrices puisque dans la prolongation de la convention 108+ il se prononce en faveur de l'interdiction de la reconnaissance comportementale et émotionnelle[1978] à l'inverse de la commission qui conditionne son usage à une transparence accrue[1979].

983. Il existe d'ailleurs une éventualité pour que ces outils soient un jour performants en plus d'être transparents, ce qui légitimerait leur usage sur le fondement de la seule problématique de transparence. Ainsi, le seul rempart contre des technologies liberticides ne peut qu'être l'exclusion. Ces outils sont autant de tentations à l'illusion d'un contrôle sur la vie des personnes et des sociétés. L'autorisation de la reconnaissance faciale sous condition, y compris pour des raisons d'ordre public tel que prévu par le règlement européen, feint d'ignorer tout à la fois le respect des droits et libertés et les principes juridiques traditionnels des démocraties libérales. Ainsi, lorsque la reconnaissance faciale est autorisée, elle remet de fait en cause la présomption d'innocence et les règles du procès équitable. L'immixtion des traitements algorithmiques en matière de police administrative ou judiciaire à des fins prédictives ne relève pas plus de la science puisqu'il n'est pas possible de prédire l'avenir. L'utilisation d'un logiciel de prédiction des infractions, comme certains sont actuellement développés par la police et la gendarmerie[1980], nourrissent une vision irrationnelle de la société, et sont sources de nombreuses boucles de rétroaction et de violations potentielles systémiques de droits et libertés[1981]. La justice n'est de plus pas à l'abri d'une tentation de l'automatisation à outrance de la procédure jusqu'au jugement[1982] ainsi que dans le suivi des peines. L'outil, même utilisé en tant qu'aide à la prise de décision sur l'évaluation d'une récidive par exemple, est en mesure d'exercer une incidence telle sur le discernement des magistrats qu'il est préférable de prohiber un tel usage[1983].

[1978] « *De même, la reconnaissance des affects peut également être effectuée au moyen des technologies de reconnaissance faciale pour prétendument détecter les traits de personnalité, les sentiments intérieurs, la santé mentale ou l'engagement des travailleurs à partir d'images des visages. Lier la reconnaissance de l'affect, par exemple au recrutement de personnel, à l'accès à l'assurance, à l'éducation peut présenter des risques très préoccupants, tant au niveau individuel que sociétal, et devrait être interdit* », Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel, « Lignes directrices sur la reconnaissance faciale », 28 janvier 2021, p. 4.

[1979] Art. 52 du projet de règlement.

[1980] Voir en ce sens, CASTETS-RENARD C., BESSE P., LOUBES J-M, PERRUSSEL L., Centre des Hautes Etudes du ministère de l'Intérieur, Rapport relatif Encadrement des risques techniques et juridiques des activités de police prédictive, *op. cit.*, et FERET C., POINTEREAU R., Rapport d'information n° 621, op. cit., faisant état du développement d'un logiciel de police prédictive par la gendarmerie afin d'anticiper les cambriolages sans avoir recours à des données à caractère personnel.

[1981] Voir en ce sens, THE CITIZEN LAB, To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada [en ligne]. [Consulté le 2 décembre 2020]. Disponible à l'adresse : https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

[1982] DUCLERCQ J-B., « Les algorithmes en procès », *op. cit.*, p. 131.

[1983] Suprem Court of Wisconsin, State of Wisconsin v. Loomis, case 2015AP157-CR [en ligne]. [Consulté le 2 mars 2021]. Disponible à l'adresse : https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690. Pour plus de précisions, *Supra.*, n° 658.

984. Il existe par ailleurs des hypothèses où l'absence de transparence technique, comme c'est aujourd'hui le cas pour les boîtes noires[1984], ou à l'inverse l'excès de transparence, justifierait l'exclusion du recours au numérique. Bien que revêtant des problématiques différentes, le vote par correspondance par internet ou le recours à des machines à voter pour des scrutins locaux et nationaux sont autant de risque pour la démocratie au sens large, la confiance en celle-ci, et spécifiquement pour les principes traditionnels du droit électoral[1985].

985. Au-delà de l'exclusion des usages ou de leur conditionnalité pour que le numérique soit autorisé, se pose également la question de l'interdiction de la recherche dans certains domaines. La recherche est libre par principe, mais une découverte implique par son existence un risque de déploiement, et parfois rapidement, sans analyse d'impact. En effet, nous apprenons beaucoup des incidences des technologies sur les individus et la société qu'ultérieurement à leur déploiement, raison pour laquelle certains universitaires se prononcent dans certains domaines en faveur de moratoires[1986]. Nous recommandons, au même titre qu'il existe des limites en matière de recherche sur le clonage humain[1987], des limitations à la recherche dans le domaine des systèmes d'armement létaux autonomes (SALA), dont le développement implique inéluctablement la prolifération[1988]. La doctrine du « zéro mort », mythe sur lequel repose l'élaboration de ces dispositifs purement autonomes consiste à ce que chaque puissance militaire pense engager un conflit armé sans subir de pertes humaines[1989]. Le gouvernement français, bien que s'opposant aux SALA[1990], puisque préférant le recours aux systèmes d'armes létaux intégrant de l'autonomie car demeurant sous planification humaine[1991], n'a pas souhaité pour l'heure engager des négociations internationales sur leur interdiction[1992]. De plus, comme

---

[1984] *Supra*., n° 16.

