BINAIRE
L'informatique : la science au coeur du numérique

05 FÉVRIER 2021

Magie numérique et défis juridiques

Un nouvel « Entretien autour de l'informatique ». Christophe Lazaro est Professeur au Centre de Philosophie du Droit, à l'Université de Louvain, et membre du Comité National Pilote d'Éthique du Numérique (France). Nous poursuivons avec lui le voyage commencé avec Célia Zolynski sur le droit du numérique. Christophe nous amène aux frontières du droit, de la philosophie et de l'anthropologie.

Cet article est publié en collaboration avec theconversation.fr.

Christophe Lazaro, UCLouvain

B : Tu es juriste. Mais en préparant l'entretien, nous avons découvert que tu étais aussi spécialiste d'autres domaines. Peut-être pourrais-tu commencer par nous dire d'où tu viens.

TL : Je suis au départ juriste, en effet. Au début de ma carrière, j'ai été avocat pendant une courte période. J''ai également étudié en parallèle la philosophie et l'anthropologie. Puis j'ai fait une thèse de droit assez tardivement, à 33 ans, à l'Institut Universitaire Européen de Florence sur les enjeux juridiques et philosophiques des rapports entre corps et prothèses. Je suis passionné par la question de la technique et du corps. Je pratique d'ailleurs le Tai Chi depuis des années. Ce qui me passionne, c'est surtout la rencontre entre l'être humain et les nouvelles technologies, d'un point de vue juridique bien sûr mais aussi anthropologique et philosophique.

B : Un de tes premiers travaux a porté sur les communautés de logiciel libre, plus particulièrement Debian.

TL : Oui. Ce travail reflète d'ailleurs bien la rencontre de mes intérêts croisés pour le droit et l'anthropologie. J'ai fait une étude anthropologique de la communauté dite virtuelle Debian. C'est une communauté très démocratique qui développe des systèmes d'exploitation basés exclusivement sur des logiciels libres. Elle est virtuelle parce que ses membres se rencontrent principalement sur Internet. C'était la première fois que j'avais vraiment l'occasion d'échanger avec des informaticiens. Dans mon labo d'alors, on travaillait sur le droit du numérique mais on ne parlait pas trop avec eux.

B : Tu as des compétences en informatique ?

TL : Je me vois un peu comme un « handicapé des machines » avec une grande soif de savoir parce que je n'y comprends pas grand-chose. Cela me pousse à poser des questions aux spécialistes. J'ai été bluffé par l'hyper-structure sociale et politique de la communauté Debian. J'ai d'ailleurs pu participer à cette communauté. C'était passionnant ! J'ai voulu comprendre comment ils fonctionnaient.

Ça a donné un livre. Ce genre d'études d'une communauté virtuelle était original pour l'époque. Avec le regain d'intérêt actuel pour les communs, cela vaut la peine d'aller regarder des communautés fondées sur cette notion de commun. Par exemple, à côté des communautés de logiciels libres, il y a des collectifs d'habitat groupé, des coopératives d'agriculture alternative ou des communautés d'éditeurs de Wikipédia. D'un point de vue anthropologique, ces initiatives interrogent l'essence même du concept de communauté. Comment peut fonctionner une communauté avec le don comme seule modalité d'échange et de coopération entre ses membres ?

B : Tu as aussi beaucoup réfléchi à l' « augmentation » de l'humain avec la technique, et aux questions que cela pose en terme de justice ?

TL : D'abord, pour moi, une technologie n'augmente pas, elle transforme. Un simple post-it que nous utilisons au bureau n' « augmente » pas la mémoire à proprement parler. Il permet d'organiser les tâches différemment, en transformant les actions à accomplir. Un sujet, par exemple, me passionne depuis ma thèse sur les prothèses : une fois la personne « transformée » par la technologie, que devient l'égalité ? Comment doit-on la traiter ? La technologie bouleverse les notions d'égalité et de mérite qui sont au cœur de nombreuses activités humaines. On peut parler d'Oscar Pistorius ou plus récemment de Blake Leeper, deux athlètes amputés équipés de prothèses souhaitant concourir au plus haut niveau aux côtés des « valide » . Mon ouvrage La prothèse et le droit (vous excuserez l'autopromotion) qui a remporté en France le prix du livre juridique en 2016, aborde ce type de questions. Maintenant, avec l'IA, on va de plus en plus loin et cela questionne radicalement la nature de certaines activités qui étaient autrefois l'apanage exclusif des humains.

Surveillance numérique @serab

B : Pour prendre un exemple concret de question que cela pose, des outils informatiques notamment basés sur l'IA aident les employés des entreprises. Mais ils posent aussi des problèmes en termes de surveillance excessive des employés. Comment gérer cela ?

TL : Dans l'entreprise, on propose des outils pour organiser et faciliter le travail, pour optimiser la coordination et l'effectuation des tâches. Mais ces outils peuvent aussi servir à de la surveillance. Est-ce que les avantages apportés par cette transformation du travail et du rôle de l'employé compensent les risques de surveillance qu'ils introduisent ? La loi devrait être là pour dissuader de certaines formes disproportionnées de contrôle des employés, mais le juriste d'aujourd'hui doit aussi être conscient des limites du droit face à l'ambivalence intrinsèque des technologies,. Je n'ai pas de solution pour empêcher les abus de ces technologies parce que celles-ci sont si géniales qu'on ne les voit pas, qu'elles

opèrent en toute discrétion, et qu'on ne sait pas comment elles fonctionnent. J'ajouterais même que plus grand est leur confort d'utilisation, plus elles « disparaissent ». Cette invisibilité rend les modes de résistances juridiques ou autres difficiles à mettre en œuvre.

B : Cette invisibilité est quand même relative. Avec le numérique, on peut garder des traces de tous les traitements. On pourrait argumenter que le numérique est au contraire beaucoup plus transparent.

CL : C'est là que ça devient intéressant. Il faudrait distinguer des régimes suivant la visibilité d'un processus. Du point de vue de l'employé, s'il ne peut pas voir la surveillance, le processus de surveillance est transparent. C'est en cela que je parle d'invisibilité car les effets de la technologie ne s'éprouvent plus, à travers le corps et les sens. Et avec l'IA, on ira vers encore plus d'invisibilité en ce qu'on ne sait souvent même pas expliquer les choix des logiciels. Je pense que c'est un sujet à étudier.

B : Qu'est ce qui pourrait débloquer la situation ?

TL : L'anthropologie. (rire) Une alliance entre des informaticiens, des philosophes, des juristes… On est par essence en pleine interdisciplinarité. Les questions ne sont pas philosophiquement nouvelles. Mais, plutôt que d'en parler abstraitement, il faut s'attaquer à des questions précises sur des pratiques, dans des situations d'usage. Pour moi, la recherche a aujourd'hui atteint un seuil. D'un point de vue juridique ou éthique, elle tourne en rond en ressassant les mêmes questions et principes. Plutôt que de disserter sur l'éthique de l'IA d'une manière désincarnée, plutôt que de proposer un énième réflexion sur le dilemme du tramway et les véhicules autonomes… il faut envisager les choses de manière empirique et poser des questions en situation.

Par ailleurs, pour développer une éthique de l'IA, il faudrait se mettre d'accord d'abord sur une véritable méthodologie et l'appliquer ensuite en faisant collaborer des points de vue interdisciplinaires. Comme toute discipline, l'éthique ça ne s'improvise pas et, dans l'histoire récente, nous ne sommes qu'aux premiers balbutiements d'une coopération entre sciences humaines et sciences dures.

B : Qu'est-ce que le juriste peut nous dire sur le contentement éclairé et libre ?

TL : C'est un des points les plus problématiques à la fois d'un point de vue juridique et philosophique pour les technologies du 21e siècle. Le problème c'est l'idée même que l'être humain pourrait exprimer un choix éclairé et libre dans ces nouveaux contextes ; les deux adjectifs étant essentiels.

Contentement totem @serab

Comment le consentement peut-il être « éclairé » ? L'utilisateur ne s'intéresse pas vraiment au fonctionnement des technologies qu'il utilise quotidiennement et on ne l'encourage pas à comprendre ce qu'elles font ou ce

qu'elles lui font faire. On lui propose des services user-friendly et cette amitié « machinique » implique des routines incorporées, un aspect prothétique fort, une forme d'hybridation. Dans ce contexte, il est difficilement envisageable d'interrompre le cours de l'action pour demander à chaque fois un consentement, en espérant en plus que ce consentement ait un sens.

Il faudrait aussi parler du caractère « libre » du consentement. Avec les GAFAM, quelle est la liberté de choix face à un tel déséquilibre de pouvoir et d'information ? Avec Facebook, par exemple, vous devez accepter des CGU qui peuvent changer par simple notification. Et quel adolescent a vraiment le choix d'aller ou non sur Facebook ? Le choix n'existe plus d'un point de vue sociologique car se passer de Facebook pour un jeune c'est synonyme de mort sociale.

Si le RGPD a fait un peu avancer les choses, l'accent qui continue d'être mis sur la notion de consentement éclairé et libre est problématique. Avec la complexité de l'informatique, c'est la fiction du sujet rationnel, autonome, capable de consentir qui s'effondre. Depuis toujours, le droit est friand de fictions ; elles lui permettent d'appréhender la complexité du réel et de gérer les litiges qui en résultent. Aujourd'hui, il faudrait sans doute en inventer d'autres, car la magie du consentement dans l'univers numérique n'opère plus.

« Vous avez consenti, alors c'est bon ». Vous acceptez de vous livrer gracieusement à la bienveillance des plateformes qui prennent les décisions à votre place. C'est peu satisfaisant. Vous pouvez aussi attendre de l'informatique qu'elle vous aide. Oui, mais ça n'existe pas encore.

Antoinette Rouvroy parle de « fétichisation des données personnelles ». On devrait aussi parler de fétichisation du consentement. On ne peut continuer à mettre autant de poids dans le consentement. Il faut imposer des contraintes beaucoup plus fortes aux plateformes.

B : Tu as parlé d'aide apportée par l'informatique. Peut-on imaginer des systèmes informatiques, des assistants personnels, des systèmes d'information personnelle, qui nous aident à exprimer nos choix ?

TL : Bien sûr, on peut imaginer une collaboration entre les machines et l'utilisateur. Mais il faudrait déjà que l'utilisateur ait les capacités de spécifier ce qu'il veut. Ce n'est pas évident. Qu'est-ce que cela représenterait pour un jeune, par exemple, de spécifier sa politique d'autorisation de cookies ?

B : Est-ce qu'on peut parler de personnalité juridique du robot ?

TL : C'est compliqué. La question fondamentale c'est de savoir si la notion de personnalité en droit procède de la simple pragmatique juridique, ou si c'est plus, si cela inclut une véritable valeur philosophique. Pour prendre un exemple, un chien d'aveugle est blessé par une voiture. Le juge a considéré ce chien comme une « prothèse vivante », une extension de la personnalité de l'aveugle. Cette construction lui a permis de donner une meilleure compensation car les régimes d'indemnisation diffèrent selon qu'il s'agisse d'une atteinte à l'intégrité physique d'un individu ou d'un dommage aux biens qu'il possède. Le droit ne dit pas ontologiquement si ce chien d'aveugle est une personne ou pas. C'est le contexte et la visée de justice qui ont conduit le juge à créer cette chimère. Pour ce qui est des robots, je pense, avec les pragmatistes, que l'on pourrait accorder une forme de personnalité aux robots. Il ne s'agit pas de dire qu'un robot

est comme une « personne physique » et qu'il peut jouir de droits fondamentaux, par exemple. Non, c'est une autre forme de personne, un peu comme on l'a fait avec les « personnes morales ». Cela permettrait de résoudre des problèmes en matière de responsabilité.

B : Quelle est le sujet de recherche qui te passionne en ce moment ?

