Le temps du numérique, le temps du droit et le temps du droit du numérique

Poullet, Yves

Published in:
Guerre et Paix

Publication date:
2023

Document Version
le PDF de l'éditeur

Le temps du numérique, le temps du droit et le temps du droit du numérique

Yves Poullet

Recteur honoraire et professeur émérite de l'Université de Namur, membre de l'Académie royale de Belgique

1. Le dialogue entre disciplines n'est pas chose aisée. Pourquoi m'est-il toujours apparu si aisé et si agréable avec toi, cher Bruno ? Sans doute, par notre goût commun pour le temps qui rythme, tant pour toi, l'historien, la vie de nos peuples, pour toi, l'homme de la science politique, l'adaptation de nos régimes constitutionnels, que, pour moi, le juriste, la nécessité pour nous, juristes, de relativiser les solutions que le droit apporte et sans cesse doit réévaluer à l'aune du juste et du bon. Cet article rend grâce à cette commune réflexion sur le temps et les institutions. Il est l'occasion, pour moi, juriste intéressé par le numérique de m'interroger avec toi, l'historien et l'homme de la science politique, celle des institutions, sur ce que le temps, celui d'hier, celui d'aujourd'hui, fait au droit.

Mon propos invite à une valse à trois temps, certes au rythme bien différent : le temps du numérique, le temps du droit et le temps du droit du numérique. Partons du premier. 1992, l'heure des premiers laptops, limités à quelques kilo-octets et de quelques bases de données isolées aux informations d'autant plus précieuses que leur stockage est coûteux ; 2022, des ordinateurs de plusieurs *giga* dans nos mallettes ; des réseaux sociaux où circulent des données à foison ; des montres connectées ; Netflix ; l'intelligence artificielle, les voitures intelligentes… Au temps accéléré des innovations du numérique s'oppose le temps long du droit. Aristote (*Politique*, liv. II) en donnait une explication qui retient l'attention : « Ce n'est pas la même chose de changer une technique et une loi ; la loi, en effet, pour se faire obéir n'a d'autre force que l'habitude, laquelle ne se manifeste qu'après beaucoup de temps, de telle sorte que passer facilement des lois existantes à d'autres lois, c'est affaiblir la puissance de la loi ». Sans doute, est-on loin aujourd'hui d'un droit qui devait, selon la formule de Montesquieu[1], s'écrire « les mains tremblantes », comme

[1] Dans l'*Esprit des lois*, Montesquieu rappelait, en 1748, que « [l]es lois inutiles affaiblissent les lois nécessaires » et qu'« [i]l ne faut toucher aux lois que les mains tremblantes ».

l'avait décidé ton stratège préféré, Napoléon Bonaparte[2], à qui on doit ce chef-d'œuvre du droit : le Code civil. Les juristes se plaignent volontiers de cette accélération du temps d'un droit qui ne s'écrit plus dans le marbre, mais dans le sable, et qui n'est plus pour le justiciable synonyme de sécurité juridique. Il ne s'agit plus d'encadrer, mais de modeler un futur souhaité du moins par nos gouvernants ou ceux qui l'inspirent[3]. Reste le troisième temps : le temps du droit du numérique. Tel est l'objet de notre propos qui entend répondre à deux questions. La première : « Comment le temps du droit accueille-t-il le numérique et la course folle de l'innovation technologique ? » ; la seconde, plus importante encore : « Que "fait" le numérique au "temps" du droit ? »

2. Le « fil rouge » de la réflexion peut s'énoncer comme suit. Celle-ci abordera, en premier lieu, le temps accéléré et court du numérique et les raisons pour lesquelles ce dernier, transformant de manière profonde notre environnement économique et social, notre culture, nos sociétés, voire nos identités, constitue un défi pour le droit. Le numérique oblige à envisager autrement l'espace et le temps du droit. Le défi lancé à l'espace du droit s'exprime comme suit. Il ne peut être question de le relever au niveau national, qu'il soit fédéral, régional ou communal, mais bien au niveau international et, à défaut, à celui européen. Quant au temps du droit, c'est en particulier le long temps de la loi qui se trouve remis en cause lorsque le droit entend encadrer la course folle de l'innovation technologique et cela, même si l'inventivité du législateur européen peut trouver des solutions… par ailleurs pas toujours heureuses. Sans doute, ce constat du dépassement de la loi au regard du rythme de l'évolution technologique explique la montée en puissance des délégations de régulation tantôt voulues par le législateur (les autorités administratives indépendantes), tantôt imposées par le secteur privé, tantôt laissées aux juges et improvisées par eux à l'occasion d'un litige particulier. Enfin, on aura

[2] En 2012, tu publiais un recueil complet avec commentaires des textes et citations de Napoléon sur sa vision de la guerre : *Napoléon. De la guerre*, Paris, Perrin.

[3] Dès 1991, le Conseil d'État sonne l'alarme, dans son rapport public annuel, intitulé « De la sécurité juridique ». Il écrit : « Le nombre de textes augmente, leur longueur s'accroît, leur instabilité s'accélère, leur qualité se dégrade » et ajoute très justement que, « lorsque la loi bavarde, le citoyen ne lui prête qu'une oreille distraite ». Il revient sur le sujet dans son rapport public de 2006 qui a pour titre « Sécurité juridique et complexité du droit ». Il observe que « [l]e droit, au lieu d'être un facteur de sécurité, devient un facteur d'inquiétude et d'incertitude. La démarche de simplification court après ses objectifs ». Dix ans plus tard, dans son rapport public de 2016 qui a pour objet « Simplification et qualité du droit », le Conseil d'État constate que peu d'améliorations ont été réalisées et il note, au total, « des efforts indéniables, des résultats insuffisants ». Sans doute, le phénomène s'est aggravé et amplifié depuis lors.

une attention particulière à la délégation explicite, mais surtout implicite donnée, au nom de l'effectivité propre à la technologie, par le droit au numérique lui-même. Cette délégation se multiplie surtout, en ces temps de législations dites d'exception, qu'elles soient justifiées par la pandémie (le badge électronique, la vérification de la validité de nos Covid Safe Tickets grâce à des bases de données, l'identification par la localisation des GSM des lieux de rassemblement, le contrôle du respect des réglementations par le *data mining*, etc.), le terrorisme ou autres mises en péril de nos sociétés. Au nom de l'effectivité du droit, le numérique ne va-t-il pas jusqu'à remplacer l'humain, mais également la loi, voire le juge ? Ces trois considérations nous permettront de conclure et de plaider pour un temps long du droit comme condition de sa maîtrise du numérique.

I. Le temps accéléré du numérique et ses enjeux : le défi lancé au droit

3. En quoi le numérique bouleverse-t-il les fondements mêmes du droit et désarme-t-il le juriste ? Ce bouleversement, pour ne pas dire cette révolution, s'explique d'abord par les caractéristiques mêmes de l'outil technologique et de ses applications. On pointe ici d'abord les capacités devenues, si on en croit les lois dites de Moore, Krydel et Nielsen, quasi infinies de nos systèmes d'information, tant du point de vue du traitement (3 GHz), du stockage (nos ordinateurs ont des capacités de l'ordre de 500 Go à quelques To) et de la communication de l'information (réseaux à plus de 10 Gbits). On ajoute la miniaturisation et l'ubiquité de nos terminaux devenus « *smart dusts* » (poussières intelligentes), capables de recevoir et d'émettre des informations, et localisés dans nos murs, sur les emballages de nos produits de consommation, dans nos objets familiers, dans nos poches… voire dans nos corps (les implants corporels), capables de réguler notre tension, d'aviver notre mémoire, de contrôler nos besoins en insuline. Chaque jour, en 2025, chaque citoyen européen sera 4.800 fois par jour avec des objets connectés. Enfin, l'informatique, jointe à d'autres sciences au sein de ce qui est appelé les NBIC, permet désormais d'agir au niveau du nanomètre, soit la distance entre deux atomes (30.000 fois plus fin qu'un cheveu) et notamment d'agir au niveau de notre bagage génétique, laissant rêver à la possibilité, demain, d'avoir des « surhommes ».

4. Ces diverses réalités technologiques multiplient les applications innovantes, en particulier celles permises par l'intelligence artificielle ou, plutôt, les artifices de notre intelligence. Ces applications conduisent à une transformation profonde de nos administrations, de nos entreprises, de nos existences professionnelles et individuelles, y compris de notre identité. Elles mettent à mal notre État de droit et présentent des risques de divers ordres :

– les premiers sont souvent évoqués : il s'agit des risques individuels, qu'il s'agisse de notre vie privée, de nos libertés individuelles (d'expression, de déplacement) ou de nos intérêts comme consommateur, patient, administré… ;
– on ajoutera les risques que nous courons comme entreprise ou professionnel, soumis aux *rankings*, à la concurrence déloyale des plateformes dites coopératives, l'irruption de nouveaux entrants offrant des services électroniques… ;
– on pointera ensuite les risques de discrimination : ceux liés à la difficulté d'accès ressentie par les populations vulnérables (l'Internet n'est-il pas comme le « pain » du XIX^e^ siècle comme le soulignait dès 2009 le Parlement européen ?) mais, au-delà, par la discrimination que favorise le profilage qui, au-delà des individus, identifie des groupes et leur réserve des sorts différents ;
– enfin, on terminera par les risques sociétaires, qu'il s'agisse de l'affaiblissement de nos souverainetés étatiques, mais également des risques environnementaux d'une technologie de plus en plus gourmande en énergie voire des atteintes au fonctionnement le fonctionnement de nos démocraties, comme l'a révélé le fameux scandale de *Cambridge Analytica*.