[1985] En effet, par exemple, dans le cadre du vote électronique la vérifiabilité impose par nature le fait de mette en place un système de retraçage de son vote numériquement afin de s'assurer que notre choix a correctement été pris en compte par la machine, ce qui peut être vu comme un excès de transparence remettant en cause le secret du vote. C'est donc ici le numérique, du fait de son utilisation pour plus de facilité, qui a des incidences sur les principes traditionnels du droit électoral. Sur ce point, voir notamment *supra*., n° 607.

[1986] Voir en ce sens, THE CITIZEN LAB, To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada, *op. cit*.

[1987] Art L. 2151-2 du Code de santé publique précise que « *La conception in vitro d'embryon ou la constitution par clonage d'embryon humain à des fins de recherche est interdite. La création d'embryons transgéniques ou chimériques est interdite.* ».

[1988] NEVEJANS N., « La légalité des robots de guerre dans les conflits internationaux », *Recueil Dalloz.* 2016, p. 1273.

[1989] RUFFO M., « La robotisation de la guerre et de la décision militaire : efficacité et éthique », in JACQUEMIN H., DE STREEL A. (dir.), *L'intelligence artificielle et le droit, Larcier*, 2017, p. 437.

[1990] DE GANAY C., GOUTTEFARDE F., Rapport d'information n°3248 de l'Assemblée nationale, 15e législature, fait au nom de la commission de la défense nationale et des forces armées, enregistré à la Présidence de l'Assemblée nationale le 22 juillet 2020., p. 4, in *Assemblee-nationale.fr* [en ligne] 22 juillet 2020 [Consulté le 2 mai 2021]. Disponible à l'adresse : https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b3248_rapport-information

[1991] Comité d'éthique de la défense - Avis sur l'intégration de l'autonomie des systèmes d'armes létaux [en ligne]. [Consulté le 2 mai 2021]. Disponible à l'adresse : https://www.defense.gouv.fr/salle-de-presse/communiques/communique_le-comite-d-ethique-de-la-defense-publie-son-rapport-sur-l-integration-de-l-autonomie-des-systemes-d-armes-letaux

[1992] « (...)l'ouverture immédiate de négociations en vue d'un traité d'interdiction des "robots tueurs" ne serait pas la réponse pertinente », Ministère des Armées, Assemblée Nationale, réponse écrite à la question n° 15168 publiée au JO le 19 mars 2019,

l'indique Nathalie Nevejans, la conception implique la compréhension des règles du droit international humanitaire, ce qu'aucune IA n'est par ailleurs capable d'effectuer.

PARAGRAPHE 2 - L'exercice de la démocratie numérique

986. Le choix de la nature et du degré de transparence ou de l'exclusion d'un usage ne peut que s'opérer par le débat démocratique, ce que ne saurait retirer la technicité de l'informatique, souvent arguée pour cantonner ces choix à des débats d'experts[1993]. Nous aborderons donc la façon dont il convient d'appréhender la mince frontière qui sépare la transparence d'une exclusion du fait de l'environnement numérique (A). Enfin, au même titre qu'il existe une démocratie environnementale, il apparaît nécessaire qu'il existe une démocratie numérique (B).

A - La théorie de l'environnement numérique

987. La théorie des environnements n'est qu'une proposition pour établir des choix politiques précis. Elle peut néanmoins être utilisée en tant que méthode d'interprétation *in concreto* pour la justice. Cette méthode a pour objectif de déterminer s'il convient d'exclure une technologie, mais aussi la façon dont la conciliation juridique doit être opérée au sein de l'environnement numérique afin de poursuivre un système de valeur.

988. Comme nous avons pu le constater tout au long de ces travaux, les techniques juridiques employées à l'environnement numérique sont souvent celles de l'environnement classique, ce qui n'est pas sans incidence. Pour préserver les principes juridiques traditionnels inhérents à l'Etat de droit, cela implique la connaissance des caractéristiques de la technologie, parce que les algorithmes ne sont ni neutres, ni souvent conçus spécifiquement pour être respectueux de l'usage souhaité. Cela implique une fine analyse de l'architecture technique de la technologie, ce qui est nécessairement fluctuant et mouvant, et en rupture avec la neutralité technique des régimes généraux abordés. Cette prise en compte spécifique de la technologie vise à se prémunir de conciliations ou d'usages qui rendraient ineffectifs ou inopérants les droits et libertés au sein de cet environnement et emporterait ensuite des conséquences sur le terrain classique puisque ces deux sphères ne sont pas cloisonnées[1994].

15e Législature [en ligne]. [Consulté le 3 avril 2021]. Disponible à l'adresse : http://questions.assemblee-nationale.fr/q15/15-15168QE.htm

[1993] BENAYOUN Y., REGNAULD I., *Technologies partout, démocratie nulle part*, *FYP*, 2020, 240 p.

[1994] L'interaction du logiciel avec le monde physique est rendue possible uniquement parce que nous avons fait le choix de leur immixtion dans les domaines dans lesquels ils sont censés résoudre ou faciliter la résolution de problèmes. A titre d'exemple, recourir à un logiciel à des fins de pure simulation n'a aucune incidence sur le terrain classique puisqu'il est cantonné à sa

989. Il ne s'agit pas ici d'appréhender la transparence ou l'usage en fonction du domaine d'intervention mais au regard de la caractéristique technique de l'architecture qui va être déployée. Cet enjeu est éminemment démocratique. L'environnement numérique est régi par des règles dont la nature n'est pas exactement la même que sur le terrain classique, ce qui nécessite parfois une adaptabilité en fonction des caractéristiques techniques des outils[1995].