CL : Je travaille sur la notion de prédiction algorithmique ; ce qui va me donner beaucoup d'occasions de travailler avec des informaticiens. Il y a aujourd'hui une véritable obsession autour des vertus prédictives de l'intelligence artificielle. Je trouve dingue l'expression « prédiction en temps réel » (nowcasting en anglais) ; une prédiction, c'est pour le futur. Comme anthropologue, je suis passionné par l'idée de comparer la prédiction algorithmique avec les pratiques divinatoires, qui restent encore très répandues. Dans son ouvrage « De divinatione », Cicéron s'attaquait à la question de l'irrationalité de la divination. C'est fascinant de voir qu'on rejoue au 21e siècle cette même question de la rationalité scientifique avec l'intelligence artificielle. C'est ça que j'essaie de comprendre. Comment est-ce qu'on part de résultats d'IA pour établir des savoirs prédictifs quasiment indiscutables ? Bien sûr, on peut comprendre la prédiction algorithmique quand elle s'appuie sur des validations expérimentales, qu'elle établit des taux de confiance dans les résultats. Mais on voit aussi se développer des prédictions algorithmiques qui par certains aspects rejoignent plus les pratiques magiques que scientifiques.

Serge Abiteboul, Inria et ENS, Paris, et **Laurence Devillers**, Professeure, Université Paris-Sorbonne

12 OCTOBRE 2020

Numérique est mon droit

Un nouvel « Entretien autour de l'informatique ». Célia Zolynski est Professeure de droit privé à l'Université Paris Panthéon-Sorbonne, co-directrice du Département de recherche en droit de l'immatériel de la Sorbonne, et membre du Comité national pilote d'éthique du numérique. Ses activités de recherche et d'enseignement portent sur le droit du numérique, le droit de la propriété intellectuelle, le droit du marché et les libertés fondamentales. Elle explique comment les utilisateurs du numérique doivent reprendre le contrôle de leurs données, et ce que la loi peut faire pour cela.
Cet article est publié en collaboration avec theconversation.fr.

Célia Zolynski, photographie Didier Goupil

B : Peux-tu nous expliquer ton parcours de recherche en droit du numérique ?

CZ : Ce qui m'a intéressée dès le début de ma carrière de chercheure a été de comprendre comment le droit pouvait se saisir de ce nouvel objet qu'était internet et comment cela conduisait à adapter un certain nombre de normes juridiques ainsi que la façon même de les concevoir. J'ai alors cherché à déterminer comment utiliser la logique de l'informatique pour poser un autre regard sur des questions juridiques. Cela m'a conduite à me rapprocher par curiosité, par intérê et pour solidifier mes compétences, de chercheurs en informatique, et à participer à des recherches à cheval sur les deux domaines.

Mon premier poste en qualité de professeur Agrégée en droit était aux Antilles. J'ai alors beaucoup travaillé sur les notions de patrimoine immatériel chères à la culture caribéenne. Cela m'a ramené sur les questions de droit d'auteur et j'ai d'ailleurs été associée à un certain nombre de débats sur la loi Hadopi.

Rentrée en métropole, j'ai été en poste à Rennes où j'ai enseigné le droit des affaires, le droit commercial. C'est alors plutôt sous l'angle du commerce électronique que je me suis intéressée au déploiement des réseaux. J'ai également animé un groupe de chercheurs en droit dans le cadre du réseau Trans Europe Experts, qui répond aux consultations des institutions de l'Union Européenne notamment sur les révisions des directives relatives au droit d'auteur dans l'environnement numérique. C'est à ce titre-là que j'ai commencé à m'intéresser au droit des données à caractère personnel, à l'époque où l'Union européenne lançait la réforme qui a abouti à l'adoption du RGPD.

J'ai ensuite été nommée au Conseil National du Numérique (sa troisième vague) dont la doctrine me semblait fondatrice pour le développement de la stratégie numérique française et européenne. Les personnes que j'y ai côtoyées m'ont permis de mieux comprendre certains aspects du numérique, la logique sous-jacente. C'est alors que j'ai pris conscience de la place essentielle que devrait avoir l'utilisateur dans la régulation du numérique. C'est devenu un axe important de mes travaux. L'objectif est de transformer cet utilisateur en un agent actif. Cela

passe par des solutions techniques mais cela demande aussi de penser différemment un cadre juridique qui lui donne les moyens d'agir sans pour autant déresponsabiliser les entreprises.

Depuis, j'ai passé 4 ans comme Professeure à l'Université de Versailles Saint-Quentin à Paris-Saclay. C'est à Saclay que j'ai pu initier des collaborations avec des informaticiens, notamment Nicolas Anciaux d'Inria. Aujourd'hui, je suis Professeure à Paris-Sorbonne 1, Université au sein de laquelle je prolonge mes travaux aux côtés de chercheurs issus des Humanités numériques philosophes, historiens et économistes.

B : Tu as insisté sur la place de l'utilisateur dans la régulation du numérique ? Tu peux nous en dire plus.

CZ : Quand on analyse, par exemple, les conséquences du RGPD ou de la loi pour une république numérique, on réalise assez vite la difficulté pour les utilisateurs de pleinement profiter des protections de leurs données personnelles et de leur vie privée. On leur propose une approche purement défensive. Au-delà, on aimerait les placer en capacité de préserver activement leur autonomie informationnelle de ne pas se contenter des murs de protection que les systèmes informatiques et la loi mettent autour de leurs données.

On peut faire une analogie avec la figure traditionnelle du consommateur. Dans le cadre d'un discours paternaliste, on cantonnait le consommateur au rôle d'un enfant à protéger. Dans une approche plus moderne, on dépasse cette vision pour en faire un véritable acteur du marché.

De la même façon, on voudrait juridiquement donner à l'utilisateur des services numériques les moyens de garantir sa pleine autonomie informationnelle. Cela peut commencer par exemple p. le droit à la portabilité des données, c'est-à-dire le droit de récupérer toutes ses données personnelles d'une application numérique. Mais on voit bien déjà, à travers cet exemple, la difficulté de mettre véritablement l'utilisateur en position de maîtriser son monde numérique. Quelles données ? Sous quel format ? Pour en faire quoi ?

Très rapidement, on se rend compte que ces pouvoirs d'agir donnés aux consommateurs peuvent n'être que des faux-nez, des faux-semblants, instrumentalisant le consentement de l'utilisateur pour faciliter la récupération de ses données. Vous acceptez les cookies d'une application parce que sans, le service se détériore, parce qu'on vous redemande sans cesse de les accepter. Quelle est alors la valeur de votre consentement ?

Un autre exemple de faux-semblant va nous être proposé par une approche qui se réclame pourtant de la défense des utilisateurs. Gaspard Koening, notamment, propose de reconnaître un droit de propriété sur ses données qui s'accompagnerait du droit de vendre ses données personnelles pour en tirer bénéfice. D'abord, on peut s'interroger sur le champ d'une telle mesure car peu de données sont réellement personnelles, les données étant le plus souvent sociales. Ai-je le droit de vendre des données qui me mettent en scène avec un grand ami ? Peut-il également les vendre ? On peut également se demander si cette consécration du droit de propriété serait conforme au RGPD. Mais, surtout, on peut craindre que, à partir du moment où l'on a vendu des données personnelles, on en perde la maîtrise. En essayant de réaffirmer le droit de l'utilisateur sur ses données, on arriverait alors à lui faire perdre tout contrôle sur ce qui en serait fait ! La propriété des données personnelles serait alors une sorte de miroir aux alouettes…

A mon avis, il faut tout au contraire redonner à l'utilisateur le contrôle sur ce qui est fait de ses données personnelles. C'est sur ça que porte ma recherche, sur comment conférer un véritable pouvoir à l'utilisateur, comment lui donner *vraiment* les moyens d'exercer son contrôle sur ses données personnelles. Pour ce faire, on va le placer en capacité, en faire un véritable agent du système en évitant des faux-semblants de liberté que sont l'instrumentalisation du consentement de l'utilisateur ou la monétisation des données.

B : Comment peut-on réaliser cela ?

CZ : On ajoute une brique supplémentaire que nous appelons, avec Nicolas Anciaux, l' « agentivité ». Au-delà de la possibilité de récupérer ses données avec la portabilité, l'agentivité implique de véritablement savoir ce qui est fait de ses données, et de pouvoir en décider les usages.

Nous allons un peu dans le même sens que Tim Berners-Lee dans son projet Solid (Social Linked Data, en anglais). Ses idées sont de dépasser la réalité actuelle du web et des risques qui résultent des monopoles de situation qui se sont installés en associant l'utilisateur à la régulation de ses données personnelles. Dans notre projet, nous sommes plus ambitieux encore en offrant à l'agent le contrôle de l'usage de ses données, voire la possibilité de générer lui-même de nouveaux usages, en lui permettant d'orchestrer sous son contrôle des traitements de données. Il déciderait des traitements réalisés et on lui garantirait la conformité de ces traitements aux décisions qu'il a prises. Ça c'est la partie technique. La partie juridique serait de faire une sorte de manifeste qui assure la conformité des traitements, et la possibilité de les contrôler tout du long.

B : Pourrais-tu illustrer avec un exemple comment cela peut marcher en pratique.

CZ : Prenons le cas du *cloud* personnel. L'utilisateur peut choisir d'auto-héberger ses données. Il en contrôle ainsi l'usage. Il choisit les algorithmes qui tournent sur ses données et protège lui-même la confidentialité de ses données. Il a une parfaite autonomie informationnelle.

Mais vous allez me dire que l'utilisateur n'a pas les compétences de faire tout cela, que même s'ils les avaient, il n'a pas forcément envie de passer son temps à gérer des données. Certes, mais il peut payer une entreprise pour le faire. Ça reste de l'auto-hébergement parce qu'il paie l'entreprise, il a un contrat avec elle qui indique que c'est à lui de décider. On est très loin du modèle classique des plateformes du web qui pour héberger vos données se rétribuent en monétisant ces données ou votre attention. Ici, vous payez pour choisir ce qui est fait de vos données.

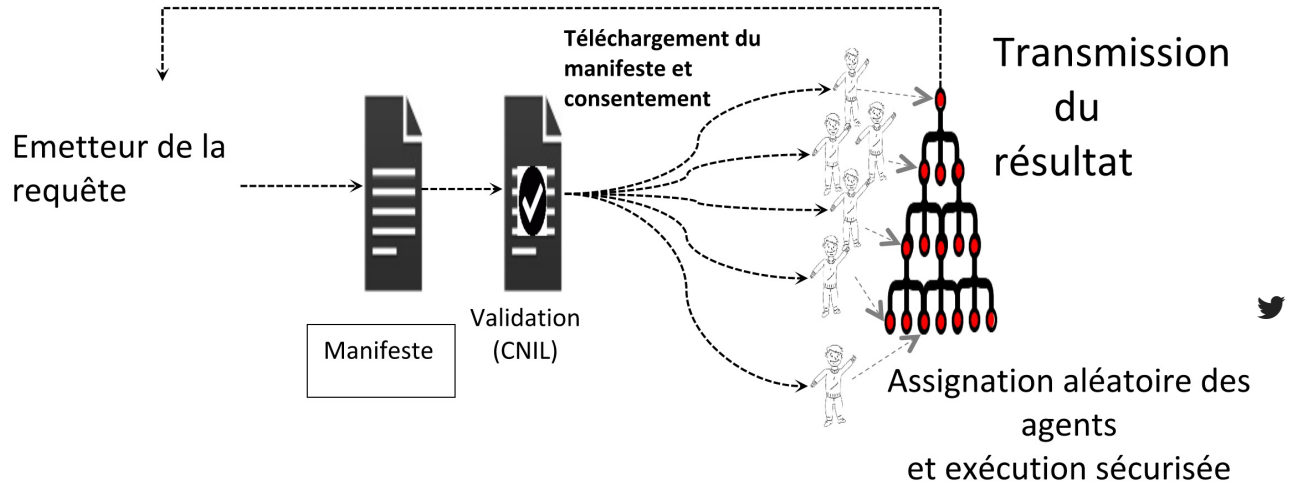
B : Mais en devenant le gérant de ses données, un utilisateur ne risque-t-il pas de devenir également responsable, de perdre la protection de lois comme le RGPD ?

CZ : C'est un vrai sujet. Qui dit liberté et choix, dit responsabilité. Mais si la responsabilité de l'utilisateur est une chose, sa responsabilité juridique aux titres de ses actes en est une autre. Toute la difficulté est là. Reprenons le cas du *cloud* personnel. Si vous décidiez d'auto-héberger vos données, seriez-vous alors le responsable de ces traitements parce que vous les avez choisis ? Perdriez-vous alors la protection du RGPD ? Ce serait terrible que le prix de votre

souveraineté numérique soit la perte des protections du droit des données à caractère personnel.