5. Face à ces enjeux de la révolution technologique, le droit se révèle mal à l'aise. Ce malaise s'explique tant par les caractéristiques de la technologie que par l'inadéquation de l'approche juridique. Parmi les caractéristiques, on se contente de souligner que :

– la dimension mondiale des infrastructures et de l'offre des produits et services électroniques remet en cause l'espace traditionnel du droit, à savoir le territoire de l'État national. Cet effacement du territoire comme base de l'action du droit ne s'opère pas en faveur des législateurs internationaux, tantôt faute de consensus, tantôt empêtrés dans des procédures longues et manquant de moyens de rendre effectives leurs dispositions. Elle explique en revanche la montée en puissance de la régulation privée des infrastructures (ICANN, IETF, W3C) et, chez

nous, du législateur européen. Nous reviendrons sur cette délégation quasi totale par nos États au législateur européen de la réglementation du numérique ;

– la révolution accélérée, continue et imprévisible du numérique désarçonne la traditionnelle prévisibilité du législateur. Lorsque les cookies ont été inventés et reconnus par l'IETF, il y a trente ans, leur but était de permettre dans un Internet balbutiant et soumis à de fréquentes coupures, faute d'une infrastructure stable, de permettre au site visité par l'utilisateur, un moment déconnecté, de poursuivre la recherche entamée, on sait ce que sont devenus les cookies comme outils à grande échelle de traçage et de profilage : la remise en cause du temps du droit[4]. Cette évolutivité permanente des outils et de leurs applications remet en cause le temps long du droit à la fois dans sa création et son application et, dès lors, son adéquation à encadrer une réalité mouvante ;
– enfin, trois caractéristiques du fonctionnement de la technologie la plus avancée questionnent le droit : son opacité soulève la question de sa compréhension tant par les citoyens que par le juge et le législateur et renvoie à la double exigence de transparence et d'explicabilité ; la dimension interactive et instantanée de son fonctionnement heurte l'exigence juridique fondamentale d'un vrai consentement fondé sur une décision réfléchie ; enfin, la mémoire de l'ordinateur n'a pas de limites, là où celle humaine permet l'oubli et justifie, comme le prévoit le Règlement général de protection des données, le droit au pardon ou au « déférencement ».

6. L'inadéquation de l'approche du droit face à l'innovation technologique s'explique au moins de trois façons.

– En premier lieu, l'approche par les « branches » du droit a-t-elle encore un sens lorsque la réalité des innovations digitales transcende ces branches du droit et exige leur appréhension globale ? Ainsi, la voiture intelligente de demain exige une réflexion tant sur des questions de droit des communications (sécurité des réseaux, interopérabilité des flux…), de droit de la concurrence, de droit de la protection des données et de la consommation, du code de la route… Sans doute, une approche liée davantage à des technologies (p. ex., l'intelligence artificielle), voire des

[4] On évoquera dans le même sens l'évolution de l'usage des Radio Frequency Identifiers (RFID), au départ utilisés pour le suivi des produits lors de leurs transports et dont l'utilisation s'est généralisée dans nos magasins, nos vêtements dans le cadre de ce qu'il est convenu d'appeler l'intelligence ambiante ou Internet des objets.

produits (la voiture intelligente, les robots…), comme y procèdent tant le *Digital Service Act* que le *Digital Market Act*, le premier, à propos des opérateurs de services électroniques d'information, le second, à propos des opérateurs de services économiques est-elle préférable ? Le *Data Act*, qui s'interroge sur l'encadrement réglementaire de la donnée, l'aborde sous l'aspect du droit de la consommation, du droit de la concurrence, du droit de la propriété intellectuelle… et constitue un bel exemple de cette approche transcendant les branches traditionnelles du droit.

– En deuxième lieu, l'approche sectorielle, par laquelle le droit délimite les secteurs d'activité et les réglemente de manière distincte, trouve ses limites par l'arrivée de nouveaux entrants prétendant ne pas être soumis aux lois de ce secteur : ainsi, Uber, vis-à-vis de la réglementation du transport de personnes, ne doit-il pas être qualifié d'opérateur de transport des personnes et soumis à la réglementation des taxis ; Facebook, qui crée une « monnaie », le Libra, peut-il échapper à la qualification de banque et aux contraintes légales liées à ce statut ? Demain, la consultation juridique ou médicale ne sera plus celle donnée uniquement par les avocats ou les médecins mais également par les Legaltech ou les Medtech, dont l'encadrement juridique des services offerts reste à définir, mais cet encadrement peut-il s'éloigner des principes légaux et déontologiques des professions traditionnelles ?
– Enfin, troisième raison, la notion, centrale dans nos droits, de « sujet de droit » repose sur la considération d'un être de chair et d'esprit doté, fiction du droit oblige, d'une conscience et d'une raison, et permanent dans son identité. Cette notion n'est-elle pas remise en cause à l'heure où les technologies réduisent nos vies à « nos » données et, grâce à la puissance de certaines applications, nous manipulent (voir les phénomènes de la désinformation et du *microtargeting*) et nous transforment, y compris dans notre identité génétique. Par ailleurs, n'est-on pas tenté d'accorder une personnalité juridique aux robots « intelligents », dont l'action simule le comportement humain ? Enfin, face aux risques dénoncés, le droit traditionnellement pensé comme un mode de régulation basé sur l'intervention *a posteriori (obligations/sanctions)* ne doit-il pas, partiellement du moins, ajouter une approche préventive fondée sur l'évaluation et la gestion des risques : un droit non postposé dans son application, mais bien anticipé par les acteurs eux-mêmes ? Le rapprochement en la matière avec le droit de l'environnement n'étonne pas, dans la mesure où le numérique constitue désormais l'environnement de nos vies et de nos sociétés.

7. Les diverses réflexions menées jusqu'ici témoignent de deux urgences : encadrer l'évolution du numérique est un devoir pour le droit au regard des défis que celui-ci pose à la société et pour ce faire, il est vraisemblable que l'approche du droit doit être modifiée à la fois dans sa temporalité, dans son espace et dans sa structure : n'est-ce pas là l'enjeu du droit du numérique ?

II. La réponse du droit du numérique

1. La loi est-elle encore le mode privilégié de création du droit numérique ?

8. Comme noté, le territoire, lieu d'exercice de la souveraineté de nos États, s'efface à l'heure où nos réseaux de communication et d'information sont sans frontières et mettent à mal les velléités nationales de les réglementer. Cette caractéristique obligerait à envisager le déplacement du législateur national vers des législateurs globaux (OMC, UNESCO, OMPI…), mais il faut bien constater que ces derniers restent souvent, sauf exception, muets, à défaut de consensus minimaux entre Nations sur l'approche à suivre et vu les intérêts que peuvent présenter économiquement un dumping réglementaire ou l'imposition par les deux géants de leurs solutions. Ainsi, les États-Unis n'ont-ils pas imposer leurs modes de régulation privées et, comme nous l'avons vu, la régulation par des organismes de normalisation dite « technique », comme l'ICANN, l'IETF et le W3C ? Contre cette tendance et afin de promouvoir autour d'une « troisième voie » aux buts tant éthiques qu'économiques, nos États européens ont consenti à une délégation de plus en plus grande au législateur européen, omniprésent en matière de réglementation du numérique. L'ubiquité du droit européen du numérique est patente et s'accélère depuis l'arrivée de la Commission van der Leyen. Ainsi, loin d'être exhaustif, on cite des propositions de réglementation majeure comme le *Data Act*, l'*IA Act*, le *Digital Market Act*, le *Digital Service Act*, le *Healthdata Space Act*…

L'analyse de l'action législative européenne révèle qu'effectivement, aucun domaine n'échappe à l'intervention de cette dernière : les exigences strictes de subsidiarité et de proportionnalité de l'intervention européenne sont à mettre aux oubliettes au motif tant de la constatation qu'Internet ne connaît plus les frontières, mais également au regard de la volonté de plus en plus proactive de l'Union européenne de refuser tant le modèle américain que celui chinois et de définir ainsi une « troisième voie ». Cette troisième voie entend promouvoir, via une réglementation

publique fondée sur la confiance (en particulier, par le respect des libertés et des exigences démocratiques) et l'excellence (la création et le développement d'un véritable marché européen des produits et services du numérique). L'intervention réglementaire est donc fondamentale pour les autorités européennes, elle l'est d'autant plus que l'Europe est loin, euphémisme, d'être leader sur le marché du numérique et trouve dans les dispositions *ad hoc* assurant l'effet extraterritorial des exigences réglementaires européennes le moyen d'imposer, à toute entreprise étrangère souhaitant pénétrer le marché européen, ses exigences, y compris les GAFAM américaines et les BATX chinoises,

9. À cet endroit, contentons-nous de nous poser la question : le temps du droit européen est-il compatible avec un objet sans cesse en évolution et qui exige, ne serait-ce que pour garantir le développement d'un marché unique européen et le protéger de l'invasion externe, à la fois une adoption et une implémentation rapides ? La réponse est positive pour diverses raisons.