990. Pour illustrer ce propos, nous souhaiterions retracer brièvement la construction du droit du respect de la vie privée et la manière dont son régime juridique a bifurqué à cause du numérique pour donner naissance à la protection des données à caractère personnel, lui conférant ainsi une quasi-autonomie par rapport à son initial droit de rattachement[1996]. La vie privée est une notion relativement récente tant la promiscuité était importante dans les habitations de l'époque médiévale. C'est notamment la raison pour laquelle cette notion ne se retrouve pas protégée par la DDHC de 1789[1997]. Sa protection est plus tardive puisque le fruit d'une longue construction, parmi laquelle l'émergence de la photographie n'est pas étrangère par la voie de procédure pour diffamation[1998]. Il convient donc d'attendre 1970 pour que le respect de la vie privée fasse son entrée dans le code civil[1999] et soit par la suite constitutionnellement protégé[2000]. En droit français, et à l'inverse de la notion anglophone de « *privacy* »[2001], la motivation première de la LIL de 1978 est pourtant le respect de la vie privée aussi bien vis-à-vis de l'Etat que des acteurs privés à un niveau législatif, n'hésitant pas à

sphère immatérielle. Voir en ce sens, PELLEGRINI F., CANEVET S., *Droit des logiciels*, *op. cit.*, p. 285, « *En effet, un logiciel ne peut avoir, par lui-même, aucune action sur le monde physique. Nous en donnons pour preuve qu'il est possible de faire fonctionner un logiciel au sein d'un simulateur sans qu'il produise les effets qu'il était censé avoir sur son environnement. C'est ainsi que l'on teste par exemple les logiciels embarqués de guidage des fusées : l'exécution de ces logiciels s'effectue non pas au sein du calculateur de la fusée, comme ce sera le cas en conditions réelles, mais au sein d'un environnement logiciel qui simule le fonctionnement de ce calculateur et de tous ses périphériques* ». Dès lors, lorsque le choix a été pris d'utiliser une technologie pour résoudre des problèmes humains, c'est prendre le risque de subordonner le monde physique aux caractéristiques du logiciel et de l'ordinateur qui l'exécute, et donc des limites de cet univers.

[1995] *Supra.*, n° 605 et s.

[1996] TAMBOU O., *Manuel de droit européen de la protection des données à caractère personnel*, *op. cit.*, p. 21.

[1997] LASCOMBE M., VANDENDRIESSCHE X., DE GAUDEMONT C., *Code constitutionnel et des droits fondamentaux*, *Dalloz*, 2016, spec. p. 19.

[1998] Tribunal civil de la Seine, Félix c. O'Connell, 18 juin 1858.

[1999] Loi n° 70-643 du 17 juillet 1970, art. 22 introduit à l'article 9 du Code civil que « *Chacun a droit au respect de la vie privée* ».

[2000] Ce n'est qu'après une construction progressive en droit national que le Conseil constitutionnel, en 1995, confronté à des dispositions relatives à l'installation de la vidéosurveillance, disposa « *que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* » prévue par l'article 66 de la Constitution. Voir en ce sens, CC, décision n° 94-352 DC, 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, cons. 3. Puis, en 1999, lorsque se pose l'instauration de la carte électronique individuelle pour la couverture maladie universelle, le Conseil précise finalement que « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression*. » ; « *que la liberté proclamée par cet article implique le respect de la vie privée* ; » sur le fondement de l'article 2 de la DDHC de 1789 ; CC, décision n° 99-416 DC, 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, cons. 45.

[2001] Voir en ce sens, WHITMAN J. Q., The Two Western Cultures of Privacy : Dignity versus Liberty, 2003, *Papers.ssrn.com* [en ligne]. [Consulté le 5 avril l2021]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=476041 ; HALPERIN J-L., « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », Les nouveaux Cahiers du Conseil constitutionnel, *Lextenso*, n° 48, 2015, p. 59.

interdire certains traitements de données pour protéger les personnes physiques[2002]. C'est sous l'impulsion de conventions internationales que la notion de données personnelles a pris toute son autonomie par rapport au respect de la vie privée[2003].

991. L'autonomie d'une telle notion est en principe justifiée pour mieux protéger les libertés au sein de l'environnement numérique, mais cela offre également paradoxalement la possibilité d'offrir un niveau de protection amoindri. En effet, bien que le respect de la vie privée soit matriciel dans la construction de la protection des données personnelles, c'est aussi la possibilité une fois cette nouvelle source créée, d'obtenir un régime juridique qui bifurquerait de sa source originelle, au point d'ouvrir droit à une nouvelle conciliation possible propre à la sphère numérique. La reconnaissance d'une nouvelle source doit alors permettre des prises en compte spécifiques à cet environnement pour parvenir à l'objectif de protection souhaité. Ces principes ne sont d'ailleurs pas ceux du terrain classique, mais bien du cyberespace, sphère sans laquelle ils n'auraient pas existé, et dont on voit bien que les régimes juridiques ne sont pas identiques et ne poursuivent pas toujours les mêmes buts. Mais le caractère pernicieux des algorithmes informatiques encourage l'acceptabilité de pratiques que l'on n'accepterait jamais sur le plan physique, et que pourtant le pouvoir politique et juridictionnel nous impose, parfois par méconnaissance de la technique. C'est donc par l'étude de la technique que le droit doit aussi être modelé en conséquence, mais volontairement. Alors qu'en apparence le droit est en réaction à un fait juridique, c'est désormais la technologie qui modifie le droit sans que nous nous en apercevions. Il ne s'agit plus d'une réaction politique à un fait juridique, mais d'un dégât collatéral au déploiement d'une technologie dont l'impact aurait mal été évalué. C'est pour cette raison que la théorie de l'environnement numérique vise à pallier ce risque.