Nous travaillons pour essayer de dégager un équilibre. L'utilisateur doit être mis en capacité cognitive de comprendre comment le système fonctionne, de faire des choix éclairés. Mais la responsabilité juridique de la sécurité du système revient à l'opérateur du *cloud*. Nous réfléchissons à des régimes juridiques de répartition « raisonnable » de la responsabilité. L'utilisateur ne serait responsable que de la partie qu'il maîtrise et le fournisseur du *cloud* personnel du reste et en particulier de la sûreté.

Tout l'intérêt du sujet de ces systèmes d'auto-hébergement, sa difficulté, réside dans le besoin d'articulation entre les aspects techniques et juridiques. Nous étudions avec Nicolas Anciaux les promesses autour de l'*empowerment* de l'utilisateur dans les solutions proposées et identifions éventuellement les vraies perspectives et les fausses promesses, en particulier les risques de responsabilisation déraisonnable des utilisateurs.



De : A Manifest-Based Framework for Organizing the Management of Personal Data at the Edge of the Network », R. Ladjel, N. Anciaux, P. Pucheral, G. Scerri, proceedings of International Conference on Information Systems Development (ISD), 2019.

B : Tu fais partie du Comité national pilote d'éthique du numérique**. Pourquoi est-ce important ?**

CZ : Le CNPEN a été mis en place en décembre 2019 sous l'égide du Comité consultatif national d'éthique à la demande du Premier ministre. Il est constitué de 27 personnes issues du monde académique, des entreprises ou de la société civile. En abordant de manière globale les enjeux d'éthique du numérique, son rôle est à la fois d'élaborer des avis sur les saisines qui lui sont adressées et d'effectuer un travail de veille pour éclairer les prises de décision individuelles et collectives.

Je suis ravie d'en faire partie. Dans le cadre de ce comité, nous pouvons explorer différents thèmes autour d'enjeux éthiques et d'éducation. Nous avons ouvert plusieurs sujets au CNPEN sur les *chatbots*, les véhicules autonomes, les décisions médicales mais aussi la désinformation, la télémédecine et les algorithmes de traçage pendant la pandémie. Chacun de ces sujets

interpelle, pose des questions critiques à la société. Au sein du CNPEN, nous pouvons en débattre sereinement ; nous avons souvent des spécialistes du domaine parmi les membres du comité.

Par exemple, les phénomènes de désinformation et de mésinformation ont été exacerbés à l'occasion de la crise engendrée par l'épidémie de COVID. Cela a conduit les plateformes numériques telles que les réseaux sociaux, moteurs de recherche, ou systèmes de partage de vidéos à développer encore plus leurs pratiques et leurs outils numériques pour lutter contre leurs effets délétères tant sur le plan individuel que collectif. Si la modération des contenus et le contrôle de la viralité jouent un rôle prépondérant dans le contrôle pragmatique de la désinformation et de la mésinformation, ces opérations soulèvent d'autres questionnements éthiques relatifs au rôle joué par différentes autorités dans ce processus.

Cela interroge tout d'abord l'autorité ainsi acquise par les plateformes et le contrôle qui devrait en résulter. Ensuite, il apparaît que ces opérations ne peuvent se passer d'instances qui identifient les informations acceptables et celles qui ne le sont pas. Différentes questions émergent alors s'agissant de la légitimité dont jouissent ces instances dès lors qu'elles sont considérées par les plateformes comme contribuant à établir la vérité, à définir notre société.

Il nous faut ensuite repenser, ici encore, le rôle joué par l'utilisateur. Sa liberté de s'exprimer doit être pleinement garantie comme vient de l'affirmer le Conseil constitutionnel dans sa décision du 18 juin dernier qui a jugé la Loi « Avia » en grande partie inconstitutionnelle. Mais, dans le même temps, l'utilisateur doit être mieux informé du rôle qu'il peut jouer en tant qu' « agent de la viralité » des contenus illicites et pouvoir contribuer à la régulation des contenus circulant sur le réseau. C'est un point essentiel auquel il convient de réfléchir tant sur le plan technique que juridique.

B : Une conclusion peut-être ?

CZ : Dans les sujets que nous discutons au CNPEN, cela devient de plus en plus évident : l'heure est venue de nous interroger collectivement sur la société que nous voulons construire demain avec le numérique. Les questions sociétales que cette technologie pose sont de plus en plus essentielles. On ne peut pas les appréhender si on ne considère qu'une facette du problème, par exemple que l'aspect technique, ou que juridique, ou qu'économique, etc. Il faut mener véritablement des recherches pluridisciplinaires.

On a déjà beaucoup avancé sur la protection de données mais la question est devenue, au-delà de la protection, de contrôler les usages des données dans la société. La même donnée peut servir pour la recherche médicale, pour des intérêts commerciaux, pour la surveillance, etc. La question n'est pas uniquement de choisir qui y a accès, mais de contrôler à quoi elle va servir. Et puis, cette donnée, ma donnée, peut aussi m'être utile personnellement, je veux également pouvoir développer mes propres usages des données.

Pour arriver à cela, il va falloir imaginer de nouvelles solutions techniques, de nouveaux cadres juridiques. Pour que cela fonctionne, la confiance est fondamentale. Je dois avoir confiance dans la robustesse de la technologie mais aussi dans la solidité du cadre juridique qui protège mes données.

Serge Abiteboul, Inria et ENS, Paris, et **Laurence Devillers**, Professeure, Université Paris-Sorbonne

05 FÉVRIER 2020

D'où vient le risque ? Des données et des algorithmes

La rencontre de chercheurs juristes et informaticiens dans le cadre du lancement du Centre Internet et Société et du montage du GdR Internet et Société, a été l'occasion de réflexions croisées et de soulever nombre de questions et premières pistes de recherche à explorer ensemble. Cet article résume le résultat d'une table ronde. ***Serge Abiteboul, Thierry Viéville***

Photo by Fernando Arcos from Pexels

Les plateformes numériques et leur rôle dans la société occupent les médias et les instances gouvernantes. Nous, juristes et informaticien·e·s, les percevons comme des nouveaux marchés de la donnée. Plusieurs acteurs humains, artistes, auteurs, créateurs de contenu, développeurs de langages, développeurs de plateformes, développeurs d'applications, internautes consommateurs, acteurs publics et privés, gravitent autour de ces plateformes et sont exposés à deux types de risque :

– Le risque-données se réfère à la protection des données sur ces plateformes.

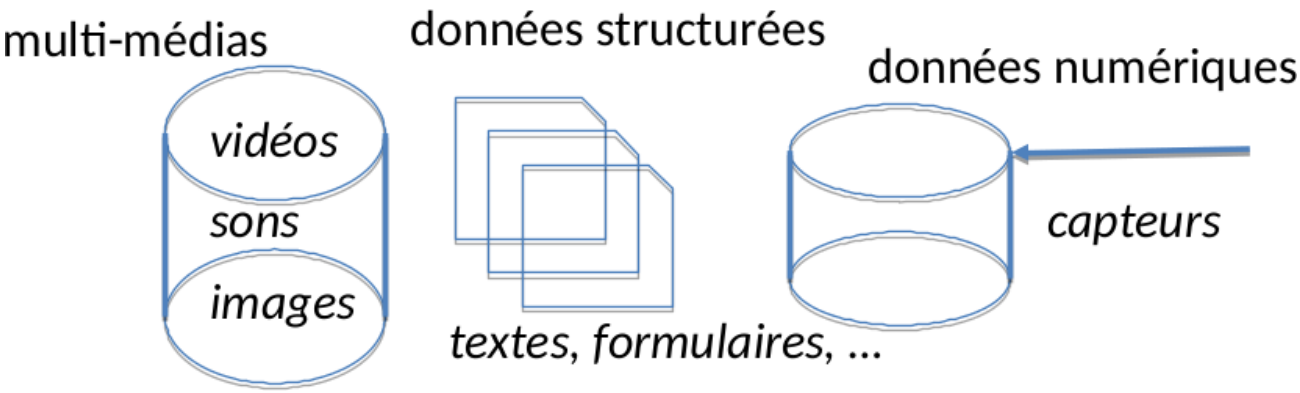
– Le risque-algorithmes se réfère aux dérives de discrimination algorithmique.

Ce document apporte une première réflexion sur comment appréhender les plateformes numériques et les risque-données et risque-algorithmes. Ces questions peuvent être abordées de deux points de vue complémentaires : le point de vue juridique dont le souci principal est de déterminer les cadres qui permettent d'identifier et de réguler ces risques, et le point de vue informatique dont le but est de développer les outils nécessaires pour quantifier et résoudre ces risques.

Les trois facettes du risque algorithmique.

Le risque-algorithmes peut être caractérisé de 3 façons.

Il s'agit d'abord de l'enfermement algorithmique qui peut aussi bien porter sur les opinions, la connaissance culturelle, ou encore les pratiques commerciales. En effet, les algorithmes confrontent l'internaute aux mêmes contenus, selon son profil et les paramètres intégrés, en dépit du respect du principe de la loyauté. C'est le cas sur les sites de recommandation de news comme Facebook ou les sites de recommandation de produits comme Amazon.
La deuxième facette du risque-algorithmique est liée à la maîtrise de tous les aspects de la vie d'un individu, de la régulation de l'information à destination des investisseurs jusqu'à ses habitudes alimentaires, ses hobbies, ou encore son état de santé. Ce traçage de l'individu laisse présager l'emprise d'une forme de surveillance qui contrevient à l'essence même de la liberté de l'individu.
La troisième est liée à la potentielle violation des droits fondamentaux. En particulier, à la discrimination algorithmique définie comme le traitement défavorable ou inégal, en comparaison à d'autres personnes ou d'autres situations égales ou similaires, fondé sur un motif expressément prohibé par la loi. Ceci englobe l'étude de l'équité (*fairness*) des algorithmes de classement (tri de personnes cherchant un travail en ligne), de recommandation, et d'apprentissage en vue de prédiction. Le problème des biais discriminatoires induits par des algorithmes concerne plusieurs domaines comme l'embauche en ligne sur MisterTemp', Qapa et TaskRabbit, les décisions de justice, les décisions de patrouilles de police, ou encore les admissions scolaires.
Nous reprenons une classification des biais proposée par des collègues de Télécom ParisTech et discutée dans un rapport de l'Institut Montaigne à Paris. Nous adaptons cette classification aux risque-données et risque-algorithmes en mettant l'accent sur les biais.



Les données proviennent de sources différents et ont des formats multiples. Elles véhiculent différents types de biais.

Des risques aux biais sur les données et dans les algorithmes.

Le biais-données est principalement statistique

Le biais des données est typiquement présent dans les valeurs des données. Par exemple, c'est le cas pour un algorithme de recrutement entraîné sur une base de données dans laquelle les hommes sont sur-représentés exclura les femmes.

Le biais de stéréotype est une tendance qui consiste à agir en référence au groupe social auquel nous appartenons. Par exemple, une étude montre qu'une femme a tendance à cliquer sur des offres d'emplois qu'elle pense plus facile à obtenir en tant que femme.

Le biais de variable omise (de modélisation ou d'encodage) est un biais dû à la difficulté de représenter ou d'encoder un facteur dans les données. Par exemple, comme il est difficile de trouver des critères factuels pour mesurer l'intelligence émotionnelle, cette dimension est absente des algorithmes de recrutement.