– L'application directe de règlements est désormais préférée aux délais et aux marges de manœuvre, dont les États membres pouvaient bénéficier lorsque l'Union européenne choisissait l'instrument de la directive. Par ailleurs, le rythme des discussions au sein du « trilogue » des institutions législatives européennes (Commission, Conseil et Parlement) s'intensifie et l'observateur s'étonnera de voir des textes aussi complexes et importants que ceux cités précédemment : *Digital Act*, *IA Act*… parcourir les diverses enceintes du Parlement, du Conseil et de la Commission en moins de deux ans, lorsqu'on sait que le RGPD, adopté en 2016, a pris plus de quatre ans de discussions. On ajoute que, par facilité d'adoption, la Commission recourt parfois à des instruments plus *soft* que sont les recommandations dont la portée est loin d'être négligeable, dans la mesure où, selon la jurisprudence de la Cour de Luxembourg, les États membres, à défaut de devoir suivre les prescrits recommandés, se voient interdits de prendre des mesures contraires à ceux-ci.
– Par ailleurs, le législateur européen se révèle conscient des nécessités d'évolution de la loi. On connaît les clauses dites de « *sunset* » qui ordonnent l'évaluation des dispositions réglementaires dans un délai généralement court et conduisent à l'adoption de nouveaux textes (p. ex., le RGPD à la place de la directive 95/47) ou à l'ajout de dispositions, comme celles introduites par le DSA dans la directive « Commerce électronique » qui devra désormais prendre en compte le rôle et donc la responsabilité des plateformes dans la désinformation. Le législateur européen suivi par les législateurs français et allemand,

a, par ailleurs, consacré ce qu'il est convenu d'appeler les législations « bac à sable » qui autorisent dans le cadre de l'expérimentation d'innovations des exceptions à la réglementation, soumises à contrôle et évaluation publics.

– Enfin, faut-il souligner le rythme des modifications de nos lois dites numériques qui cherchent à suivre l'évolution galopante des innovations technologiques et des risques y liés. Bien des exemples pourraient être donnés ici. Contentons-nous de pointer que depuis 1981, date de la Convention n° 108 qui a inspiré les premières législations européennes, le rythme s'est accéléré. La directive de 1995 sur la protection des données a été suivie par une seconde directive dès 2002, la directive e-Privacy revue dès 2009. Par ailleurs, l'article 7 de la Charte des droits fondamentaux de l'Union européenne, adoptée le 12 décembre 2007[5], consacre la valeur quasi actuellement en cours de remplacement par un règlement constitutionnelle du droit à la protection des données. Sans doute, les besoins de protection de notre vie privée et de nos données face aux progrès technologiques ont rapidement exigé l'adoption de nouveaux droits pour la personne concernée, la consécration de nouveaux principes et définitions, voire, enfin, un nouveau champ d'application territorial. Dès 2012, les acteurs institutionnels européens se remettaient à l'ouvrage pour aboutir en 2016 à l'adoption du Règlement général de protection des données (le RGPD), en vigueur depuis juin 2018. Le mouvement s'arrête-t-il là ? Cinq ans après l'adoption du RGPD, des préoccupations nouvelles voient le jour. La confrontation des dispositions du RGPD face en particulier aux enjeux liés à la multiplication des applications de l'IA introduit une mise en question du « modèle européen » de protection des données ou plutôt le renforcement de son effectivité et une approche plus centrée sur les risques.

10. Pour se faciliter la tâche et hâter la solution réglementaire favorable à la protection de l'outil technologique, le législateur utilise la plasticité des concepts juridiques. Il s'agit de profiter de l'interprétation large susceptible d'être donnée à un concept de droit pour élargir à l'outil technologique les dispositions liées à ce concept. Ainsi, l'approche fonctionnelle des notions d'écrit et de signature ont légitimé la valeur de la signature électronique, fixé certaines conditions et justifié le principe de non-discrimination entre, d'une part, la signature ou l'écrit papier et, d'autre part, la signature et l'écrit électronique. Le logiciel a été, dès 1987, qualifié

[5] *J.O.*, C.302, 14 décembre 2007. On sait que la Charte est jugée comme ayant une valeur « quasi constitutionnelle ». L'article 16 du Traité de Lisbonne sur le fonctionnement de l'Union européenne a entériné la création de ce droit nouveau.

d'œuvre pour permettre l'application des règles de droit d'auteur. On sait les dangers que parfois recèle l'utilisation de cette « plasticité », au service certes de l'économie de l'innovation, mais au détriment des valeurs qui fondent certains de nos concepts juridiques. Ainsi, où sont les requis d'originalité et comment assurer les exceptions que la loi sur le droit d'auteur institue au bénéfice de certaines libertés ou de l'intérêt général ? Dernier exemple, faut-il, comme le Parlement l'avait un moment souhaité, accorder la « personnalité juridique » au robot, au motif que son intelligence vaut bien celle des humains et peut causer des dommages ou créer des œuvres ?

2. L'application efficace de la règle, réflexion majeure du droit du numérique

11. Au-delà de ces raccourcis législatifs, nous distinguerons une caractéristique propre à l'application du droit du numérique, liée à ce que nous avons appelé le temps accéléré du numérique. Il s'agit de la multiplication des délégations. Elle s'opère vis-à-vis de divers acteurs : les premiers sont indiscutablement les autorités administratives indépendantes créées par les textes européens ou en vertu de ceux-ci (a) ; la seconde délégation concerne le secteur privé lui-même, sujet de la réglementation, mais chargé de mettre en œuvre celle-ci (b). La jurisprudence s'arroge un pouvoir important d'interprétation des dispositions réglementaires (c). Enfin, la technologie se voit confier dans certaines réglementations la mission de veiller à l'effectivité de la norme (d).

A) Les autorités administratives indépendantes

12. Afin de répondre aux exigences d'encadrement d'une réalité technique sans cesse mouvante, les législations européennes ont pris l'habitude de confier à des autorités administratives indépendantes le soin d'intervenir soit à l'occasion d'un litige particulier mais également lorsqu'il s'agit de conseiller, de recommander, voire d'intervenir au fur et à mesure de l'apparition de technologies innovantes au vu des risques y liés. Ainsi, nombre de textes créent ainsi des agences ou des autorités européennes en charge d'assurer la cohérence des actions des autorités nationales et de veiller à une interprétation et application uniformes des textes. Ces autorités s'expriment par voie de « Lignes directrices », de recommandations, d'avis, de rapports, et conseillent la Commission dans son œuvre réglementaire. Sans être exhaustif, citons : l'EDPB en matière de protection des données, l'ENISA, en matière de cybersécurité, le Groupe de coordination

en matière de dispositifs médicaux, le Comité européen de l'intelligence artificielle, le Groupe des régulateurs européens pour les services de médias audiovisuels (ERGA), le BEREC (Body of European Regulators for Electronic Communications ou, en français, l'ORECE) (ce dernier fournit un appui administratif et professionnel à la Commission européenne, en matière de réglementation des télécommunications), enfin, les futures autorités nationales de supervision en matière d'intelligence artificielle, etc.

13. Sans vouloir remettre en cause l'intérêt de telles autorités administratives indépendantes ayant donc un statut d'autonomie vis-à-vis des autorités étatiques, on soulève cependant deux difficultés.

– La *prolifération d'autorités administratives* créées par de nombreux et récents textes en droit du numérique rend difficile l'examen de manière transversale des technologies innovantes et de leurs impacts ou la solution d'un litige qui met en cause les diverses thématiques envisagées séparément dans le cadre réglementaire. La culture en silo propre à chacune de ces autorités, dont par ailleurs les prérogatives sont différentes, empêche cette analyse globale d'un phénomène[6]. Pour ne prendre que l'exemple[7] de l'utilisation, par les plateformes numériques, de systèmes de recommandation et de profilage des internautes, il s'agit bien là d'un problème touchant à la protection des données, à la liberté d'expression, à la régulation des médias, à la concurrence et à la protection des consommateurs. On ajoute que les questions de préséance et de priorité dans la résolution de conflits entre les différents points de vue peuvent à terme éroder leur crédibilité[8] – le second point concerne la multiplication des textes pris par ces instances qui, sous prétexte d'interprétation, ajoute encore à la complexité des textes initiaux et rend le droit de plus en plus introuvable, certes un droit doux, mais qui s'aviserait de se soustraire aux « opinions » « recommandations », « *best practices* ».

[6] Cette nécessité d'une approche transversale ne peut, à notre avis, être rencontrée que par une clarification du rôle et des compétences de chaque catégorie d'autorités administratives, mais, surtout, par la création institutionnalisée de lieux de dialogue entre ces différents organes, sans quoi on risque des interventions dans des sens contradictoires, voire des rivalités entre instances.

[7] Autre exemple, la réglementation des voitures connectées touche à des questions du choix de l'infrastructure (5G ou WiFi), de protection des données, d'interopérabilité, de normes de sécurité.

[8] On relèvera, à l'occasion de la désignation des organes nationaux de supervision proposés en matière d'IA, la revendication des autorités de protection des données d'assurer cette compétence, alors même que les enjeux de protection des données ne constituent qu'une partie des risques à envisager lors de l'évaluation des systèmes d'IA. Sans doute, une des premières initiatives de réglementation transversale d'une technologie. Exemple à suivre ?

Ainsi, pour ne reprendre que l'exemple de la protection des données, le nombre sans cesse croissant de textes émis par le CEPD[9], en sus du ou interprétant le RGPD, donne le vertige à l'entreprise qui souhaite être le bon élève de la classe.