992. Même si les régimes juridiques généraux sont tenus d'aborder de tels domaines avec une neutralité technique, il convient cependant dans certains cas, d'entrer dans le détail de certaines technologies dans le débat politique ou pour l'application de la loi, ne serait-ce que parce que des technologies sont amenées à conditionner l'exercice des droits et libertés.

993. Nous avons néanmoins conscience que cette approche peut légitimer une restriction des libertés puisque le régime juridique qui est l'émanation du terrain classique ne peut pas toujours être identique à celui nécessaire pour poursuivre l'exercice d'une liberté sur le terrain numérique. En effet, certains pourront toujours arguer que l'environnement numérique exige

[2002] *Supra.*, n° 148.
[2003] *Supra.*, n° 908 notamment.

d'amoindrir des droits et libertés, et qui légitimerait des usages particulièrement intrusifs qu'il est pourtant impensable d'opérer sur le terrain classique. A titre d'exemple, la Cour EDH reconnait que la sphère numérique est source de nouvelles menaces, ce qui implique le recours à des outils de surveillance de masse[2004]. En d'autres termes, cela revient à considérer que le régime juridique applicable à l'environnement numérique et donc aux droits et libertés à cet environnement, ne peuvent être les mêmes que sur le terrain classique, et ce alors que cette nouvelle conciliation est défavorable pour les libertés, et emporte physiquement des conséquences. Nous imaginons pourtant mal la Cour de Strasbourg admettre une surveillance physique de masse aussi intrusive que ne l'est la surveillance numérique à des fins de préservation de l'ordre public. Pourtant, les conséquences d'un tel postulat sont tout aussi graves. Au même titre que le numérique est facilitateur en matière de liberté d'expression, il l'est tout aussi en termes de surveillance qu'elle soit privée ou publique.

994. Nous pensons, contrairement à la Cour, et ce quelles que soient les garanties qui seraient mises en œuvre, que du fait de sa nature, l'environnement numérique demande plus de protection tant les outils qui y sont déployés ont des incidences systémiques et potentiellement liberticides. Raison pour laquelle il serait même envisageable de reconnaître des sanctuaires dans l'environnement numérique, où l'on pourrait même imaginer que des droits de détachement seraient absolus, car à défaut le principe même d'une conciliation les rendrait inopérants.

995. Même si aujourd'hui il existe également « *Law is code* » aux cotés de « *Code is Law* »[2005], c'est le matériel informatique et le logiciel qui conditionnent en partie l'exercice de l'Etat de droit dans cet environnement, et qui par ricochet impactent le terrain classique. Ne serait-ce que parce que si un Etat devait par exemple imposer une porte dérobée dans un système de télécommunication centralisé, quand bien même il serait chiffré, il permettrait à toute personne connaissant cette ouverture d'accéder aux messages échangés. C'est donc la nature même de la communication qui est modifiée par le numérique puisqu'en effet, on imagine mal comment sur le terrain classique il serait possible d'opérer l'ouverture et la lecture de tout le courrier postal, et d'y faire humainement des recoupements identiques à ce que permet l'informatique, preuve que la nature y est différente.

[2004] Cour EDH, Grande chambre, Big brother watch c. Ru, du 25 mai 2021 « *Il y a là une menace grave pour la sécurité nationale qui, par définition, n'existe que dans le domaine numérique et ne peut donc être détectée et investiguée qu'à l'aide de moyens numériques.* », § 323.
[2005] GROFFE-CHARRIER J., « La loi est-elle dictée par le code ? », *op. cit*.

996. Reconnaître une autonomie de l'environnement numérique, c'est accepter qu'un régime juridique ne puisse être identique entre ce terrain classique et l'environnement numérique. Ainsi, l'attention faite à une liberté hors ligne ne peut être en réalité identique dans la sphère numérique. En ce sens, l'interdiction d'un usage au sein de cet environnement ne signifie pas qu'il n'existe pas d'alternative dans l'autre monde. Ne pas souhaiter recourir à des dispositifs à des fins de surveillance de masse, n'implique pas un renoncement d'opérations de surveillance par des voies plus traditionnelles car nos capacités humaines ont des limites observationnelles qui sont par ailleurs des protections physiques pour les libertés. Ainsi, le fait qu'un agent du renseignement intègre, comme cela est déjà le cas, une cellule djihadiste qui communiquerait par la voie d'une messagerie chiffrée est moins attentatoire aux droits et libertés que l'instauration de portes dérobées[2006] dans un tel système, ce qui offrirait la possibilité d'une captation de tout cet environnement.

997. De la même manière, et bien que nous soyons conscients des avantages du vote électronique tendant vers un exercice plus direct de la démocratie[2007] pour les scrutins nationaux et locaux, l'appréhender comme simple dématérialisation du vote traditionnel papier, c'est faire fi de l'environnement numérique qui exerce une pression sur les principes traditionnels du scrutin. L'étude des architectures techniques proposées dans le cadre des machines à voter ou du vote par internet ne saurait permettre une transparence directe, sans remettre en cause le secret du scrutin. Telle est actuellement la nature de l'informatique, que nous le voulions ou non. La matière électorale est par ailleurs si sensible quant aux incidences démocratiques que même la désignation d'un tiers de confiance ne saurait empêcher un risque significatif de fraudes ou d'erreurs sur le résultat du scrutin[2008]. De la même manière, concernant le vote par internet, c'est prendre le risque que des données personnelles, portant notamment sur les opinions politiques puissent être manipulées et piratées. Il convient alors de garder une garantie collective lors des opérations de vote, ce que seul le scrutin traditionnel sur support papier en dehors de tout vote par correspondance est pour l'heure en mesure d'assurer[2009], ce qui permet

[2006] « *Le principe de la mise en œuvre d'une « Backdoor » ou porte dérobée correspond à prévoir un accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel. Le principe de la mise en œuvre d'une « Master Key » ou « clé maître » correspond à prévoir ouvertement un tel accès, mis en œuvre via cette clé, aux données chiffrées contenues dans un logiciel ou sur un matériel.* », définition donnée par la CNIL [en ligne]. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://www.cnil.fr/fr/definition/porte-derobee-ou-backdoor

[2007] Ces facilités logistiques semblent même au premier abord susceptibles de favoriser l'exercice de la souveraineté politique par le Peuple, laissant entrevoir de nouveaux mécanismes démocratiques.