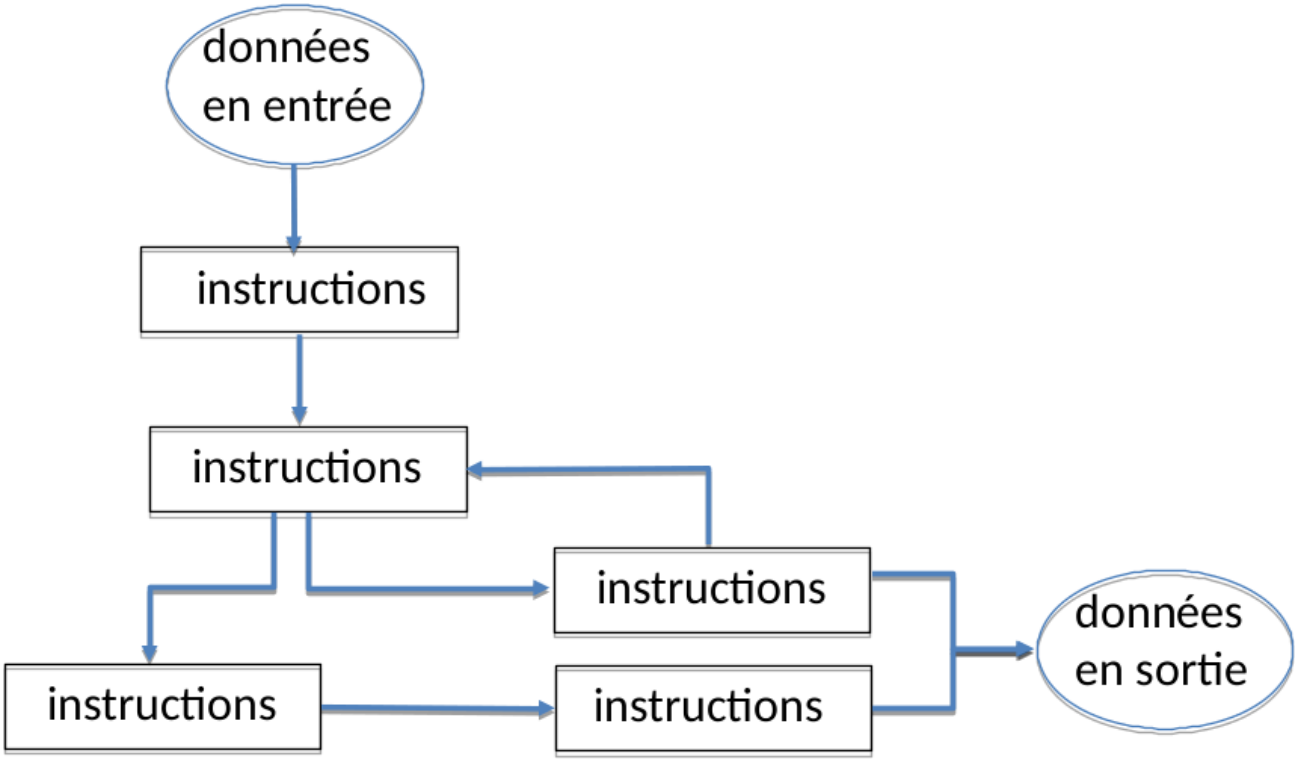
Le biais de sélection est lui dû aux caractéristiques de l'échantillon sélectionné pour tirer des conclusions. Par exemple, une banque utilisera des données internes pour déterminer un score de crédit, en se focalisant sur les personnes ayant obtenu ou pas un prêt, mais ignorant celles qui n'ont jamais eu besoin d'emprunter, etc.

Le biais algorithmique tient principalement du raisonnement.

Un biais économique est introduit dans les algorithmes, volontairement ou involontairement, parce qu'il va être efficace économiquement. Par exemple, un algorithme de publicité oriente les annonces vers des profils particuliers pour lesquels les chances de succès sont plus importantes ; des rasoirs vont être plus présentés à des hommes, des fastfood à des populations socialement défavorisées, etc.

Il convient également de citer toute une palette de biais cognitifs

Les biais de conformité, dits du « mouton de Panurge », correspondent à notre tendance à reproduire les croyances de notre communauté. C'est le cas, par exemple, quand nous soutenons un candidat lors d'une élection parce que sa famille et ses amis le soutiennent.
Le biais de confirmation est une tendance à privilégier les informations qui renforcent notre point de vue. Par exemple, après qu'une personne de confiance nous a affirmé qu'untel est autoritaire, remarquer uniquement les exemples qui le démontrent.
Le biais de corrélation illusoire est une tendance à vouloir associer des phénomènes qui ne sont pas nécessairement liés. Par exemple, penser qu'il y a une relation entre soi-même et un événement extérieur comme le retard d'un train ou une tempête.
Le biais d'endogénéité est lié à une relative incapacité à anticiper le futur. Par exemple, dans le cas du *credit scoring*, il se peut qu'un prospect avec un mauvais historique de remboursement d'emprunt puisse changer de style de vie lorsqu'il décide de fonder une famille.



Les algorithmes sont une série d'instructions qui manipulent des données en entrée et retournent des données en sortie. Ces données en entrée véhiculent parfois des biais. Les biais peuvent aussi se trouver dans une ou plusieurs instructions des algorithmes.

Doit-on aborder les risque-données et risque-algorithmes sur les plateformes numériques ensemble ou séparément ?

Considérons deux exemples, le contexte de la technologie blockchain, et celui des systèmes d'Intelligence Artificielle.

Sur la blockchain, l'on retrouve tout d'abord les données, les risques et leur biais. Prenons l'exemple des données et des risques associés. La blockchain fonctionne par un chiffrement à double clés cryptographiques : des clés privées et des clés publiques. Beaucoup d'internautes confient aux plateformes leurs clés privées, leur délégant ainsi la gestion de leur adresse et les mouvements de fonds. Ces clés privées sont stockées soit dans un fichier accessible sur Internet (*hot storage*), soit sur un périphérique isolé (*cold storage*). Le premier est évidemment très vulnérable au piratage, tandis que 92 % des plateformes d'échange déclarent utiliser un système de *cold storage*. Depuis 2011, 19 incidents graves ont été recensés pour un montant estimé des pertes s'élevant à 1,2 milliards de dollars. Les causes de ces incidents sont multiples. La plus courante vient de la falsification des clés privées, suivie par l'introduction de logiciels malveillants. Le *hack* de la plateforme Coincheck au Japon, en janvier 2018, illustre la faiblesse de la protection du système de *hot storage*.

Autre exemple sur les algorithmes et les risques associés, l'échange de cryptomonnaies sur des plateformes voit se développer et se diversifier les infrastructures de marché. L'ambition est *« de permettre la mise en place d'un environnement favorisant l'intégrité, la transparence et la*

sécurité des services concernés pour les investisseurs en actifs numériques, tout en assurant un cadre réglementaire sécurisant pour le développement d'un écosystème français robuste » . La France s'est dotée récemment d'un cadre juridique permettant de réguler ces activités de manière souple. Pour autant, au niveau mondial, les risques attachés à des cotations non transparentes ou à des transactions suspectes s'apparentant à des manipulations directes de cours ou de pratiques d'investisseurs informés, de type *frontrunning*. Le *frontrunning* est une technique boursière permettant à un courtier d'utiliser un ordre transmis par ses clients afin de s'enrichir. La technique consiste à profiter des décalages de cours engendrés par les ordres importants passés par les clients du courtier.

Venons en à la question « doit-on aborder les risque-données et risque-algorithmes sur les plateformes numériques ensemble ou séparément ? » Concernant la blockchain, la réponse du droit est séparée, car les risques saisis sont différents. D'un côté, certaines dispositions du droit pénal, de la responsabilité civile ou de la protection des données à caractère personnel seront mobilisées. Alors que de l'autre côté, en France, le récent cadre juridique visant à saisir les activités des prestataires de services sur actif numérique et à éviter le risque algorithmique est principalement régulatoire.

Sur les systèmes d'IA, nous prendrons pour répondre à notre question le prisme de la responsabilité (liability) et de la responsabilisation (accountability).

Cette question est diabolique car elle impose au juriste de faire une plongée dans le monde informatique pour comprendre ce en quoi consiste l'intelligence artificielle, ce mot-valise qui recouvre, en réalité, de nombreuses sciences et techniques informatiques. Et faut-il seulement utiliser ce terme, alors que le créateur du très usité assistant vocal Siri vient d'écrire un ouvrage dont le titre, un tantinet provocateur, énonce que l'intelligence artificielle n'existe pas… (Luc Julia, L'intelligence artificielle n'existe pas, *First editions,* 2019).

Un distinguo entre les systèmes d'IA est néanmoins souvent opéré : seuls certains systèmes sont véritablement « embarqués » dans un corps afin de lui offrir ses comportements algorithmiques : robot, véhicule « autonome »… Les autres systèmes d'IA prennent des décisions ou des recommandations algorithmiques qui peuvent avoir un effet immédiat sur le monde réel et l'esprit humain, sans avoir besoin de s'incarner dans un corps : recommandations commerciales à destination du consommateur, fil d'actualité des réseaux sociaux, justice prédictive et sont souvent considérés comme « dématérialisés ». Cependant, tous les systèmes d'IA finissent par être incorporés dans une machine : robot, véhicule, ordinateur, téléphone… et tous les systèmes d'IA peuvent potentiellement avoir un impact sur l'esprit ou le corps humains, voire sur les droits de la personnalité (M. Baccache, Intelligence artificielle et droits de la responsabilité, in Droit de l'intelligence artificielle, A. Bensamoun, G. Loiseau, (dir.), L.G.D.J., Les intégrales 2019, p. 71 s.), tant et si bien que nous choisirons ici de saisir la question de la responsabilité lors du recours aux systèmes d'IA d'une manière transversale.

La question transversale que précisément nous poserons consistera à nous demander si la spécificité des systèmes d'IA, tant au regard de leur nature évolutive et de leur gouvernance complexe, qu'au regard des risques découlant de leur mise en œuvre pour l'humain et la société n'appelle pas à préférer à la responsabilité, entendue comme la seule sanction a posteriori de la réalisation d'un risque, une complémentarité entre responsabilisation de la gouvernance de chaque système d'IA tout au long de son cycle de vie et responsabilité a posteriori. Si la responsabilisation est reconnue comme étape préalable à la responsabilité, elle impliquera

d'envisager les risques-données et les risques-algorithmiques, de manière conjointe, préservant ainsi la spécificité de chacun de ces risques, mais en les reliant, parce c'est par la conjonction de ces deux types de risques, que des conséquences préjudiciables pour l'humain ou la société peuvent se réaliser.

En effet, dans ses « lignes directrices en matière d'éthique pour une IA digne de confiance » datant d'avril 2019, le Groupe d'experts de haut niveau sur l'intelligence artificielle, mandaté par la Commission européenne, rappelle dans l'une de ses propositions un point fondamental, à savoir les nécessaires reconnaissance et prise de conscience que « certaines applications d'IA sont certes susceptibles d'apporter des avantages considérables aux individus et à la société, mais qu'elles peuvent également avoir des incidences négatives, y compris des incidences pouvant s'avérer difficiles à anticiper, reconnaître ou mesurer (par exemple, en matière de démocratie, d'état de droit et de justice distributive, ou sur l'esprit humain lui-même) » (Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle, Lignes directrices en matière d'éthique pour une IA digne de confiance, avril 2019, constitué par la Commission européenne en juin 2018,).

Ce faisant, le groupe d'experts de haut niveau en appelle à « adopter des mesures appropriées pour atténuer ces risques le cas échéant, de manière proportionnée à l'ampleur du risque » et, en se fondant sur les articles de la Charte des droits fondamentaux de l'Union européenne, à « accorder une attention particulière aux situations concernant des groupes plus vulnérables tels que les enfants, les personnes handicapées et d'autres groupes historiquement défavorisés, exposés au risque d'exclusion, et/ou aux situations caractérisées par des asymétries de pouvoir ou d'information, par exemple entre les employeurs et les travailleurs, ou entre les entreprises et les consommateurs ».

Alors même que certains risques et la protection de certains groupes vulnérables l'imposent, prendre les mesures appropriées n'est cependant pas aisé, et ce au-delà même de la tension récurrente entre principe d'innovation et principe de précaution. La raison en est que tant les briques techniques utilisées, que les personnes impliquées dans le fonctionnement d'un système d'IA sont nombreuses, variées et en interactions complexes, entraînant de nombreuses interactions qui ne sont pas aisées à maîtriser. Il convient de constater que le groupe d'experts de haut niveau formule un ensemble de propositions, à visées d'éthique et de robustesse technique des systèmes d'IA, qui véhiculent l'idée selon laquelle la confiance en un système d'IA, au regard des risques actuels du déploiement de ceux-ci, se doit de reposer sur une responsabilisation a priori de la gouvernance de celui-ci tout au long de son cycle de vie, qui passe, entre autres choses, par un objectif d'explicabilité de ces actions.