B) Le secteur privé

14. La délégation de l'œuvre régulatrice aux fins d'en garantir à la fois l'adaptation facile et l'effectivité se conçoit également par la reconnaissance, voire la promotion de codes de conduite, de bonnes pratiques, de labels, de certificats sous toutes leurs formes et appellations et dont la rédaction, la conception ou l'octroi sont abandonnés au secteur privé : soit l'autorégulation. Certes, nombre de textes réglementaires de l'Union européenne réservent à cette source normative une place, mais il faut bien reconnaître que cette place est sérieusement encadrée. La volonté de l'Europe d'atteindre ses objectifs explique sa préférence pour la norme publique et sa défiance vis-à-vis d'une autorégulation difficilement contrôlable et surtout apanage des puissants. Cette attitude n'est pas en contradiction avec des formes de corégulation[10] que, dans de précédents

[9] En 2009, par exemple, le CEPD a adopté plus de cent avis de contrôle préalable, portant essentiellement sur des questions telles que les données médicales, l'évaluation du personnel, le recrutement, la gestion du temps de travail, les outils d'enregistrement téléphonique et les enquêtes de sécurité. Ces avis sont publiés sur le site web du CEPD et leur mise en œuvre fait l'objet d'un suivi systématique. À noter qu'au nombre s'ajoute la longueur des avis et recommandations, ainsi, l'avis tout récent sur les méthodes de calcul des amendes administratives en cas de violation des dispositions du RGPD comprend pas moins de quarante pages.

[10] Cette tendance se retrouve dans de nombreux textes et, parfois, de manière explicite, comme dans ces considérants (n^os^ 12 et 14, traduits par l'article 4*bis*) de la directive « services audiovisuels » : « Les États membres devraient, dans le respect de leurs différentes traditions juridiques, reconnaître le rôle que peut jouer une autorégulation efficace en tant que complément aux mécanismes législatifs, judiciaires et administratifs existants, ainsi que l'utilité de sa contribution à la réalisation des objectifs de la directive 2010/13/UE. Toutefois, si l'autorégulation peut constituer une méthode complémentaire pour la mise en œuvre de certaines dispositions de la directive 2010/13/UE, elle ne devrait pas pouvoir se substituer aux obligations qui incombent au législateur national. La corégulation, dans sa forme la plus simple, assure un lien juridique entre l'autorégulation et le législateur national, dans le respect des traditions juridiques des États membres. Dans la corégulation, le rôle de régulateur est partagé entre les parties prenantes et les pouvoirs publics ou les autorités ou organismes de régulation nationaux. Le rôle des autorités publiques compétentes comprend la reconnaissance du dispositif de corégulation, l'audit de ses procédures et son financement. La possibilité d'une intervention de l'État devrait exister, dans le cadre de la corégulation, lorsque les objectifs du système ne sont pas atteints… ». Même remarque à propos de la récente proposition de « *Data Act* » (proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des

textes, nous qualifions de descendantes, c'est-à-dire que les mécanismes privés de régulation sont certes promus, mais sévèrement encadrés par une réglementation qui en fixe les balises, voire contrôlés par les autorités administratives indépendantes mises en place ou par la Commission elle-même[11]. Cette tendance est illustrée par la façon dont, en matière de désinformation, après avoir accepté en 2018 une autorégulation par les acteurs majeurs du marché, la Commission fit volte-face. En effet, l'Union européenne, après avoir suscité et salué l'existence d'un *Code of Practice on Disinformation* signé en septembre 2018 par les grands opérateurs de réseaux sociaux (Twitter, Facebook, YouTube, Instagram, Microsoft), constate, deux ans après, l'échec de cette méthode de régulation et se prononce pour une intervention plus proactive. Outre le lancement de la proposition du DSA déjà mentionnée, la Commission publie le 26 mai 2021 – le titre est évocateur – les « Lignes directrices pour renforcer le Code de conduite relatif à la désinformation ». Elle définit, cette fois de manière ferme, les engagements des opérateurs sociaux dans le cadre de la lutte contre la désinformation. Le retour à la prédominance d'une réglementation publique semble donc bien acquis dans ce domaine comme dans d'autres, objets du droit du numérique[12].

15. La compliance et l'approche préventive des risques : les obligations d'évaluation internes. Ce souci d'une effectivité renforcée et rapprochée explique l'imposition de mécanismes de *compliance* interne. Le RGPD (art. 37 et s.) oblige certaines institutions à nommer un délégué à la protection des données, jouissant d'un statut lui assurant une certaine protection et disposant de nombreuses compétences et missions afin de veiller au respect du RGPD. D'autres textes ont, depuis, appliqué ce même mécanisme. Ainsi, la proposition dite DSA oblige, d'une part, les plateformes à instituer des systèmes internes de traitement des réclamations, chargés de veiller à la légalité des décisions prises automatiquement ou non par la plateforme et, d'autre part, les très larges plateformes à désigner

données [règlement sur les données, février 2022, en abrégé *Data Act*]), proposition née en particulier de l'échec relatif du SWIPO [SWItching Cloud Providers and POrting Data] et des codes de conduite qui visaient à établir un meilleur partage des données entre entreprises (mise à disposition de contrats modèles, incitants de divers ordres).

[11] Pour un exposé plus complet des relations entre la réglementation européenne, l'autorégulation et la *lex informatica*, lire Y. Poullet, « Vues de Bruxelles. Modes alternatifs de régulation et libertés dans la société du numérique », in C. Castets-Renard *et al.* (dir.), *Enjeux internationaux des activités numériques*, Bruxelles, Larcier, 2020, pp. 91-137.

[12] N. Bontridder et Y. Poullet, « La 'cancel culture', la technologie et le rôle des plateformes à l'aune du principe de la liberté d'expression », *J.T.*, 17 décembre 2022, pp. 657 à 670.

un ou plusieurs responsables de la conformité au Règlement[13]. L'article 15 du Règlement de 2017 sur les dispositifs médicaux prévoit que « les fabricants disposent au sein de leur organisation d'au moins une personne chargée de veiller au respect de la réglementation possédant l'expertise requise dans le domaine des dispositifs médicaux ». Inscrite au sein de l'institution, cette personne au statut protégé veille à une application des réglementations immédiate et adaptée aux besoins de l'organisation.

La même volonté réglementaire justifie pleinement le passage d'une rédaction légale classique – fondée sur la définition de contenus comportementaux à respecter et, en cas de non-respect, sur la répression ou la sanction *a posteriori* des infractions à la réglementation – à *une approche* a priori *fondée sur l'obligation d'évaluation des risques*, soit la mise sur pied d'une procédure en la matière et du contrôle du respect de cette procédure. L'approche préventive fondée sur les risques semble être une caractéristique des textes réglementaires européens récents. L'exemple déjà cité du « *Privacy Impact Assessment* », introduit par le RGPD, déplace ainsi le champ d'intervention de la réglementation vers une démarche préventive d'écartement des risques par la nécessité de mise sur pied d'une procédure de leur évaluation dès la conception du traitement. La même idée traverse les autres règlements cités au paragraphe précédent. En particulier, la proposition d'*AI Act* développe à loisir cette procédure, définissant ses étapes, son contenu, insistant sur la participation de tous les acteurs intéressés, etc. On louera cette manière de faire, certes plus lourde administrativement et qui, selon nous, ne peut être justifiée que dans les cas de risques importants.

C) La jurisprudence

16. Sans doute, ne peut-on point parler ici de délégation dans la mesure où c'est l'essence même de la fonction juridictionnelle d'interpréter les textes réglementaires, face à des faits dont la survenance échappait au législateur au temps de son adoption et dans la mesure permise par les silences, les obscurités, les lacunes de la loi, les textes réglementaires. Les juges ont ainsi exploité la « plasticité » des concepts réglementaires de manière parfois osée afin de répondre aux défis posés par les innovations technologiques. Deux exemples suffiront : en 2009, les juges de la Cour constitutionnelle allemande, saisis de la question de la validité de

[13] Art. 32.2 : « Les très grandes plateformes en ligne désignent uniquement comme responsables de la conformité des personnes qui disposent des qualifications professionnelles, des connaissances, de l'expérience et des aptitudes nécessaires pour mener à bien les tâches visées au paragraphe… ».

l'utilisation d'un *spyware* par la police aux fins de découverte de l'auteur d'une infraction, ont jugé illégale une telle pratique (sauf en cas de crimes graves) sur la base d'un raisonnement assimilant l'ordinateur à une maison virtuelle et ont donc affirmé l'interdiction de pénétrer ce périmètre protégé par l'article 8 de la CEDH en accordant à son possesseur de l'ordinateur une garantie contre toute intrusion policière. Plus récemment, la Cour de justice de l'Union européenne a considéré, afin de lui appliquer les multiples prescrits du règlement de 2017 en matière de dispositif médical, le logiciel d'aide à la prescription médicale comme un « dispositif médical »[14]. En revanche, nonobstant la pression des banques, au nom de l'interprétation restrictive du droit pénal, les juges, sans doute après quelques hésitations ont rejeté la qualification d'escroquerie aux retraits d'argent pratiqués avec une carte bancaire volée (tromper une machine n'est pas tromper une personne) et ont ainsi renvoyé le législateur à ses devoirs.