[2008] *Supra*., n° 538 et s.

[2009] Pour le professeur Jean-Philippe Derosier, la technicité du vote par Internet *« semble a priori empêcher le contrôle éclairé des citoyens ». La CNIL souligne également « l'opacité et la technicité importante des solutions mises en œuvre ». Elle reste, d'une manière générale, « réservée quant à l'utilisation de dispositifs de vote par correspondance électronique, notamment via Internet, pour des élections politiques »*, BUFFET F-N., Rapport d'information n° 240 relatif au vote à distance du Sénat, session ordinaire 2020-2021, fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du

notamment de conserver l'effectivité des autres principes du droit électoral qui auraient été remis en cause par nature, par l'utilisation de ces techniques pour les raisons explicitées.

998. Il y a donc des domaines dans lesquels le recours exclusif à l'environnement classique offre le plus de garanties, quand bien même le numérique serait plus efficace. C'est donc aussi parce qu'une technologie est trop efficace qu'il est nécessaire de l'exclure pour s'en prémunir, et ce que quel que soit les garanties de transparence et de contrôle humain sur l'outil. Ainsi, l'interdiction du recours au numérique dans un environnement ne veut pas dire que l'on obtiendra aucun résultat sur le terrain classique.

999. Les parlementaires et les citoyens ont donc besoin de discuter précisément des technologies qui vont être déployées, raison pour laquelle notre autorité de contrôle unique aura également pour mission de cartographier les technologies et leurs incidences sur les libertés et la société, ce qui conditionne leurs choix. Nous gageons donc que la révision des institutions[2010] que nous souhaitons offrira plus de protection et empêchera cette déviance.

B - Principe de participation aux décisions en tant que composante de la démocratie numérique

1000. La transparence ne pouvant pas apporter toutes les garanties nécessaires à l'épanouissement de l'Etat de droit, le choix de l'exclusion ou d'une plus grande transparence d'un usage, doit aussi pouvoir s'effectuer à travers la participation du public, ce qui vient compléter la démocratie représentative telle qu'abordée précédemment[2011].

1001. La démocratie numérique dont il est question dans cette démonstration n'est pas l'évolution des institutions par les nouveaux outils[2012], mais la façon dont il est possible pour le public de participer aux prises de décisions qu'elles soient d'ailleurs publiques ou privées.

1002. Pour l'heure, la démocratie environnementale, partie intégrante de la démocratie administrative[2013], connait une expansion et ne peut que servir de modèle à bien des égards en matière de participation numérique. Elle est intéressante en ce qu'elle illustre l'émergence d'un

Règlement et de l'administration générale, enregistré à la Présidence du Sénat le 16 décembre 2020, p. 49, *Senat.fr* [en ligne]. [Consulté le 2 mai 2021]. Disponible à l'adresse : http://www.senat.fr/rap/r20-240/r20-2401.pdf

[2010] *Supra*., n° 694 et s.

[2011] *Ibid.*

[2012] Certains auteurs pensent en effet que les nouveaux outils numériques peuvent modifier la nature de la participation citoyenne, ce que nous ne nions pas, mais cela n'est pas l'objet de l'actuelle démonstration.

[2013] Voir en ce sens, CHEVALLIER J., « De l'administration démocratique à la démocratie administrative », *Revue française d'administration publique, ENA*, 2011/1, p. 217 à 227.

fait juridique contemporain et une réponse juridique particulière, parmi laquelle nous retrouvons le principe de participation du public[2014], qui par ailleurs est désormais intégré au bloc de constitutionnalité[2015]. Même si la mise en œuvre de ce principe demeure imparfaite[2016], nous souhaiterions que la démocratie numérique puisse s'en inspirer. Il convient toutefois d'aller plus loin que ce que permet la démocratie environnementale et administrative. En effet, la participation du public que nous souhaiterions ne poursuit pas totalement les mêmes objectifs, puisqu'au-delà de la participation aux prises de décision publique, il s'agirait également d'un principe hybride prenant en compte aussi bien la problématique de la démocratie administrative que de la démocratie directe.

1003. Contrairement au principe de participation en matière environnementale qui a été le fruit de décennies de construction notamment par la voie de conventions internationales[2017], les sources manquent cruellement dans le domaine numérique. En effet, il n'y a pas pour l'heure de source internationale pouvant influencer une éventuelle transposition rapide dans le droit régional ou national. Tout reste donc à bâtir. Certaines déclarations de normes informelles telle que la déclaration de Montréal pour une IA responsable évoquent toutefois un tel principe[2018]. Par exemple, au même titre que la convention d'Aarhus pour l'environnement, nous retrouvons dans la convention sur l'IA l'accès à l'information, et donc à la transparence de ces outils, pour que puissent s'exercer le débat et le contrôle démocratique. Il existe donc une troublante symétrie avec la démocratie environnementale, à la différence que le numérique ne peut se cantonner qu'aux prises de décision publique. En ce sens, il ne sera donc pas possible de qualifier cela de démocratie administrative.