La notion d'*accountability* est à cet égard une notion centrale pour comprendre la complémentarité et le long continuum existant entre responsabilisation et responsabilité. Plus que par le terme de responsabilité, cette notion d'*accountability* peut justement être traduite par les notions de reddition de compte et/ou de responsabilisation. Cette responsabilisation permet d'envisager les risques-données et les risques-algorithmiques, de manière conjointe, préservant ainsi la spécificité de chacun de ces risques, mais en les reliant, parce c'est par la conjonction de ces deux types de risques, que des conséquences préjudiciables pour l'humain ou la société peuvent se réaliser.

En résumé. Le point de vue juridique différera selon les enjeux et les concepts applicables. Dans le cas de la blockchain, il est important de séparer le risque-données du risque-algorithmes

puisqu'ils traitent de problématiques différentes et nécessitent des cadres de loi différents. Le premier traite de la question de la divulgation de l'identité des parties qui relève de la sécurité des données alors que le second traite de la question des actifs numériques frauduleux. Dans le cas des systèmes d'intelligence artificielle, tout déprendra du point de savoir s'il convient de prévenir le dommage ou de le sanctionner une fois qu'il s'est réalisé. Dans le cas d'une recherche de responsabilisation, il convient d'envisager les risques-données et les risques-algorithmes de manière conjointe.

Si la question est celle de la responsabilité (*liability*) et la responsabilisation (*accountability*), i.e., celle d'imputer la faute à une personne physique, il sera important de séparer les deux risques. Cette séparation est aussi celle qui est préconisée en informatique pour permettre d'identifier les "coupables": données ou algorithmes. Les techniques de provenance des données et de trace algorithmique permettront d'isoler les raisons pour lesquelles il y a faute. Il s'agira d'abord d'identifier si la faute est due à un risque-données du type divulgation de la vie privée ou à un biais statistique dans les données, ou à un risque-algorithmes du type économique ou cognitif, ou si la faute est due aux deux. On ne pourra donc imputer la faute et déterminer les cadres de loi applicables que s'il y a séparation. De même si l'objectif est de "réparer" les données ou l'algorithme, l'étude des deux types de risque doit s'effectuer séparément. C'est ce qu'on appelle l'orthogonalité en informatique. Selon le dictionnaire, le jeu d'instructions d'un ordinateur est dit *orthogonal* lorsque (presque) toutes les instructions peuvent s'appliquer à tous les types de données. Un jeu d'instruction orthogonal simplifie la tâche du compilateur puisqu'il y a moins de cas particuliers à traiter : les opérations peuvent être appliquées telles quelles à n'importe quel type de donnée. Dans notre contexte, cela se traduirait par avoir un jeu de données parfait et voir comment l'algorithme se comporte pour déterminer s'il y a un risque-algorithmes et avoir un algorithme parfait et examiner les résultats appliqués à un jeu de données pour déterminer le risque-données. Ces stratégies ont de beaux jours devant elles.

Sihem Amer-Yahia (DR CNRS INS2I, Univ. Grenoble-Alpes)
Amélie Favreau (MdC Droit Privé, Univ. Grenoble-Alpes)
Juliette Sénéchal (MdC Droit Privé, Univ. de Lille)

21 NOVEMBRE 2019

La régulation des contenus en ligne : défaire Charybde en prévenant Scylla

Le sujet de la régulation des contenus, par le prisme de la régulation des nouvelles plateformes que sont les réseaux sociaux, s'impose à l'ordre du jour des agendas parlementaires nationaux, Allemagne puis France, et bientôt européen. La société entière est traversée par ces réseaux mondiaux qui séduisent, fascinent parfois jusqu'à l'addiction, font résonner des tendances, raisonner des consciences, et aussi malheureusement charrient des flots d'immondices *ad nauseam*.

Qu'ils soient de provocation aux actes terroristes ou apologiques, pédopornographiques, haineux, discriminants, harcelants, porteurs de fausses nouvelles, violant les droits d'auteurs et voisins, la toxicité variée de certains contenus nécessite des traitements différenciés en vertu du principe de proportionnalité. Le réseau lui-même, moyen d'expression populaire extraordinaire, se retrouve ainsi en accusation et rejoint sur la sellette l'auteur du contenu toxique.

Il serait affligeant d'oublier que ces incroyables outils interconnectent des milliards d'individus pour ne voir que leurs dérives. S'assurer de leur bon usage revient à se poser la question d'une modération de leurs contenus dans le respect des utilisateurs et des droits fondamentaux, sans, en ce faisant, obérer la capacité des entreprises à innover.

Le défi est le suivant : quelle ligne de crête à inventer pour nos démocraties modernes, irriguées d'expression citoyenne mais menacées dans la cohésion sociale par une toxicité imparfaitement maîtrisée ?

Les réflexions ultérieurement exposées sont nées en partie de travaux sur la modération des discours de haine chez la société Facebook, en France, à l'occasion d'une mission regroupant des membres de diverses administrations publiques[1]. Évidemment, les mêmes principes peuvent potentiellement s'appliquer à d'autres contenus toxiques, à d'autres plateformes permettant à des utilisateurs de publier des contenus, que ce soient des réseaux sociaux (Twitter, YouTube, Snapchat…) voire d'autres médias (lemonde.fr, jeuxvideo.com…), et à d'autres échelles, notamment l'Union européenne.

Aujourd'hui, une modération traditionnelle fondée sur la loi pénale existe déjà, émanation régalienne de l'État de droit. La modération technologique des conditions générales d'utilisation (CGU), émanation « régalienne de la plateforme souveraine », s'y superpose. Leur effectivité et leur articulation restent insatisfaisantes.

Si elle dérange, l'expression « plateforme souveraine » recouvre une certaine réalité. Au triptyque, un territoire, une population, une autorité, caractéristiques de l'État en droit international, se substitue dans le monde numérique : un cyberespace, des usagers et la capacité autoproclamée de définir les règles.

L'État de droit, afin de préserver nos valeurs démocratiques, doit s'assurer des standards de qualité et d'efficience de la modération mais également prévenir toute censure privée excessive. Il est naturel pour ce faire de passer par un régulateur des réseaux significatifs. En effet, par leur caractère systémique[2], les grands réseaux ont pris une importance considérable dans l'espace public. Un retour en arrière semble improbable, hormis l'hypothèse radicale d'un démantèlement imposé par la puissance publique (américaine).

Deux lignes directrices pourraient sous-tendre une telle régulation :

Un équilibre entre le droit d'expression et le droit des internautes d'être protégés de contenus toxiques ;
Un partage des rôles entre les juges arbitres ultimes de l'illégalité des contenus, et un régulateur public en charge des réseaux sociaux contrôlant le fonctionnement des plateformes systémiques.

1. La liberté d'expression des deux côtés de l'Atlantique

La force et la portée du 1er amendement de la Constitution américaine, ratifié en 1791, demeurent inoxydables. Le droit américain et notamment le principe de *Freedom of speech*, plus absolu que le principe européen de la liberté d'expression imprègne les CGU des réseaux sociaux. Sur le vieux continent, la Cour européenne des droits de l'homme a su apprécier le principe de la liberté d'expression avec la souplesse nécessaire. Consacrée par l'article 10 de la Convention européenne des droits de l'homme[3], la liberté d'expression est tempérée par de possibles restrictions « nécessaires dans une société démocratique ». La Cour considère la liberté d'expression comme un pilier de la démocratie, une condition basique pour le développement humain, et sait affirmer que les idées exprimées peuvent et doivent parfois choquer ou troubler l'État ou des fractions de sa population. Ces expressions « politiquement incorrectes » sont le fruit concret du pluralisme, de la tolérance et de l'ouverture d'esprit sans lesquels il n'existerait pas de société démocratique. En conséquence, les restrictions légitimes pouvant être apportées à la liberté d'expression doivent impérativement respecter le principe de proportionnalité[4].

Ces distinctions fondamentales entre les conceptions juridiques ont non seulement participé à l'incompréhension entre les plateformes et les États européens désormais enclins à légiférer afin de faire respecter leur souveraineté, mais freinent également l'accès à la preuve numérique dans la nécessaire répression judiciaire des abus constatés.

L'accord récent entre anglais et américains pour améliorer l'accès transfrontalier à la preuve[5] l'illustre à nouveau, puisque les États-Unis font valoir une exception pour toute requête susceptible de porter atteinte au *Freedom of speech*, portant notamment sur les données de contenu, étant rappelé que dans l'écrasante majorité des cas les données numériques sont en possession des réseaux sociaux ou hébergeurs américains.

Toutefois, des marges de manœuvres sont parfois possibles sur certaines catégories de données, telles les adresses IP, moins sensibles que les correspondances elles-mêmes. Ainsi les échanges institutionnels entre autorités publiques et plateformes privées peuvent aboutir à de réelles avancées, à l'instar de Facebook qui a modifié en juillet dernier ses pratiques, afin de mieux répondre aux réquisitions judicaires visant les auteurs de contenus haineux. Un futur règlement actuellement en cours de négociation au parlement européen devrait également faciliter ces premiers actes d'enquêtes.

2. La régulation des messages de haine

Quand il s'agit de régulation de messages de haine, on peut distinguer trois approches essentiellement différentes.

L'approche prônée notamment aux États-Unis qui consiste à laisser toute responsabilité et liberté aux plateformes. Des plateformes s'attaquent donc au sujet, y affectant parfois des ressources

considérables avec des succès mitigés. Leurs efforts souffrent d'un déficit de légitimité et sont très critiqués.
Le contrôle étroit des réseaux sociaux par les États, prôné principalement par des régimes totalitaires, mais tentant aussi pour les démocraties. En supposant que les États aient les moyens d'un tel contrôle, on peut questionner leur légitimité à le réaliser seuls. Et même, la solution des problèmes serait alors au prix du recul de la démocratie.
Une troisième voix est envisageable, un modèle européen conforme à des valeurs universelles qui protège la liberté d'expression bien affirmée, mais aussi la liberté d'être correctement informé, et d'être protégé des prédateurs du réseau, humains ou organisations. Les trois facettes d'une telle régulation, comme souligné dans une tribune du Monde par un groupe de ministres français[6], sont : « punir les auteurs de comportements illicites, responsabiliser les réseaux sociaux et améliorer l'éducation et la formation des citoyens, en premier lieu des plus jeunes ». Nous nous focalisons dans cet article sur la seconde.
Les propositions de la « mission FB ». Début 2019, un groupe de fonctionnaires français, à la demande de l'État et avec le soutien de Facebook, a étudié comment était réalisée la modération des contenus haineux dans les réseaux sociaux et en particulier Facebook. À partir de ce constat, il a proposé une structure de modération avec pour vocation de dépasser le cadre de Facebook, des contenus haineux, et de la France.

Trois principes directeurs sont préconisés : suivre une logique de conformité où le régulateur supervise la mise en œuvre de mesures préventives et correctrices au sein des réseaux sociaux ; se concentrer sur les acteurs systémiques sans créer de barrière à l'entrée à de nouveaux acteurs européens ; assurer une fonction de régulation en « mode agile » et non figée afin d'éviter une obsolescence prématurée.

La politique publique de régulation serait garante des libertés individuelles et de la liberté d'entreprendre des plateformes. Elle serait mise en œuvre en toute transparence par une autorité administrative indépendante en partenariat avec les différentes branches de l'État, et avec la participation effective de la société civile.

L'autorité régulerait la responsabilisation des principaux réseaux sociaux via le contrôle des obligations de transparence des fonctions d'ordonnancement et de modération des contenus, et de devoir de diligence leur incombant. Elle ne serait ni le régulateur des réseaux sociaux dans leur globalité, ni le régulateur des contenus spécifiques qui y sont publiés. Surtout, elle ne serait pas compétente pour qualifier les contenus pris individuellement (du domaine de la justice). Elle coopérerait avec les services de l'État et les services judiciaires. D'autre part, elle participerait activement à un réseau des régulateurs européens.