17. Ce dernier propos renvoie à une autre conséquence de l'intervention des tribunaux. Ne peut-on voir, dans certaines décisions mettant en cause l'adéquation d'une intervention réglementaire à des principes législatifs, l'aiguillon judiciaire puissant forçant l'autorité publique à réviser ses textes ou à en adopter de nouveaux ? On songe certes aux arrêts *Schrems* en matière de protection des données et de flux transfrontières, considérant les accords US-UE comme non conformes aux exigences de protection adéquate, interprétée comme protection quasi équivalente ; on songe à l'arrêt *Uber* qui force à revoir la qualification d'Uber, mais plaide également pour une réglementation sectorielle proportionnée[15]. Ainsi, si l'interprétation jurisprudentielle, large, peut retarder la nécessité d'une révision de la loi, rédigée de manière stricte, elle peut, également, la hâter.

[14] La Cour (C.J.U.E., 7 décembre 2017, *SNITEM et Philips France c. Premier Ministre*, aff. C.329/16, cons. n° 21) a même précisé à propos de logiciel d'aide à la prescription qu'« un logiciel dont l'une des fonctionnalités permet l'exploitation de données propres à un patient aux fins notamment de détecter des contre-indications, les interactions médicamenteuses et les posologies excessives, constitue, pour ce qui est de cette fonctionnalité, un dispositif médical, et ce, même si un tel logiciel n'agit pas directement dans ou sur le corps humain ».

[15] Dans cet arrêt du 20 décembre 2017, la Cour de justice décide « qu'un service d'intermédiation, tel que celui (d'Uber), qui a pour objet, au moyen d'une application pour téléphone intelligent, de mettre en relation, contre rémunération, des chauffeurs non professionnels utilisant leur propre véhicule avec des personnes qui souhaitent effectuer un déplacement urbain, doit être considéré comme étant indissociablement lié à un service de transport et comme relevant, dès lors, de la qualification de "service dans le domaine des transports"… (dès lors) exclu du champ d'application de l'article 56 TFUE, de la directive 2006/123 et de la directive 2000/31 ».

D) La technologie mise au service d'une effectivité du droit

18. La technologie peut servir à l'effectivité de la réglementation et, dès lors, prévenir des conflits potentiels par une intervention automatique *a priori* dictée par une régulation inscrite au cœur des systèmes technologiques mis en place. À cet égard, on souligne la façon dont les législations ont accueilli avec faveur l'aide apportée par la technologie à l'effectivité des dispositions réglementaires. Le RGPD insiste sur le principe du « *privacy by design* »[16] et, demain, d'« *ethical values by design* ». Les systèmes d'accès conditionnels réservent aux seules personnes autorisées l'accès aux données à caractère personnel ou les techniques de pseudonymisation constituent autant de mesures techniques de sécurité de nos données à caractère personnel. La directive « Copyright » de 2001 interdit tout contournement des systèmes techniques, ce qu'on pourrait qualifier de IPETS (*Intellectual Property Enhancing Technologies*) visant à protéger les œuvres[17]. Ces « *anticopyright devices* » sont nombreuses. Ainsi, les systèmes dits de « *Digital Copyrigt Management Systems* » (DCMS) permettent de régler l'utilisation des œuvres et d'empêcher la multiplication de copies, voire restreignent cette utilisation à un terminal précisé ou à la simple visualisation sans possibilité de copie. Les systèmes dits de « *watermarking* » permettent de signer des images grâce à quelques pixels et de détecter dès lors la reproduction partielle ou totale de l'œuvre. On peut de même parler de CPETS (*Consumer Protection Enhancing Technologies*) comme autant de mesures technologiques destinées à traduire les exigences légales, ainsi celles de l'écriture en gras de certaines clauses dites

[16] Soit l'article 25.1 du RGPD : « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ». Sur ce principe, lire EDPB, *Guidelines 4/2019 on Article 25: Data Protection by Design and by Default*, 13 novembre 2019.

[17] La directive européenne 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information met en place un système de protection juridique « contre le contournement de toute mesure technique efficace ». Ainsi, les hackers et autres pirates d'œuvres protégées techniquement seront visés, mais aussi les sites internet qui mettent à disposition des outils conçus pour le piratage, puisque la directive prohibe « la fabrication, l'importation, la distribution, la vente, la location, la publicité […] de dispositifs, produits ou composants ou la prestation de services », qui, de manière générale, permettent ou facilitent le détournement de la protection.

surprenantes, l'information sur les qualités du vendeur via un lien sécurisé vers une page web mentionnant les informations légales, la nécessité de récapitulatif des commandes, la distinction entre « information commerciale » et description du produit, la double signature. La personne concernée, l'auteur, le consommateur, le citoyen se réjouissent de cette traduction technologique des exigences de nos lois. Ceci dit, ces outils doivent trouver la limite de leur efficacité dans le cadre d'un examen de la conformité de la protection offerte aux limites imposées par le droit. Nous reviendrons sur ce point.

19. Plus discutable est le deuxième point : la technologie n'est plus là pour traduire une exigence réglementaire, elle en devient la condition de possibilité. Expliquons-nous. Ce qui, sans doute, est propre aux temps de crise, c'est que l'utilisation de l'outil trouve, à l'occasion de ces périodes de troubles, une légitimité qui fasse oublier au droit ses propres assises. Les mesures réglementaires prises frénétiquement aujourd'hui ou envisagées pour demain, dans le cadre de la lutte contre la pandémie, ont une portée restrictive des libertés, qui va plus loin que de simples limitations, mais constitue une remise en cause de l'essence même de celles-ci. Le numérique est omniprésent dans ces mesures : création de bases de données, qu'il s'agisse des personnes contaminées, vaccinées ou des soignants ; suivi des personnes, on songe ici aux systèmes mis en place dans nos mobilophones, chargés de détecter, parmi notre entourage, la présence ou non de personnes contaminées ; à l'utilisation de systèmes d'intelligence artificielle tantôt pour la recherche, tantôt pour le repérage de clusters, tantôt pour la prévention ; à l'usage de drones pour contrôler le respect des réglementations interdisant les déplacements ou les déplacements interdits, etc. Ce qui est ici affirmé à propos de la lutte contre le Covid, vaut, hier, pour la lutte antiterrorisme et, demain, pour rencontrer d'autres préoccupations d'intérêt général, comme la protection de l'environnement. On parle ainsi de « *solutionnisme technologique* »[18], c'est-à-dire

[18] « Courant de pensée originaire de la Silicon Valley qui souligne la capacité des nouvelles technologies à résoudre les grands problèmes du monde, comme la maladie, la pollution, la faim ou la criminalité. Le solutionnisme est une idéologie portée par les grands groupes internet américains qui façonnent l'univers numérique. Lors de l'édition 2008 du festival South by Southwest, Mark Zuckerberg, fondateur de Facebook, déclarait : « Le monde étant confronté à de nombreux enjeux majeurs, ce que nous tentons de mettre en place en tant qu'entreprise, c'est une infrastructure sur laquelle s'appuyer pour en dénouer un certain nombre ». Dans le même esprit, Eric Schmidt, président exécutif de Google, annonçait lors d'une conférence en 2012 : « Si nous nous y prenons bien, je pense que nous pouvons réparer tous les problèmes de monde » (F. LAUGEE, Solutionnisme, *Revue européenne des médias et du numérique*, n° 33, 2014, repris sur le site de la revue le 30 juillet 2021 : https://la-rem.eu/2015/04/solutionnisme/.

le recours facile de la réglementation au déploiement de l'outil technologique pour répondre au défi posé par l'urgence des situations avec la croyance que ce recours permettra de résoudre le problème. Ainsi, sans le dire, s'installe, de manière durable, l'état d'exception à travers la mise sur pied, en temps de crise, d'outils technologiques. Si l'utilité, même contestable, de la création et du fonctionnement de ces outils peut se justifier en un moment de crise, il est à craindre leur maintien au nom des services rendus, des intérêts de ceux qui les gèrent ou y contribuent, des investissements y consentis et de l'habitude de leur présence prise par des citoyens devenus dociles. Si l'état d'exception explique aisément le recours au numérique, à son tour, le numérique s'empare, avec *in fine* la complicité inconsciente des populations, de l'état d'exception pour rendre cette « exception permanente ».

20. La tentation de la délégation réglementaire au numérique du respect de la loi, déjà illustrée par l'adoption en temps de crise de mesures technologiques, prend, avec les développements de l'intelligence artificielle, en particulier grâce aux outils de « *machine learning* », une autre dimension : celui de pouvoir se passer dorénavant de l'intervention humaine dans le contrôle du respect de la loi. Prenons quelques exemples : les systèmes de détection automatique des contenus (textes ou images) des messages permettent de déprioritiser, voire de bloquer automatiquement, certains messages jugés indésirables ; d'autres systèmes sont utilisés pour repérer les bots sociaux ou les « *deepfakes* » ; d'autres encore servent à la lutte contre les copies illicites et leurs « intelligences » repèrent l'utilisation d'œuvres par des personnes non autorisées. Ainsi, les universités utilisent à cet égard des logiciels capables de repérer le plagiat d'étudiants, mais également de soi-disant auteurs, se nourrissant de la prose ou de travaux de collègues. Les systèmes d'accès conditionnels qui réservent aux seules personnes autorisées l'accès aux données à caractère personnel ou les techniques de pseudonymisation sont autant de mesures techniques de sécurité de nos données à caractère personnel. Enfin, les textes sur la désinformation[19] préconisent la mise en œuvre d'outils capables de lutter contre la désinformation, à tel point qu'on peut parler d'une tentation de délégation du droit à la machine de manière à garantir pleinement l'application des législations[20]. Si cette délégation peut présenter un avantage

[19] Voy. *supra*, n^os^ 8 et s.