1004. La transparence juridique que nous nous sommes efforcés à construire tout au long de ces travaux rencontre donc nécessairement l'une de ses finalités essentielles, à savoir la participation du public grâce au droit à l'information, offrant un débat et une prise de décision éclairée. En effet, comme le note Julie Arroyo au sujet de la transparence administrative, ce que nous pouvons dupliquer à la transparence générale des traitements algorithmiques, elle

---

[2014] VAN LANG A., « Le principe de participation : un succès inattendu », *Les nouveaux Cahiers du Conseil constitutionnel*, n° 43, 2014, p. 25.

[2015] « *Toute personne a le droit, dans les conditions et les limites définies par la loi, d'accéder aux informations relatives à l'environnement détenues par les autorités publiques et de participer à l'élaboration des décisions publiques ayant une incidence sur l'environnement.* » art 7, Charte de l'environnement.

[2016] *Infra*., n° 1006 et s.

[2017] La démocratie environnementale est composée du triptyque de l'information, de la participation et de l'accès à la justice telle que présentée notamment par la Convention sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement, dite d'Aarhus, du 25 juin 1998.

[2018] Principe 5 : « principe de participation démocratique », Déclaration de Montréal pour un développement responsable de l'intelligence artificielle [en ligne]. [Consulté le 15 juin 2021]. Disponible à l'adresse : https://www.declarationmontreal-iaresponsable.com/la-declaration

« *participe à la réalisation de ces nouvelles exigences démocratiques en assurant l'information des administrés, cette information leur permettant de se livrer à une forme de contrôle du pouvoir ainsi que, dans une certaine mesure, d'y participer* »[2019].

1005. Ainsi, il convient de déduire que lorsque cette transparence ne peut être exercée techniquement, du fait d'une architecture opaque par nature, cela peut être légitimement un motif à son exclusion. C'est la raison pour laquelle le droit d'information en tant que technique juridique de mise en œuvre du principe de transparence des traitements algorithmiques, ne doit connaître que de rares exceptions[2020]. Dans ces rares hypothèses c'est à la commission technique de contrôle unique qu'il reviendra alors de procéder à ces expertises, et de diffuser les rapports et études d'impact nécessaires à l'épanouissement du débat. En effet, des informations minimales certifiées seront nécessaires au public pour qu'il puisse également se prononcer sur certaines orientations privées.

1006. Le droit interne nous renseigne déjà en droit de l'environnement ou en urbanisme sur la forme que pourrait prendre cette participation même si elle ne s'applique qu'aux décisions d'autorités publiques[2021]. Nous retrouvons par exemple en amont de la mise en œuvre des projets les procédures de participation du public au débat ou à la décision finale aussi bien au plan local que national. Bien que ces procédures soient critiquables à certains égards, car elles ne lient pas la décision finale dans la plupart des cas, il convient de s'en inspirer. De nombreuses collectivités territoriales[2022] sont par exemple tentées par des expérimentations attentatoires aux libertés comme le déploiement de drones, de reconnaissance faciale, ou détecteurs de bruits dans l'espace public, sans qu'il ne soit spécifiquement possible pour les administrés de s'y opposer publiquement autrement que par la voie d'élections générales, de collectifs ou judiciairement.

1007. A l'inverse de la participation aux débats publics en matière environnementale qui s'apparente davantage à un processus de légitimation[2023] d'un projet, les réserves émises par le

---

[2019] ARROYO J., Un droit à l'oubli dans le champ des documents administratifs ?, *RDLF*, chron. n° 6, 2016 [en ligne]. [Consulté le 15 juin 2020]. Disponible à l'adresse : http://www.revuedlf.com/droit-administratif/un-droit-a-loubli-dans-le-champ-des-documents-administratifs/#note-6120-99

[2020] *Supra*., n° 938 et s.

[2021] *Infra*., n° 1007.

[2022] FRENOIS M., Nice : Caméra, reconnaissance faciale, détecteur de bruits… Un collectif lancé pour « résister à la surveillance », *20 minutes.fr* [en ligne] 17 septembre 2019 [Consulté le 3 février 2021]. Disponible à l'adresse : https://www.20minutes.fr/nice/2605395-20190917-nice-camera-reconnaissance-faciale-detecteur-bruits-collectif-lance-resister-surveillance

[2023] Comme l'indique Jacques Chevallier « *Les procédures délibératives apparaissent, dès lors, moins l'instrument permettant aux citoyens de définir, par le biais de leurs discussions, les contours de l'action publique, que le moyen pour les gouvernants*

public devraient être prises en compte lors de la phase d'élaboration du projet numérique, ou à défaut, permettre par un droit de pétition de faciliter la possibilité d'une consultation locale ou nationale qui lierait le maître d'ouvrage. Les projets concernés seraient les plus importants, et ceux nécessitant la désignation d'un architecte du numérique que nous avons abordé[2024].