Le gouvernement de son côté, via son pouvoir règlementaire, fixerait les principes comme l'obligation de défendre l'intégrité du réseau social et de ses membres, et le cadre de la régulation comme les seuils de déclenchement des obligations ou les modalités des obligations de transparence des fonctions d'ordonnancement des contenus.

Le travail de ce groupe, limité dans le temps, ne visait pas l'exhaustivité. Certains sujets n'ont pas été examinés en détail comme l'analyse de l'impact concurrentiel du schéma de régulation proposé sur les autres offres de services de réseaux sociaux[7] et les échanges de contenus au sein de groupes privés sur les réseaux sociaux (dont service de messagerie privée type Telegram ou WhatsApp). Les réseaux sociaux « non-coopératifs », qui ne répondent pas à une rationalité économique classique, qu'ils soient prisés des activistes (4chan, 8chan…) ou

contrôlés par un État étranger poursuivant des stratégies d'influence, n'ont pas été pris en compte.

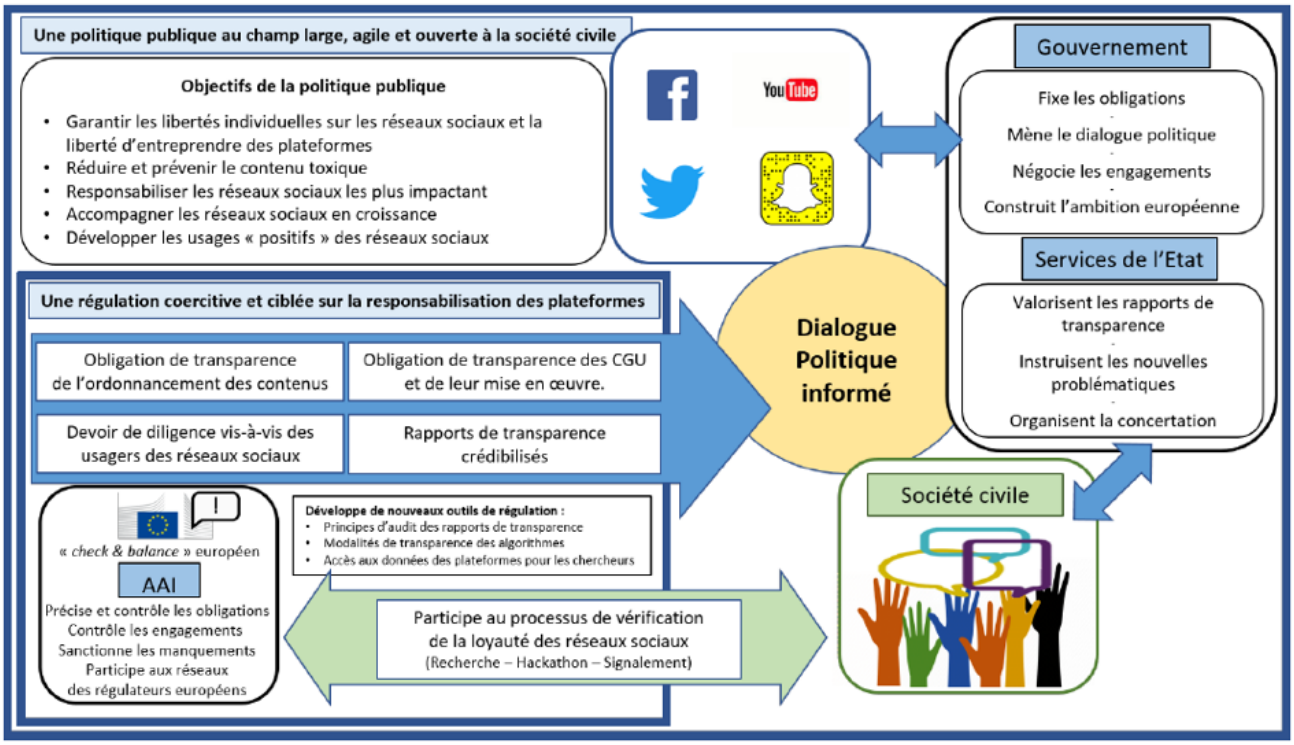


Figure 1 Schéma extrait du rapport « Régulation des réseaux sociaux »

3. Le régulateur national, réseau social

Le problème ne peut être selon nous résolu que par la combinaison des efforts des plateformes, des services de l'État, de la justice et de la société civile. La participation de la société civile est indispensable pour que, quelle que soit la modération des réseaux envisagée, elle soit perçue comme légitime par les internautes.

Cela conduit à la transparence des plateformes pour que les internautes comprennent comment la modération fonctionne et qu'ils aient confiance dans ses choix. Un monitoring fin de l'activité de modération doit être mis en place avec le régulateur qui partagera ces informations avec la société civile. Les internautes doivent pouvoir participer activement à la plateforme par leurs signalements, en pouvant suivre les procédures et faire appel des décisions. Ils devront en particulier être informés des motifs d'une modération qui les concerne, si le contenu a été jugé indésirable ou même toxique selon les CGU mondiales de la plateforme ou illégal selon une norme nationale ou européenne.

Cela conduit également à ce que la société civile soit associée à la spécification des choix de modération de la plateforme, à côté de l'État et de la justice, par l'intermédiaire notamment des associations d'internautes, et des chercheurs en informatique et en SHS.

Cela nous paraît être des conditions indispensables pour que la modération soit acceptable, pour que les blocages significatifs de contenus voire d'internautes, puissent se réaliser sans lever des soupçons de censure, sans craintes d'atteintes excessives à la démocratie. Le processus de

modération doit au contraire permettre de consolider la démocratie, de la réinventer, dans une transparence quasi-sacrée avec une vraie implication de la société civile.

Le régulateur pourrait également veiller aux formations et conditions de travail des employés chargés de la modération de ces plateformes, même si des progrès ont pu être réalisés notamment après une première série de révélations dans la presse outre-Atlantique[8]. Les dimensions du flot de contenus conduisent à une culture de la performance, un modérateur n'ayant en moyenne que quelques secondes ou minutes pour « traiter » un contenu. Des temps de formation renforcés, une sensibilisation à la culture locale et linguistique des contenus modérés, sans oublier des garanties sociales et une valorisation des carrières semblent s'imposer. Le temps de la modération doit aussi permettre, dans les cas litigieux, un véritable dialogue entre le modérateur et l'usager/créateur de contenu, afin de comprendre le contexte et éclairer le modérateur.

Enfin, on peut largement remettre en cause la conception extensive des clauses de type NDA (*Non Disclosure Agreement*) qui, sous couvert légitime de respecter la vie privée des usagers, prennent des airs de baillons inavouables imposés aux salariés, rarement employés par les plateformes elles-mêmes mais par des prestataires. Cette culture du secret est en totale contradiction avec la transparence nécessaire pour l'acceptabilité de la modération. Les premiers lanceurs d'alerte commencent d'ailleurs à se manifester, et un régulateur national semble un interlocuteur privilégié pour obtenir des informations de première main[9].

4. Le numérique à la rescousse

Pour avoir un espoir de régler ces problèmes des plateformes, il faut se déplacer volontairement dans le monde du numérique et intégrer les forces et faiblesses de ses structures technologiques.

Détection de contenus nocifs. Des algorithmes sont de plus en plus utilisés pour la détection de contenus toxiques ou illégaux. La question est complexe. Si les modérateurs humains tombent facilement d'accord sur des contenus « manifestement » terroristes, violents, haineux, etc., la qualification des contenus est plus complexe dans une large zone grise où le manifestement n'est plus de mise. Les modérateurs humains se divisent alors sur la question de « bannir ou pas ». La question peut également diviser les magistrats et seule une décision de justice peut alors trancher. Des algorithmes vont typiquement se fonder sur l'apprentissage automatique à partir de corpus de données annotées par des humains. Ils vont essayer de faire émerger un point de vue de compromis entre tous les modérateurs humains.

Dans ce contexte, une tendance de la justice questionne. Dans une décision du 3 octobre 2019, la Cour de Justice de l'Union européenne[10] précise qu'un tribunal d'un pays de l'Union européenne peut demander à un réseau social de retirer non seulement un contenu jugé illégal (procédure classique) mais également tout contenu « identique ou équivalent », sans même attendre son signalement, l'obligation pouvant être étendue au niveau mondial. Au-delà de cette interprétation qui élargit l'exception au principe de non surveillance générale des contenus de la part des hébergeurs[11], on pourra noter une relative imprécision sur la nature d'un contenu « identique ou équivalent ». Un texte peut être modifié caractère par caractère. À quel moment cesse-t-il de devenir identique ou équivalent ? Et pour une photo, si la résolution est modifiée, le

cadrage, si les couleurs sont modifiées pas à pas, à quel moment cesse-t-elle de devenir identique ou équivalente ? La notion subtile de « message véhiculé » paraît centrale.

Le raisonnement de la Cour se justifie essentiellement par son désir de rendre efficace l'injonction de retrait et de prévenir la réitération de l'acte illicite, sans obliger la victime à « devoir multiplier les procédures ». Or l'acte illicite « résulte non pas en soi de l'emploi de certains termes, combinés d'une certaine manière, mais du fait que le message véhiculé par ce contenu est qualifié d'illicite », comme des propos diffamatoires (§39-41).

Une interprétation plus large encore conduirait donc les plateformes à bloquer « par analogie » des contenus qui présenteraient des caractères semblables à ceux trouvés dans des contenus jugés illégaux, en tant qu'indices probables d'un « message véhiculé » équivalent. Se pose alors la question d'évaluer automatiquement ces analogies. C'est ce que font aujourd'hui les algorithmes de détection, la responsabilité de la qualification étant laissée ultérieurement à des modérateurs humains.

Les algorithmes ont l'avantage de « lisser » des choix humains qui peuvent présenter une large variance car trop souvent dans la subjectivité ; les signalements des internautes sur les réseaux sont notamment en moyenne de piètre qualité. Les algorithmes présentent aussi l'avantage de permettre une réaction rapide, et ce même avant que le contenu ait pu être vu par un internaute et causer des dégâts. Pour ces raisons, les algorithmes seront vraisemblablement de plus en plus la clé de voute de la modération, en termes de détection de contenus nocifs et de priorisation des actions des modérateurs humains. S'ils sont déjà performants dans les domaines du terrorisme et de la pédopornographie, les algorithmes de détection rencontrent, avec les messages de haine, tout comme avec les *fakenews*, des défis plus grands encore. Dans ces deux domaines, la qualification est plus complexe et il ne faut surtout pas attendre des algorithmes une « vérité » absolue :

parce qu'une telle vérité n'existe pas,
parce qu'il peut leur manquer des éléments de contexte indispensable pour évaluer la nature véritable d'un contenu et, surtout,
parce que ces algorithmes sont encore très perfectibles.
Si on peut espérer qu'ils apporteront une aide considérable à la modération, il est indispensable de collectivement travailler à améliorer les algorithmes pour les différentes facettes de la modération sans croire leurs résultats aveuglement et sans en attendre des miracles. Une condition essentielle de leur utilisation est la qualité de leurs résultats, qui doit être mesurée en permanence.

Les données de la modération. Comme déjà souligné, ces algorithmes s'appuient, dans une phase d'entraînement, sur des corpus de données. La qualité de la modération tient donc en grande partie de la qualité des données, et donc du travail des humains qui développent ces corpus. Ce sont des choix humains qui guident les propositions des algorithmes de modération.

De tels corpus sont donc essentiels pour le bon fonctionnement de la modération, en cela ils forment des « données d'intérêt général ». Il faut que ces données soient disponibles pour tous, en particulier pour les chercheurs et pour les petites entreprises confrontées aux problèmes et qui n'ont pas les moyens de les obtenir. On notera que si les plateformes semblent parfois soucieuses de partager de telles données, leur tendance naturelle est d'avoir du mal à les ouvrir.

Facebook, par exemple, a mis en place un partenariat avec des chercheurs. En septembre 2019, ces chercheurs ont menacé de quitter ce partenariat parce qu'ils n'avaient pas accès aux données[12]. On peut aussi s'interroger sur la liberté d'expression de ces chercheurs quand ils dépendent aussi étroitement des plateformes pour les données sur lesquelles ils travaillent, voire parfois pour leurs ressources financières.