[20] À propos des liens entre droit et technologie : Y. POULLET, « Technology and law: From alliance to challenges », in U. GASSER (éd.), *Information Quality Regulation: Foundations, Perspectives and Applications*, Baden-Baden, 2004.

pour le régulateur[21], il n'empêche qu'elle comporte des risques que progressivement les législateurs ont souhaité prendre en compte, en mettant quelques balises à l'utilisation des systèmes technologiques créés à l'appui des législations.

21. Notre propos se limite ici à énoncer quelques principes qui, dès maintenant, devraient entourer le développement et l'utilisation des systèmes technologiques, en particulier ceux utilisant la technologie d'intelligence artificielle. On cite : premièrement, la conformité à la loi ; deuxièmement, la transparence ou du moins l'intelligibilité des systèmes utilisés ; troisièmement, le dernier mot à l'humain ; quatrièmement, la nécessité d'une évaluation et d'une réflexion pluridisciplinaire sur l'impact du système tant sur les libertés, la justice sociale que sur le respect de la règle du droit ; cinquièmement, la responsabilisation des concepteurs et des fournisseurs de tels systèmes au-delà de celle des utilisateurs, des agents de l'administration ou des entreprises.

Ces principes permettent de circonscrire les dangers de la régulation que le fonctionnement des systèmes d'intelligence artificielle pourrait induire. On soulignera d'abord le fait que le fonctionnement de nombre de ces systèmes se fonde sur la technologie du *machine learning* qui se caractérise par une certaine opacité, dans la mesure où les agrégations qui conduisent à la décision (celle de juger un texte, une copie illicite de l'œuvre ; celle de considérer de tels propos comme une désinformation) ne reposent pas sur un raisonnement causal, mais font appel à des probabilités qui, par leur

[21] Ainsi, en matière de protection des données à caractère personnel, la détection automatique des contenus permet, par exemple, à des moteurs de recherche de bloquer, à la suite des demandes de déréférencement, des liens vers des sites reprenant des informations jugées illicites au regard du RGPD. Voy., à ce propos, l'arrêt de la C.J.U.E. du 24 septembre 2019 (*Google c. CNIL*, C-507/17 [espèce I]), qui oblige les plateformes offrant des services de moteur de recherche à « déréférencer » les sites qui contiennent des informations, y compris journalistiques, relatives à des données sensibles dépassées depuis le moment de leur publication : « Compte tenu des responsabilités, des compétences et des possibilités de l'exploitant d'un moteur de recherche en tant que responsable du traitement effectué dans le cadre de l'activité de ce moteur, les interdictions et les restrictions prévues à l'article 8, paragraphes 1 et 5, de la directive 95/46 ainsi qu'à l'article 9, paragraphe 1, et à l'article 10 du règlement 2016/679 ne peuvent […] s'appliquer à cet exploitant qu'en raison de ce référencement et, donc, par l'intermédiaire d'une vérification à effectuer, sous le contrôle des autorités nationales compétentes, sur la base d'une demande formée par la personne concernée ». Sur cette décision de la Cour européenne, depuis relayée par treize arrêts du Conseil d'État français, lire T. Leonard et Y. Poullet, « L'intérêt général comme arbitre du débat Vie privée *vs* Liberté d'expression », in Y. Poullet (dir.), *Vie Privée, transparence et démocratie*, Actes du colloque du REHNAM, Namur, le 28 novembre 2019, *Cahier du CRIDS*, n° 50, 2020, en particulier, le n° 26 qui décrit le risque ici aussi d'une délégation aux plateformes privées de juger, grâce à l'IA, du déréférencement ou non d'un site.

complexité, peuvent dépasser l'entendement humain. On note ensuite que ces systèmes peuvent aller au-delà du respect de la loi. Ainsi, pour ne reprendre que l'exemple des DRMS (*Digital Rights Management Systems*), on note que les algorithmes peuvent ne faire aucune différence entre des demandes licites d'accès ou de copies, par exemple à des fins de copie privée, pour des recherches scientifiques, à des fins de citation ou pour parodier l'œuvre, autant d'usages pourtant protégés par des exceptions légales. Pire, ces systèmes peuvent protéger les œuvres bien au-delà de ce que la loi autorise. Ainsi, la protection assurée par des systèmes de *watermarking* peut détecter quelques pixels communs à deux œuvres parfaitement originales et, dès lors, bloquer l'une d'entre elles. En réalité, certains systèmes protègent chaque partie de l'œuvre au-delà de la protection instaurée par le droit d'auteur, qui vise l'originalité de l'œuvre, et non de chacune de ses parties, fussent-elles minimes et non essentielles. Ensuite, on craindra, en matière de désinformation, la difficulté pour les systèmes de détecter certains faux positifs (p. ex., un article scientifique qui reprendrait pour les critiquer certains arguments complotistes) comme certains faux négatifs (p. ex., la représentation d'un faux discours de notre ministre de la Santé) et, toujours dans ce domaine, on épinglera le risque de biais : ainsi, telle plateforme considérera que le mot « antivax » est automatiquement synonyme de complot alors qu'il peut être lié à des discussions, par exemple, sociologiques sur la motivation des personnes opposées à la vaccination. Ce risque de biais, c'est-à-dire de distorsions conscientes ou inconscientes dans le traitement *cognitif* d'une information, qui conduisent à distinguer ou, au contraire, confondre des situations là où l'examen de la réalité conduit à éviter de telles conclusions est d'autant plus à souligner que cette erreur de raisonnement s'inscrit automatiquement dans le fonctionnement du système et, donc, conduit à des conclusions ou décisions invalides.

Une autre préoccupation concerne le fait que l'automatisation galopante des processus de décision engendre une acceptation quasi automatique de la validité et de la pertinence des décisions prises ainsi automatiquement et, corrélativement, un désinvestissement et une déresponsabilisation de décideurs « humains »[22]. Enfin, la délégation dite à la technologie cache en réalité une délégation aux personnes qui programment ou utilisent de tels algorithmes, en particulier, les plateformes de communication et d'information qui, par là, disposent du pouvoir d'inscrire leur « loi » dans

[22] À cet égard, les experts AI de la Commission relèvent que « *the results produced by the machine, using more and more sophisticated software, and even expert system, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities* ».

le fonctionnement de ces derniers. À tous ces dangers que recèle l'utilisation de la technologie comme mode de contrôle particulièrement effectif et rapide du respect de la réglementation, le droit, sans pour autant rejeter le bénéfice de la technologie[23], se doit de se montrer circonspect et exiger l'audit ou du moins l'évaluation préventive des mécanismes, permettre la contestation facile de la décision et exiger la supervision humaine des décisions automatiques *in fine*. Le propos suivant prolonge cette réflexion, le système technologique peut être un mode non seulement de contrôle du respect de la réglementation, mais, au-delà, également d'application de cette dernière.

III. Au-delà, la technologie comme « mode de conception et d'application de la réglementation »

22. La réflexion qui suit s'origine à partir d'une information lue sur le Net : le mot « ordinateur » aurait été trouvé par un professeur de lettres de la Sorbonne en 1955 et serait un adjectif désignant un « Dieu mettant de l'ordre dans le monde ». Le rapprochement avec le droit, qui prétend réguler nos sociétés, m'apparaissait évident. L'ordinateur aurait-il pour vocation de remplacer le droit ? Sans doute, prend-on l'habitude de

[23] On soulignera la décision du 21 juin 2022 de la C.J.U.E. qui concernait la possibilité d'utilisation de technologies de *machine learning* à l'appui du système PNR. La Cour rejette une telle utilisation en raison des dangers d'opacité et de biais que représentent de tels systèmes : « S'agissant des critères que l'UIP peut utiliser à cet effet, il convient de relever, tout d'abord, que, selon les termes mêmes de l'article 6, paragraphe 3, sous b), de la directive PNR, ces critères doivent être "préétablis". Ainsi que M. l'avocat général l'a relevé au point 228 de ses conclusions, cette exigence s'oppose à l'utilisation de technologies d'intelligence artificielle dans le cadre de systèmes d'autoapprentissage (*machine learning*), susceptibles de modifier, sans intervention et contrôle humains, le processus de l'évaluation et, en particulier, les critères d'évaluation sur lesquels se fondent le résultat de l'application de ce processus ainsi que la pondération de ces critères. Il importe d'ajouter que le recours à de telles technologies risquerait de priver d'effet utile le réexamen individuel des concordances positives ainsi que le contrôle de licéité requis par les dispositions de la directive PNR. En effet, comme M. l'avocat général l'a relevé, en substance, au point 228 de ses conclusions, compte tenu de l'opacité caractérisant le fonctionnement des technologies d'intelligence artificielle, il peut s'avérer impossible de comprendre la raison pour laquelle un programme donné est parvenu à une concordance positive. Dans ces conditions, l'utilisation de telles technologies serait susceptible de priver les personnes concernées également de leur droit à un recours juridictionnel effectif consacré à l'article 47 de la Charte que la directive PNR vise, selon son considérant 28, à garantir à un niveau élevé, en particulier pour contester le caractère non discriminatoire des résultats obtenus » (voy. C.J.U.E., 21 juin 2022, n^{os} 193 et s., ECLI:EU:C:2022:491).