1008. Il serait même concevable d'aller plus loin en incluant dans ce principe, la participation à la gouvernance de grandes plateformes numériques, y compris privées, qui exercent une influence significative sur la société et les libertés. Il convient désormais que le public prenne part aux décisions des grands réseaux sociaux qui modèlent le monde par l'intermédiaire de traitements algorithmiques, notamment afin qu'ils participent au design et aux orientations des architectures techniques de ces derniers, ce qui n'empêchera pas la plateforme de pouvoir continuer à avoir une politique commerciale dans les domaines qui ne sont pas du ressort des libertés. Il ne s'agit pas pour autant, par cette participation, d'aboutir à l'émergence d'un droit qui bifurquerait du cadre posé par l'Etat, mais cela offrirait cependant des marges de manœuvre suffisantes pour que ces espaces, devenus de fait des activités d'intérêt général par la sociabilisation humaine, puissent définir certaines orientations en tant que gestion d'un commun, et pourquoi pas de manière transnationale. Dans le cadre des réseaux sociaux centralisés par exemple, un seuil de connexion minimal comme c'est déjà le cas dans la LRN pour imposer des obligations de transparence, permettrait une participation du public à ces réseaux qui sont devenus de fait par extension des espaces publics. Cette approche admet, comme le propose Jason Barrett Prado, des règlementations particulières en fonction du nombre d'utilisateurs[2025]. Certains auteurs considèrent toutefois que la taille des services privés ne fait pas tout et que leur régulation peut notamment s'effectuer à travers plusieurs critères tels que la fonction ou le pouvoir qu'ils exercent[2026].

1009. C'est aussi une manière de contrecarrer les tentatives d'entreprises comme Facebook, qui sous réserve de conditions générales d'utilisation, se permettent même de proposer une construction juridictionnelle sans légitimité, aboutissant à un droit alternatif concurrençant le

de consolider celle-ci, sur un plan pratique comme sur un plan symbolique. », CHEVALLIER J., « De l'administration démocratique à la démocratie administrative », *op. cit.*, p. 227.

[2024] *Supra.*, n° 890 et s.

[2025] Selon Jason Prado, si un service bénéficie de moins de 5 millions d'utilisateurs, il est soumis aux règles classiques de confidentialités. Entre 20 et 50 millions d'utilisateurs, la plateforme serait contrainte par des obligations de transparence telles que la publication de rapports sur les données utilisées et la manière dont elles sont utilisées. Tandis qu'au-delà de 100 millions d'utilisateurs, il ne serait plus possible de distinguer le service d'un Etat, raison pour laquelle elle doit être gouvernée démocratiquement avec un conseil d'administration représentatif. Voir en ce sens, PRADO Jason Barrett, Taxonomizing platforms to scale regulation, *Venturecommune.substack.com* [en ligne] 18 novembre 2019 [Consulté le 2 novembre 2020]. Disponible à l'adresse : https://venturecommune.substack.com/p/taxonomizing-platforms-to-scale-regulation

[2026] TARNOFF Ben, Platforms don't exist, *Bentanoff.substack.com* [en ligne] 22 novembre 2019 [Consulté le 11 janvier 2021]. Disponible à l'adresse : https://bentarnoff.substack.com/p/platforms-dont-exist

l'autonomie des citoyens en démocratie en modelant par exemple l'exercice de la liberté d'expression qui s'effectue de plus en plus sur ces plateformes. Un tel principe devrait également être constitutionnalisé car il se heurte à des principes préexistants qui n'assurent pas une conciliation en ce sens[2027].

1010. Au-delà des plateformes numériques, nous considérons également que le principe de participation doit s'étendre à l'élaboration des standards techniques en informatique, voire des normes ISO, qui bien que privées, mettent en œuvre le principe de transparence d'un point de vue technique et façonnent le numérique en général. Ainsi, une convergence doit désormais s'opérer entre spécialistes et la poursuite de l'intérêt général, car mêmes les choix techniques apparaissant comme anodins sont aussi des choix de nature politique concernant la société humaine.

CONCLUSION DU CHAPITRE II

1011. Le principe de transparence des traitements algorithmiques connait des limites. Même avec les bénéfices d'une constitutionnalisation, il existe de fait plusieurs manières d'assurer sa mise en œuvre, ce qui impacte de fait la protection des droits et libertés qu'il est censé protéger. L'étude des approches effectuées dans le cadre de ce chapitre revient donc à considérer que pour garantir son effectivité, la prise en considération du risque de l'usage et de la légitimité doivent être combinés à l'inverse de ce que propose le projet de règlement européen qui doit être enrichi en ce sens.

1012. Enfin, la transparence ne peut se suffire à elle-même puisque, quand bien même elle serait absolue d'un point de vue juridique et technique, elle est susceptible de légitimer des usages liberticides. Il convient alors pour les usages les plus sensibles et inconciliables avec les valeurs de notre Etat de droit, de procéder à une exclusion de ces traitements. Ces exclusions doivent être discutées grâce à un principe de participation du public à la prise de décision aussi bien publique que privée du fait des incidences sur la société que les algorithmes exercent.

[2027] SUPREME COURT OF THE UNITED STATES OF AMERICA, Manhattan community acces corp. ET AL. V. Halleck Et AL, 17 juin 2019. Voir en ce sens, G'SELL F., « Remarque sur les aspects juridiques de la souveraineté « numérique » », *La Revue des juristes de Science Po*, n° 19, octobre 2019, spec. p. 55 : « *la Cour Suprême y juge que les acteurs privés hébergeant des espaces de discussion ouverts au public sont libres de les modérer à leur discrétion.* ».

CONCLUSION DU TITRE II

1013. La mise en œuvre d'un principe général de transparence des traitements algorithmiques ne peut être effectuée que par l'intermédiaire des pouvoirs constitués de l'Etat. Mais la société civile ne saurait être en reste et doit pouvoir bénéficier d'un rôle plus significatif afin de participer à son effectivité. De nombreuses associations ou encore des lanceurs d'alerte ont par exemple démontré qu'ils concouraient à une meilleure compréhension des outils numériques. L'éthique est de plus un guide, une « antichambre » du droit, qu'il convient de prendre en considération, même si elle ne doit pas avoir vocation à se substituer au droit. Les acteurs de la chaîne algorithmique sont susceptibles de prendre part à la réalisation de cet objectif. L'institution DPD devrait être élargie afin que tout traitement de données personnelles ou non, puisse être explicité, dès lors qu'il exerce une incidence sur la société. Une nouvelle profession, comme l'architecte du numérique, pourrait être le garant, pour les plus grands projets, du respect de toutes ces nouvelles obligations.