Ces algorithmes et leurs données d'apprentissage prennent désormais une importance considérable dans notre société en évaluant les contenus qu'il est acceptable ou pas de partager, ils participent à la définition de notre société et leur régulation s'impose :

Transparence : on doit leur demander d'être transparents sur les traitements algorithmiques et les données qui servent à les entraîner.
Supervision : le régulateur doit surveiller ces algorithmes pour en déceler les manques ou les excès, puis en alerter la plateforme. La tâche est complexe et exige de fortes compétences du régulateur. Il pourra aussi s'appuyer sur le recueil de données de la foule et sur les travaux de chercheurs.
Co-design : les plateformes décident déjà leur modération. Même si le sujet est délicat, on peut collectivement parvenir à les aider à faire des choix aussi essentiels.
L'accélération. Un nœud du problème est qu'un contenu posté par un internaute sur une plateforme peut devenir viral et rapidement atteindre des milliers de personnes, voire des millions. Bien sûr, le créateur reste l'internaute. Mais la plateforme permet la viralité, avec des usagers diffuseurs qui donnent un effet de levier à l'usager créateur, et surtout elle l'encourage même en « accélérant » ce contenu, par exemple par le système de recommandations.

En cela, la plateforme joue un rôle essentiel dans la propagation de l'information, et peut avoir une influence considérable sur l'opinion publique. Les plateformes ont longtemps refusé cette responsabilité, se retranchant derrière le fait qu'elles n'éditent pas les contenus. Ce n'est plus possible aujourd'hui : leurs algorithmes et les données numériques sur lesquels elles s'appuient sont tenus pour responsables.

Les algorithmes de recommandation doivent participer du même effort de transparence, supervision et co-design.

4. La dimension internationale

Facebook met en place fin 2019 un « *Oversight Board* » (conseil de surveillance) international d'une quarantaine de membres[13]. S'inspirant sans doute de formations en assemblée plénière de certaines juridictions, amenées à dire le droit dans des affaires de principe, participant à la création prétorienne de la norme, son rôle sera de trancher les cas les plus litigieux et les plus contestés par les auteurs du contenu, et en quelque sorte de définir « la norme » du réseau. Des garanties d'indépendance sont évoquées, notamment une gestion de ce « conseil de surveillance » par un trust, certes financé intégralement par Facebook mais extérieur à sa structure de décision.

Toutefois, aussi louable soit l'intention, il nous paraît indispensable d'éviter toute confusion avec une quelconque « Cour suprême » afin de respecter clairement les prérogatives des systèmes

judiciaires des États. La justice française est ainsi rendue « *au nom du peuple français* » (article 454 du code de procédure civile), et devra conserver le dernier mot en la matière, quitte à assumer des divergences d'interprétation avec d'autres droits locaux. Cette proposition tient, nous semble-t-il, d'une tentation de Facebook de trouver en interne une solution à un problème qui doit par essence impliquer aussi les États, leurs justices, et les sociétés civiles.

Il existe par exemple des particularités bien nationales, telle l'incrimination en France du négationnisme depuis la loi Gayssot du 13 juillet 1990, confortée en 2016 par le Conseil constitutionnel[14]. Là encore, une fine pesée avait été opérée par la juridiction constitutionnelle, qui à l'inverse censura une disposition législative visant à étendre l'infraction de négationnisme notamment au génocide arménien, la considérant non nécessaire ni proportionnée, aucune juridiction nationale ou internationale n'ayant jamais jugé les faits en cause, susceptibles de faire l'objet de débats historiques[15]. De manière symétrique, la liberté d'expression doit également être protégée par le régulateur par des remises en cause éventuelles par les plateformes, pour le moment relativement limitées[16].

La plateforme ne peut donc être « souveraine » en ce qu'elle doit se plier à la souveraineté des États, qui ne peuvent se résumer à des marchés d'usagers. Une des conséquences est la prise en compte par la plateforme dans sa politique de modération des arbitrages légaux pris dans chaque pays démocratique relatifs à la liberté d'expression.

Se posera ainsi la question de savoir si le régulateur pourra infléchir les CGU des plateformes, ou leur interprétation, afin de préserver un droit d'expression politique d'un pays. Par exemple, on sait aujourd'hui combien le marché émergeant de la Chine est important auprès de certaines entreprises numériques, et l'expression de soutien aux manifestations récentes à Hong Kong peut induire une pression économique en faveur d'une censure (habillée en modération standard), ou de techniques plus classiques de manipulation de l'information[17]. Pour le moment, les réseaux sociaux tels que Twitter ou Facebook semblent résilients, mais la vigilance semble être de mise[18].

La France n'a sans doute pas seule un poids suffisant pour faire bouger des plateformes de la taille de Facebook. La bonne granularité pour une telle régulation est donc bien l'Union européenne. Après le succès du RGPD, qui intéresse de nombreux pays, l'Europe a l'opportunité d'apporter une autre contribution majeure à la démocratie. Une telle régulation implique donc un régulateur européen qui conçoit les grandes lignes de la régulation et coordonne les régulateurs nationaux, ce qui existe déjà en matière de données personnelles ou plus récemment de cybersécurité.

Les initiatives nationales conservent leur intérêt, mais davantage dans un premier temps stratégique, afin d'établir un rapport de force avec les plateformes et de déplacer les lignes. La loi NetzDG allemande et la future loi dite Avia en sont des démonstrations éclatantes.

Dans un deuxième temps, la dimension européenne permet à la régulation d'avoir plus de poids vis-à-vis des plateformes hyper puissantes, tout en réduisant les risques de régulation nationale inadaptée et manichéenne, réagissant à des événements particuliers. Le régulateur européen peut vérifier et équilibrer les réponses.

Toutefois, si l'Europe est le bon niveau de granularité pour une telle modération, le portage de la régulation au niveau européen soulève un risque sérieux, à savoir le choix des critères de compétence du régulateur. Le critère du « pays de destination », c'est-à-dire le pays où réside l'internaute qui a été (ou pense avoir été) victime d'un discours de haine est le plus adapté, et pas le critère du « pays d'installation de la plateforme ». En effet, concrètement cela reviendrait à confier aux autorités hôtes (comme l'Irlande) la modération de la quasi-intégralité des plateformes systémiques quand les effets toxiques sont massivement ressentis et la volonté de corriger ailleurs, ce qui résulterait en un affaiblissement de l'engagement du régulateur.

La régulation du cyberespace est une gageure, et s'il est toujours facile de voter une loi de régulation, mieux vaut armer correctement son régulateur, le doter d'une souplesse d'action suffisante, d'une compréhension poussée de l'écosystème des algorithmes, avec des objectifs ambitieux et porteurs des valeurs démocratiques, sans quoi ladite loi risque bien de n'être que… virtuelle.

Serge Abiteboul (Inria et ENS, Paris) et **Jacques Martinon** (magistrat judiciaire)

[1] *https://www.numerique.gouv.fr/uploads/rapport-mission-regulation-reseaux-sociaux.pdf*

[2] En France, 35 millions d'usagers actifs mensuels et 22 millions quotidiens pour le service Facebook (Q2 2019).

[3] *« Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. […]. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique ».*

[4] CEDH, Handyside v. the United Kingdom, arrêt du 7 Déc. 1976.

[5] https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019?utm_source=b4d391f0-3d36-4077-8793-d5b2b06944c1&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate

[6] https://www.lemonde.fr/idees/article/2019/06/18/mettre-fin-a-l-impunite-sur-le-web-des-ministres-soutiennent-la-proposition-de-loi-avia_5478019_3232.html

[7] Le risque de travailler avec des acteurs comme Facebook ou YouTube, et dans une moindre mesure, Twitter, est de surdimensionner le dispositif de régulation, de créer une barrière à l'entrée insurmontable pour des acteurs de taille intermédiaire ou de nouveaux entrants.

[8] https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona

[9] https://www.theverge.com/2019/6/19/18681845/facebook-moderator-interviews-video-trauma-ptsd-cognizant-tampa

[10] CJUE 3 oct. 2019, *Facebook Ireland Limited c/ Eva Glawischnig-Piesczek*, aff. C-18/18

[11] Article 15, paragraphe, 1 de la directive « commerce électronique » 2000/31/CE du 8 juin 2000, transposé à l'article 6-I, 7, de la loi n° 2004-575 du 21 juin 2004, dite « LCEN »

[12] https://www.lemonde.fr/pixels/article/2019/08/28/des-chercheurs-en-partenariat-avec-facebook-posent-un-ultimatum_5503821_4408996.html

[13] https://fbnewsroomus.files.wordpress.com/2019/09/oversight_board_charter.pdf

[14] Décision n° 2015-512 QPC du 8 janvier 2016.

[15] Décision n°2016-745 DC du 26 janvier 2017.

[16] On rappellera la politique très stricte de certains réseaux sociaux sur la nudité, même partielle et dénuée de caractère pornographique ou choquant.

[17] https://www.nytimes.com/2019/08/19/technology/hong-kong-protests-china-disinformation-facebook-twitter.html

[18]http://www.slate.fr/story/182751/lutte-contre-fakes-news-facebook-refuse-supprimer-pub-donald-trump-contient-une-usa

25 FÉVRIER 2019

Un robot dans la robe des juges

Nous vivons au temps des algorithmes, ces outils ne décident rien mais fournissent des réponses statistiquement significatives, au point de provoquer un dilemme au moment de prendre une décision, quand notre conviction intime rentre en contradiction avec ce que le résultat de l'algorithme propose. Et un domaine où cela devient critique est celui de la justice. Voyons comment dépasser ce dilemme avec Serge Abiteboul. ***Thierry Viéville****.*

Les algorithmes exécutés par des ordinateurs sont entrés dans nos vies : ils nous conseillent des films, nous proposent des chemins pour nous rendre à notre prochain rendez-vous… Bientôt, ils conduiront nos voitures ou nous permettront de rester chez nous dans notre quatrième âge. En prenant autant d'importance, ils soulèvent des questionnements, des inquiétudes. Prenons un exemple frappant dans un domaine régalien, la justice. Aux États-Unis, le logiciel Compas

Fresque représentant la justice de Luca Giordano ©wikicommons

assiste les juges pour décider de libérations conditionnelles, en évaluant le risque de possibles récidives – la décision de remise en liberté est strictement liée à la probabilité de récidive. L'algorithme assiste, mais ne décide pas. Oui, mais un juge aura-t-il le courage, ou la légèreté, de remettre un condamné en liberté contre l'avis du logiciel si l'on peut prouver que l'algorithme fait statistiquement de meilleures prédictions que les juges ?

Justice et inégalité ©wikicommons

La question est philosophique : y a-t-il des tâches de telles natures que les confier à des machines nous ferait perdre une part de notre humanité, des tâches qu'il faut leur interdire même si elles les réalisent mieux que nous ? Nous ne répondrons pas à cette question, mais relativisons son importance aujourd'hui. Si les algorithmes deviennent de plus en plus intelligents, ils sont loin de pouvoir, par exemple, remplacer les juges dans des cas encore plus complexes que celui de la libération conditionnelle aux États-Unis. Quand des algorithmes participent à la vie de la cité se pose également la question de leur responsabilité. Revenons sur le logiciel Compas. Il présente sur un juge l'avantage d'une certaine cohérence. Il a été montré notamment que les décisions des juges sont dépendantes de l'heure ; il vaut mieux passer après le repas qu'avant. Et celles des cours de justice, par exemple aux prud'hommes, varient énormément d'une chambre à une autre. Pa de cela avec les algorithmes ! Ils peuvent garantir une certaine cohérence.

Nous pourrions également espérer qu'ils soient plus « justes », qu'ils ne discriminent pas suivant les origines ethniques, le genre… Pourtant, des journalistes ont évalué les prédictions de Compas et découvert qu'il surestimait largement les risques de récidives des condamnés noirs. Des informaticiens racistes ? Pas vraiment, mais on ne sait pas écrire un algorithme qui prédise les récidives – la question est trop complexe. Alors on utilise un algorithme d'apprentissage automatique. On lui apprend le travail à réaliser en l'entraînant sur un grand volume de données de décisions de juges, à imiter des humains. Ce sont ces décisions, qui présentaient des biais raciaux, que Compas a reproduites. Il faut avoir conscience des problèmes que l'utilisation de programmes informatiques peut soulever, vérifier ces programmes et les données qui sont utilisées pour les « entraîner », surveiller leurs résultats.