« gouverner par les nombres », c'est-à-dire de légiférer en se référant aux indications, aujourd'hui, statistiques, demain, en fonction des résultats des algorithmes d'intelligence artificielle[24]. La loi obéit ainsi aux lois dictées par la technologie, dans la mesure où elle n'a plus besoin du temps long de la transformation des habitudes, sans doute aidée par les décisions des juges et les contrôles mis en place par les administrations policières et autres. Dictée dans son intervention par les « nombres », comme dit Supiot[25], elle peut en outre s'appuyer sur la technologie pour veiller à son application effective. Ainsi, la phrase d'Aristote reprise en exergue de ce propos : « Ce n'est pas la même chose de changer une technique et une loi ; la loi, en effet, pour se faire obéir n'a d'autre force que l'habitude, laquelle ne se manifeste qu'après beaucoup de temps, de telle sorte que passer facilement des lois existantes à d'autres lois, c'est affaiblir la puissance de la loi », ne trouve plus à s'appliquer dans la mesure où le temps du droit devient le temps du numérique. Fr. Ost, à propos de la réglementation Covid, relevait : « Il y eut ensuite la cohabitation entre un système juridique classique et une réglementation nouvelle relevant de ce qu'Alain Supiot a appelé la "gouvernance par les nombres", combien de mesures n'étaient-elles pas conditionnées par les chiffres et statistiques… Ces statistiques faisaient loi et déterminaient les politiques chiffrées… »[26]. Sans doute, le refuge, de plus en plus fréquent, de nos gouvernants derrière les chiffres « objectifs » et les vérités sorties de l'ordinateur peut s'interpréter comme une déresponsabilisation du politique. Les législations Covid en sont un exemple, mais on reconnaît la même tendance dans bien d'autres domaines, qu'il s'agisse de la fixation des salaires, des pensions, etc.

23. Si la technologie peut dicter sa loi au législateur, sans doute comme nous l'avons montré, avec une certaine complicité de ce dernier, la technologie devient l'outil d'application du droit. Qu'il s'agisse de déterminer la redevance fiscale, la pension, l'admissibilité d'un citoyen ou d'une entreprise à un avantage légal… pourquoi ne pas confier à la machine le soin de veiller au rapide, juste et neutre respect de la loi ou de la réglementation ? L'application de la loi se mue en un simple fonctionnement d'un système algorithmique. Le droit certes peut entourer ce recours à la

[24] A. Rouvroy, « L'usage des *big data* pour gouverner », *Politique, revue de débats*, 2020, pp. 115-119.

[25] A. Supiot, *La gouvernance par les nombres*, Cours au Collège de France (2012-2014), Paris, Fayard, 2015, 512 p., « Notre temps serait victime de "quantophrénie", de confiance immodérée et presque monomaniaque dans l'abstraction de chiffres et de nombres devenus le langage dominant de l'agir politique ».

[26] Fr. Ost, « Nécessité fait loi ? La santé n'a pas de prix ? Ce que le Covid fait au droit », in S. Parsa et M. Uyttendaele (dir.), *La pandémie de COVID-19 face au droit*, Limal, Anthemis, 2021, p. 32.

technologie de certaines précautions : ainsi, interdire les systèmes entraînant des risques inacceptables ; exiger l'évaluation des systèmes d'IA dès la conception de ceux-ci pour les « hauts » risques que la proposition de règlement énumère et dont nombre d'entre eux ressortissent à l'action de l'administration, ainsi en matière policière, d'éducation, d'emploi, etc. Les fournisseurs (*providers*) de systèmes IA à haut risque[27] se voient imposer de multiples devoirs[28]. La proposition impose, pour les systèmes dits à haut-risque, un système de gestion des risques qui implique le suivi de bonnes pratiques et l'évaluation préventive des systèmes (absence de biais, qualité des données…)[29] et, surtout, de surveillance humaine (*human oversight*)[30]. Cette obligation préventive des systèmes trouve dans le RGPD sa son double : l'article 35 exige pour les responsables de traitements de données à caractère personnel présentant un risque élevé[31] le soin de procéder à un

[27] Soit, selon la définition de la proposition (art. 1er (2)) : « fournisseur », 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 [;] ». L'utilisation des mots « mise sur le marché » exclut-elle les autorités publiques et les institutions universitaires ?

[28] Art. 16 du projet de règlement : « Les fournisseurs de systèmes d'IA à haut risque :
(a) veillent à ce que leurs systèmes d'IA à haut risque soient conformes aux exigences énoncées au chapitre 2 du présent titre ;
(b) mettent en place un système de gestion de la qualité conforme à l'article 17 ;
(c) établissent la documentation technique du système d'IA à haut risque ;
(d) assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque, dans la mesure où ces journaux se trouvent sous leur contrôle ;
(e) veillent à ce que le système d'IA à haut risque soit soumis à la procédure d'évaluation de la conformité applicable, avant sa mise sur le marché ou sa mise en service ;
(f) respectent les obligations en matière d'enregistrement prévues à l'article 51 ;
(g) prennent les mesures correctives nécessaires si le système d'IA à haut risque n'est pas conforme aux exigences énoncées au chapitre 2 du présent titre ;
(h) informent les autorités nationales compétentes des États membres dans lesquels ils ont mis le système d'IA à disposition ou en service et, le cas échéant, l'organisme notifié, de la non-conformité et de toute mesure corrective prise ;
(i) apposent le marquage CE sur leurs systèmes d'IA à haut risque afin d'indiquer la conformité au présent règlement, conformément à l'article 49 ;
(j) à la demande d'une autorité nationale compétente, apportent la preuve de la conformité du système d'IA à haut risque aux exigences énoncées au chapitre 2 du présent titre ».

[29] L'article 10 mentionne divers devoirs liés à la gouvernance des données, ainsi, le *testing* et la validation des choix de design et des données prises en compte, l'examen des biais possibles, etc. On ajoute les obligations de documentation technique, par ailleurs détaillée dans son contenu et son format par l'annexe IV de la proposition, de *loggings*.

[30] Art. 14.1 : « La conception et le développement des systèmes d'IA à haut risque permettent, notamment au moyen d'interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant la période d'utilisation du système d'IA ». On notera le flou d'une telle disposition.

[31] L'article 35 du RGPD conduit à considérer les applications d'IA comme un « traitement à haut risque », en tout cas, dans les trois hypothèses suivantes. Ces trois hypothèses sont

Privacy Impact Assessment. On ajoute l'obligation d'informer de l'utilisation opaque de systèmes d'IA, par exemple, en cas de *chatbots*. Faut-il aller plus loin, et sur la base de la loi sur la transparence administrative, exiger la publication des algorithmes qui commandent le fonctionnement des systèmes IA utilisés par l'autorité publique ? Enfin, l'article 22 du RGPD affirme le droit de la personne concernée « de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ». Cet article appelle les remarques suivantes[32]. L'analyse de cette disposition laisse apparaître nombre de lacunes[33] ou, en tout cas, d'ambiguïtés. Que veulent dire « décision fondée exclusivement » ou « uniquement » ? Que penser de l'exception particulièrement invocable par l'administration : « [l'article 22. 1. reçoit exception lorsque la décision automatisée] est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée [;] » ? « [Ces] garanties appropriées […] devraient comprendre, selon le considérant n° 71 du RGPD, une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, *d'obtenir une explication quant à la décision* prise à l'issue de ce type d'évaluation[,] et de contester la décision ». Ainsi, le droit impose, à la toute-puissance du numérique, les temps humains de l'évaluation du système, de l'explication et de la contestation.

---

particulièrement pertinentes lorsqu'il s'agit de traitements utilisant des systèmes d'intelligence artificielle :

> « a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
>
> b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; ou
>
> c) la surveillance systématique à grande échelle d'une zone accessible au public ».

[32] De manière plus complète sur cet article et les multiples questions posées, ainsi que l'analyse des dispositions à ce propos du Code français des relations du public avec l'administration en date du 20 février 2020, lire Y. POULLET, « Le RGPD face aux défis de l'intelligence artificielle », *Cahier du CRIDS*, n° 48, 2020, pp. 175 et s.

[33] La décision dont parle l'article 22 doit viser une « personne (physique) concernée ». C'est la conséquence certes d'une législation centrée sur la protection de personnes individuelles, mais ne faudrait-il pas également prendre en compte le fait que des systèmes en particulier prédictifs visent des catégories de personnes : ainsi, les personnes habitant tel quartier, ayant tel type de comportement sur le Net, telle mobilité… ? Le risque est ici collectif et, de ce fait, mériterait *a fortiori* d'être pris en compte.

24. Dernière tentation de voir l'application du droit transformée en système algorithmique, celle du « juge robot », c'est-à-dire du remplacement du juge humain par un robot qui, sur la base d'un système d'IA, pourrait, comme c'est – dit-on – le cas en Estonie, trancher des litiges certes dans des domaines particuliers et peut-être concernant des montants limités. Le terme renvoie à un ensemble d'instruments logiciels utilisant des systèmes de *machine learning* qui, grâce à l'analyse corrélationnelle de grandes masses de décisions de justice, permettent aux juridictions[34] de prévoir autant qu'il est possible l'issue d'un litige… voire d'en décider l'issue. On connaît les arguments invoqués par certains[35] : la diminution des coûts, certes, mais surtout l'efficacité, la fiabilité[36] et la parfaite neutralité des décisions là où le juge humain est souvent suspecté de subjectivité.