1014. Enfin, il n'y a pas d'intérêt à ce que tous les traitements algorithmiques soient transparents. Certains algorithmes des opérateurs économiques ne sont pas susceptibles de l'être lorsqu'ils n'ont pas d'effets juridiques, tandis que ceux de l'administration, y compris lorsqu'il s'agit de simples outils d'aide à la décision politique doivent l'être pour alimenter le débat public. L'étude des nouvelles techniques juridiques proposées par la Commission européenne sont intéressantes, notamment par l'intermédiaire d'une approche graduée par les risques, c'est-à-dire que plus un traitement algorithmique est susceptible d'exercer une incidence sur les personnes et la société, plus la nature et le degré de la transparence à effectuer sont significatifs.

1015. Néanmoins, quand bien même elle serait effective, il convient dans de nombreuses hypothèses d'exclure certains usages algorithmiques car trop attentatoires aux libertés. En effet, le principe de transparence connaît des limites et n'a pas vocation à légitimer des usages. Pour ce faire, un principe de participation permettrait aux citoyens de se prémunir des effets indésirables d'une transparence utilisée en tant que faire-valoir, et de choisir le cas échéant, quels seraient les usages algorithmiques à exclure ou à autoriser sous condition.

CONCLUSION DE LA SECONDE PARTIE

1016. Nous sommes incontestablement à un tournant où les nouveaux enjeux du numérique interrogent le fonctionnement de nos institutions, mais également de la hiérarchisation des valeurs constitutionnelles entre elles. En effet, le secret ou les libertés économiques doivent-elles l'emporter sur la transparence des traitements algorithmiques ? Ce débat, y compris entre juristes, n'aura jamais été aussi contemporain. A défaut, cela reviendrait à s'empêcher d'observer un environnement parallèle au terrain classique, alors que l'étude de certains outils, y compris par un tiers de confiance indépendant, est nécessaire car il conditionne l'exercice de nos libertés. Bien entendu, il est toujours possible de saisir certaines logiques sans avoir accès à toutes les informations d'un algorithme et de ses données, mais cela limiterait considérablement la compréhension de nombreux systèmes qui pourtant exercent une incidence sur la société et les personnes. C'est la raison pour laquelle pour des raisons démocratiques il est impératif qu'une telle transparence puisse s'opérer à travers un principe constitutionnel général de transparence des traitements algorithmiques qui bénéficierait d'une unité conceptuelle, à savoir que l'observation conditionne nécessairement les choix démocratiques qui en découlent. A défaut, le secret annihilerait toute possibilité de se saisir d'un fait juridique, mais aussi de permettre l'effectivité des droits et libertés et de l'ordre juridique.

1017. Ce principe de transparence ne peut toutefois se mettre en œuvre de manière liberticide. En effet, l'excès de transparence est souvent associé au totalitarisme, surtout lorsqu'il est exigé des individus. La transparence doit s'effectuer dans le respect des droits et libertés et sous l'égide d'une autorité de contrôle purement technique et indépendante, dont le rôle serait d'expertiser ces algorithmes. Ensuite, c'est naturellement au pouvoir politique de préciser la nature et le degré de l'information à communiquer à la société et aux personnes concernées, afin de garantir d'autres exigences constitutionnelles comme la vie privée notamment. Pour ce faire, il nous est apparu opportun que les pouvoirs constitués prennent en compte les particularités du numérique pour une meilleure action de l'Etat. En ce sens, une chambre dédiée ainsi que la création de chambres spécialisées en matière du numérique semble indispensable pour que cette transparence soit effective.

1018. Pour finir, comment ne pas considérer que le rôle de la société civile doit aussi être encouragé dans cette quête de transparence, ne serait-ce que parce qu'elle exerce également un contrôle sur ces algorithmes et éclaire la société dans son ensemble au sujet de leur compréhension. L'Etat gagnerait à encourager de telles initiatives qui ont déjà, dans de

nombreux domaines, pu faire leur preuve comme en matière d'obsolescence programmée notamment à travers des associations de consommateurs. Il en est de même concernant le rôle des lanceurs d'alerte et qui contribuent à l'observation de certains comportements au sein de l'environnement numérique.

1019. L'éthique est par ailleurs amenée à bénéficier d'un rôle de plus en plus significatif afin de penser le droit de demain. De nouvelles professions permettront également, sur le modèle du DPO, d'être acteur et interlocuteur en matière de droit à l'information des traitements algorithmiques, qu'ils manipulent des données personnelles ou non, dès lors qu'ils ont une incidence sur la société. Enfin, certains grands projets recourant au numérique et ayant un potentiel caractère systémique, devraient être subordonnés à la désignation d'un architecte du numérique s'assurant que le cadre réglementaire en la matière est correctement respecté. Il s'agirait d'un contrôle *a priori* des algorithmes.

1020. La transparence ne doit cependant pas occulter la problématique selon laquelle des usages algorithmiques demeurent risqués, et ce malgré une explicabilité et un contrôle effectif. Dans cette hypothèse, il conviendrait davantage d'interdire les algorithmes d'intervenir dans le déroulement des procédures scrutins nationaux. Cette exclusion pourrait s'effectuer aussi bien par les représentants que par la voie d'un principe de participation du public.