[34] Les systèmes d'intelligence artificielle dans le domaine du droit apportent nombre de services non seulement aux juges, mais également aux auxiliaires de la justice, voire aux firmes qui les développent (éditeurs juridiques, sociétés informatiques travaillant dans le domaine juridique : les « LegalTech » : aide à la recherche, conseils juridiques, prévisions de l'issue d'un litige, voire médiation). Ces services sont offerts y compris aux acteurs traditionnels du droit comme les cabinets d'avocats, mais également directement aux citoyens ou aux entreprises. Cette exploitation en direct par des acteurs relevant de professions non soumises aux règles du barreau vers une clientèle crée des risques à la fois d'ubérisation de la profession de conseil juridique, mais également de non-respect de règles déontologiques propres à la profession d'avocats. Sans doute, on félicitera l'initiative prise par la CEPEJ (Commission européenne pour l'efficacité de la Justice) de rédiger la « Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement », adoptée à Strasbourg les 3 et 4 septembre 2018.

[35] Voy. l'ouvrage publié par A. Van Den Branden (*Les robots à l'assaut de la Justice*, Bruxelles, Larcier, 2018). L'auteur comparait systématiquement l'office du juge robot à celui du juge humain sur bien des critères et proclamait *in fine* la victoire du premier sur le second. La démonstration était séduisante, à défaut d'être pleinement convaincante. Callipel résume comme suit l'argumentation en faveur du robot, avant de s'en distancer : « En général, la plus-value des décisions algorithmiques se situe au plan de leur rapidité et de leur capacité à prendre en compte une quantité phénoménale de données premières, se conjuguant avec une analyse en temps réel et plus fine des différentes variables et contraintes. S'y ajoute cette "infatigabilité" propre aux machines et une résistance bienvenue à l'arbitraire des émotions ainsi qu'à toute distorsion cognitive. Un agent conversationnel est imperméable aux insultes, témoigne d'une équanimité d'humeur à toute épreuve et répétera avec courtoisie ses explications autant de fois que nécessaire sans changer de ton ni d'attitude. On se sent conforté à l'idée qu'une décision algorithmique ne va pas dépendre de la plus ou moins bonne impression laissée par des usagers, d'une mémoire (in)consciemment sélective ou d'émotions négatives et, encore moins, de l'heure de la journée ».

[36] À titre d'exemple, en 2016, un groupe de chercheurs britanniques et américains a élaboré un algorithme de type machine à vecteurs de supports (SVM) capable d'arriver aux mêmes verdicts que les juges de la Cour européenne des droits de l'homme dans 79 % des cas en croisant les arguments des parties, les faits et le droit positif pertinent.

Il n'empêche que bien des arguments peuvent être opposés à cette informatisation de la décision judiciaire[37]. Le premier est la question des biais et des choix implicites qui seront faits à l'occasion de la construction des modèles. Le deuxième craint que l'application des résultats de décisions passées n'aboutisse à un certain conservatisme du droit et surtout nie la possibilité pour un juge d'une interprétation innovante du droit. P. Berlioz attire l'attention sur le risque lié à la justice décidée par ordinateur : « […] Mais ces outils ne font que mettre en lumière une tendance passée. Ils ne permettent dès lors de dégager que des présomptions, non des prédictions. Et ces présomptions peuvent être renversées par un travail d'analyse et de conviction, de sorte que la solution résulte nécessairement de ce travail, non du simple constat qu'à une question donnée, il a majoritairement été apporté une certaine réponse ». Le troisième est celui de l'opacité du fonctionnement de tels systèmes. Le droit du justiciable à l'explication de la décision prise par le juge se heurterait à cette non-transparence. Les questions des choix algorithmiques et de la transparence de leur fonctionnement à l'occasion d'un litige concret se posent en effet différemment dans le cadre de l'utilisation par le juge que vis-à-vis d'une pure utilisation privée. L'office du juge est en effet un service public dont chacun doit pouvoir connaître les règles de fonctionnement[38]. Il est également une instance humaine, capable à la lecture des faits et sensible aux accents des plaideurs, de proposer une solution inédite qui, à défaut d'être celle dictée immédiatement par les algorithmes, sera celle dictée par sa réflexion qui peut être longue et sa conscience humaine.

Conclusions : ce que le numérique « fait » au droit et ce que le droit « fait » au numérique

25. Il est incontestable que le numérique bouleverse à un rythme vertigineux nos sociétés, nos modes de produire, de consommer, de vivre avec autrui, voire nos identités. L'appréhension de ces transformations

[37] Sur ces différents arguments, l'excellent article de Boris Barraud : « Un algorithme capable de prédire les décisions des juges : vers une robotisation de la justice ? », *Les Cahiers de la justice*, Paris, Dalloz, 2017, pp. 121-139.

[38] À cet égard, la question des critères pris en charge par l'algorithme est délicate. Ainsi accordera-t-on plus de poids à un arrêt de la Cour de cassation, tiendra-t-on compte du nombre de décisions dans tel ou tel sens ou préférera-t-on des critères plus qualitatifs ? Quel poids accordera-t-on à la langue d'origine du jugement ? Comment s'opèrent les corrélations, en particulier jusqu'où va-t-on dans la prise en compte des faits ?

s'accommode mal du rythme du droit ; il en révolutionne les piliers tant temporels que spatiaux ; il heurte l'approche sectorielle et par branches du droit, il questionne les concepts mêmes de nos ordres juridiques jusqu'à celui de l'identité. À ces défis sociétaires et à son propre fonctionnement, le droit se doit de répondre. Ainsi se conçoit un droit du numérique plus agile dans sa formulation réglementaire, considérée comme jamais achevée ; un droit qui, au-delà des bouleversements apparents qu'engendre le donné technique, refuse de céder à l'innovation juridique servile aux promoteurs de cette technologie, mais au contraire maintient la réflexion sur la *ratio legis* des prescriptions prises dans un contexte alors non numérique et qui, dès lors, donne, tant que faire se peut, à la plasticité des concepts juridiques son plein sens ; un droit qui multiplie les relais et, de ce fait, perd parfois le citoyen dans le dédale des sources dérivées, qu'il s'agisse de celles émanant des autorités administratives indépendantes, d'une jurisprudence hardie ou de l'autorégulation. ; enfin, un droit qui se tourne vers les individus et les entreprises, pour en faire les premiers contrôleurs du respect des réglementations, et qui en particulier invite les acteurs du marché, au regard des risques que présente l'innovation, à configurer, dans le système technologique lui-même, les garanties qui permettront d'assurer le respect des réglementations. Le temps du droit, c'est également ce déplacement dans le temps du contrôle de son application : ce contrôle devenu d'abord préventif dans les mains de ceux qui doivent y obéir, le contrôle externe et *a posteriori* n'étant plus que résiduaire.

Ce que le numérique fait au droit ne se limite pas à ces premières considérations. Le propos met en lumière, nous l'avons dit, la délégation du droit au numérique comme outil commode et rapide de sa propre légitimité et de son effectivité. Le numérique fait rêver le juriste : n'est-il pas un outil capable d'appliquer, voire de définir, le droit plus objectivement, plus efficacement que l'humain, qu'il soit législateur, agent de l'administration ou juge ? La « vérité » sortie de l'ordinateur éclipsera bientôt le travail patient des agents en charge de faire respecter, d'appliquer, voire, en cas de litige, de dire le droit.

26. Une constante nous semble ressortir des diverses considérations esquissées ci-avant. En définitive, ce que le droit cherche à maintenir, c'est la présence de l'homme afin qu'il ne perde pas la maîtrise de la technologie. Même si sa réalité est souvent illusoire, la place du consentement libre, informé, univoque et spécifique comme cause de légitimité des traitements de données à caractère personnel est rappelée. Mais, au-delà, il est demandé que la mise sur pied et le fonctionnement de systèmes numériques à haut risque soient l'objet d'un contrôle humain, si possible interdisciplinaire, tant préventif que continu sur la base de la formule « *human*

in the loop, human on the loop, human in command »[39]. Ensuite, nous nous sommes attardé sur l'exigence de nos réglementations de ne pas confier à la seule machine le soin de décider et de faire place à la nécessité d'une explication humaine et d'un recours auprès d'une instance composée de femmes et d'hommes. Enfin, on le pressent, la création de commissions d'éthique, lieux ouverts et interdisciplinaires de discussion, en charge de l'évaluation de l'impact individuel, collectif et sociétaire de nos artifices numériques de notre intelligence humaine, témoigne de la nécessité de penser le droit comme un outil indispensable de la maîtrise humaine de l'évolution de notre société numérique. Le temps du droit doit consacrer, face au temps du numérique, ce temps obligé d'intervention tant de la conscience et de la raison individuelles que de la réflexion collective. Voilà ce que le juriste doit à l'historien, cher Bruno.

[39] Suivant la formule proposée par le HLGE (High Level Group of experts on AI). Sur ce groupe et ses travaux, https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence et notamment sa publication des *Lignes directrices en matière d'éthique pour une IA digne de confiance* (publiées le 8 avril 2019), texte disponible sur le site : *Ethics Guidelines for Trustworthy AI*, Publications Office of the EU (europa.eu), https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.