Notre exemple nous a permis d'insister sur un aspect essentiel de la responsabilité : l'absence de biais, l'équité. La transparence en est un autre. Nous pouvons, par exemple, nous inquiéter de ce que Facebook fait de nos données personnelles dans une relative opacité. Nous pourrions aussi parler de la loyauté : faut-il accepter un service qui propose des restaurants en disant ne tenir compte que des avis de consommateurs et qui remonte en réalité dans sa liste de résultats les commerçants qui paient pour ça ? La responsabilité sociétale des algorithmes a nombre de facettes.

Les algorithmes peuvent nous permettre d'améliorer nos vies. Il faut corriger leurs défauts, combattre leurs biais inacceptables. Il peut s'avérer difficile de vérifier, d'expliquer leurs choix, s'ils proviennent de statistiques mettant en jeu des milliards d'opérations ou s'ils se basent sur

des motifs complexes découverts par des algorithmes d'apprentissage. Pourtant, notre incompétence ne peut pas servir de justification pour autoriser le viol de principes moraux. Quand les effets des décisions sont sérieux, comme garder une personne incarcérée, sans doute vaut-il mieux attendre d'être certain du fonctionnement de l'algorithme, exiger qu'il explique ses choix et, bien sûr, faut-il pouvoir les contester.

Serge Abiteboul, Inria et ENS, Paris

Cet article est paru dans Le magazine La Recherche, N°531 • Janvier 2018

Saint Thomas d'Aquin : pour lui, la justice est une morale
©wikicommons

Tweet

21 SEPTEMBRE 2018

Blockchain publique : la fin des tiers juridiques de confiance ?

Les blockchains constituent un sujet au cœur de l'actualité des technologies numériques. Sur le plan juridique, elles suscitent également de nombreuses interrogations dont celle de la disparition annoncée des tiers de confiance, spécialement des tiers juridiques de confiance. Lêmy Godefroy, spécialiste du droit du numérique à l'Université Côte d'Azur, nous livre ici son point de vue sur le possible devenir des tiers juridiques de confiance dans l'univers des blockchains publiques. ***Thierry Vieville***

Lire, écrire, exécuter, trois mots qui résument les fonctionnalités des blockchains. Cette technologie s'apparente à un registre recevant des données lues par tous les participants si la blockchain est publique ou par quelques personnes si elle est privée. Associée aux *smart contracts* qui recèlent un potentiel varié d'usages (paiement d'intérêts, versement d'indemnités,

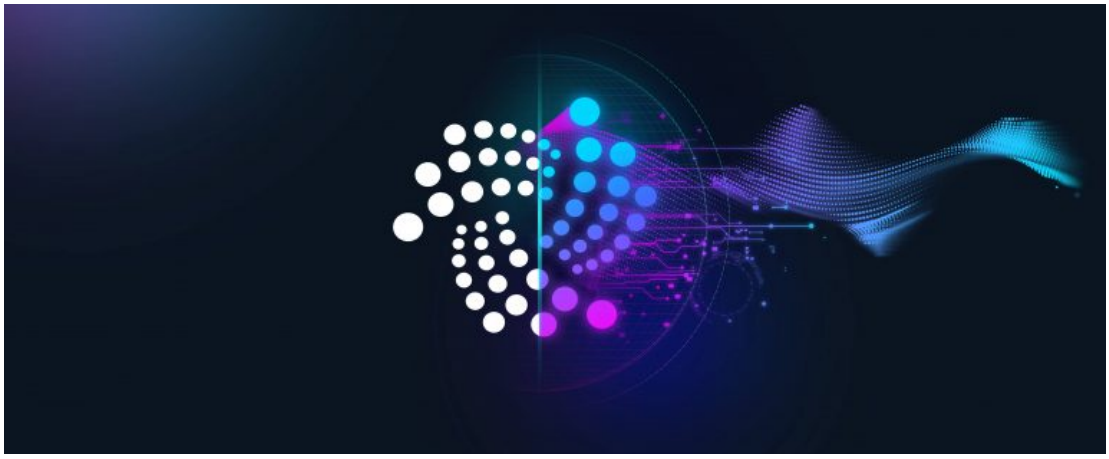
blocage d'un objet connecté, etc.), elle sert de support à l'exécution automatisée d'instructions si certaines conditions prédéterminées sont remplies. La particularité de la blockchain publique réside dans son caractère ouvert et décentralisé. Aucun intermédiaire n'est nécessaire pour valider des informations préalablement à leur enregistrement sur le réseau[1]. C'est en cela que cette technologie conduirait à se passer des tiers juridiques de confiance (agents de l'état-civil, huissiers de justice, notaires, juges, etc.) dont la caution est remplacée par la transparence du processus, la visibilité des opérations et la détention d'une copie du registre par l'ensemble des membres. Toutefois, cette décentralisation montrerait des limites qui amènent à s'interroger sur la nécessité d'en appeler in fine à ces tiers pour jouer le rôle d'interface entre l'extérieur et l'intérieur de la blockchain ou de régulateur des systèmes blockchain.

La confiance par la démultiplication des contrôles internes à la blockchain

Les transferts de données (unités monétaires, informations personnelles, relations d'affaires, etc.) de pair à pair au moyen des blockchains reposent sur la démultiplication d'un contrôle décentralisé. Les utilisateurs adoptent le protocole qui établit les modalités de validation et d'enregistrement sur le réseau. Par le procédé du minage, ce sont encore eux, alors appelés mineurs, qui s'assurent que les opérations sont conformes.

Les mineurs se substituent aux tiers de confiance habituellement chargés par les parties de transcrire une pièce ou d'effectuer un ordre de transactions. Toutefois, si chaque usager de la blockchain peut théoriquement être mineur, tous n'ont pas les moyens de l'être et seuls ceux qui possèdent une force de calcul suffisamment importante – et, partant, une grande puissance économique – pour résoudre des problèmes mathématiques complexes sont capables de procéder aux opérations de vérification du respect du protocole. Autrement dit, ce pouvoir décentralisé est censitaire[2], ce qui génère des doutes sur l'organisation démocratique des blockchains publiques et des craintes d'accaparement de leur gouvernance, les mineurs détournant à leur profit ce pouvoir originellement voulu collaboratif et participatif[3].

Pour contrecarrer cette dérive vers une centralisation contrainte[4], un nouveau protocole appelé « iota » a été imaginé dans le domaine des cryptomonnaies. Alors que les mineurs sont rémunérés pour chaque validation effectuée, « iota » repose sur la règle selon laquelle l'utilisateur qui demande l'inscription d'une transaction doit en valider deux réalisées par d'autres membres. Chaque utilisateur est donc réellement un validateur d'autant que la preuve de travail n'exige pas de puissance de calcul élevée et peut être accomplie par des terminaux comme l'ordinateur portable ou le téléphone.



Il n'en demeure pas moins que ce contrôle informatique du respect du protocole et de la validité formelle des transactions (identité certifiée, compte approvisionné, acte signé, etc.) n'atteste pas de leur conformité au droit. Les tiers juridiques de confiance seraient ainsi de retour à l'interface du monde réel et de la blockchain.

Les tiers juridiques de confiance à l'interface du monde réel et de la blockchain

Les *smart contracts* intégrés à une blockchain illustrent pleinement le besoin de contrôle juridique des cas qui déclenchent l'application programmée d'instructions. Or, celle-ci dépend de données provenant de *l'extérieur* de la blockchain : le bien n'a pas été livré, un dommage a été causé, le vol de telle compagnie a décollé avec retard, etc. Par construction, une blockchain ne peut pas récupérer ces informations par elle-même. Celles-ci doivent lui être apportées. C'est ainsi que le concept d'oracle a été créé. Un oracle fournit un service qui consiste à entrer une donnée extérieure dans la blockchain à un instant prédéfini. Ultérieurement, le *smart contract* va rechercher cette information stockée sur la blockchain pour lancer sa programmation.

Certains systèmes qui délèguent à la technologie la tâche de produire de la sécurité recourent à des oracles automatisés pour garantir que les données insérées dans la blockchain sont fidèles à la réalité. Ils fonctionnent selon le procédé de la « preuve d'honnêteté » (TLS Notary proof)[5] ou du consensus (consensus-based oracle)[6].

Mais leur intervention laisse en suspens le problème de la conformité juridique de l'information déposée sur la blockchain. La réintroduction d'un tiers de confiance humain dans un rouage pourtant *trustless* s'imposerait, par exemple, quand il s'agit de vérifier l'identité civile d'une personne, la légalité d'un titre de propriété ou encore l'existence d'une créance. Les traditionnels tiers juridiques de confiance se verraient sollicités comme validateurs d'un fait, d'un document, d'un état, etc.

Cette recentralisation questionne sur la régulation des systèmes blockchains et, notamment, sur leur gouvernance.

La régulation des blockchains : quelle gouvernance ?

Différents modes de régulation sont envisageables.

Une régulation souple par un mécanisme de normalisation à l'échelle internationale pourrait être mise en place. Cette normalisation, d'application volontaire, énoncerait les exigences minimales requises pour assurer la fiabilité des blockchains.

Des mesures typiquement techniques seraient également une piste. Par exemple, pour préserver le secret des données, l'idée a été émise de reporter sur la blockchain non pas l'information brute elle-même, mais son empreinte digitale. Celle-ci servirait de preuve du dépôt et sa lecture serait possible uniquement par des personnes autorisées[7].

Enfin, un droit des systèmes blockchain pourrait reposer sur le triptyque législateur/juge/arbitre.

La loi organiserait les fonctionnalités de la blockchain. Les règles de preuve en vigueur pourraient y être transposées. La force probante des informations importées serait celle d'un acte sous seing privé (c'est à dire sois signature privée) ou authentique selon qu'un tiers juridique de confiance aurait attesté ou non de la réalité des données.

Quant au juge, il interviendrait sur saisine des parties pour apprécier la légalité de la formation et de l'exécution des *smart contracts* (par exemple en cas de codage de conditions illicites ou manifestement abusives) ou pour prononcer des sanctions (dommages-intérêts après l'annulation d'un accord invalidé). Cette intervention judiciaire aurait lieu dans le cadre d'un règlement contentieux du litige né après qu'un contrat automatisé eut causé un dommage ou soulevé une contestation.

Mais il est également possible que l'une des clauses d'un *smart contract*, dans un contexte de résolution amiable, prévoie une disposition qui bloque le programme et engendre un mécanisme de règlement alternatif des conflits par un arbitre dont la décision interférerait sur la blockchain par l'entrée de nouvelles variables.

Blockchain publique et tiers juridique de confiance se complémenteraient ainsi pour une sécurité accrue indispensable au développement de cette technologie.

Lêmy Godefroy, Maître de conférences spécialisée en droit du numérique, au GREDEG de l'Université de Nice Côte d'Azur.

Pour en savoir plus :

Une présentation de la blockchain
Une podcast qui explique bitcoin et blockchain

Notes :

1 Les blockchains privées recourent de manière privilégiée au **minage par tiers de confiance.**

2 Antoine Garapon, « La blockchain va-t-elle remplacer tous les tiers de confiance ? », interview de Primavera De Filippi, France Culture, 15 février 2018.

3 Voir par exemple la controverse entre le Bitcoin Core et le Bitcoin Unlimited.

4 D'autres techniques de minage ont été imaginées comme le « minage par consensus ». « Un algorithme permet à des nœuds maîtres du réseau de se mettre d'accord entre eux sur les opérations à accepter. L'identité des nœuds maîtres est connue ». Ou encore le « minage par preuve d'enjeu ». Dans ce cas de figure, « un des utilisateurs est désigné pseudo-aléatoirement avec une probabilité proportionnelle à sa fortune détenue sur la blockchain. Ce modèle fait donc porter la responsabilité du minage sur ceux qui ont le plus d'enjeu dans la blockchain [et] (…) qui ont le plus intérêt à maintenir la confiance dans le système » (Jean-Baptiste Pleynet, « Le minage expliqué aux non-initiés », https://medium.com/@JB_Pleynet/le-minage-expliqu%C3%A9-aux-non-initi%C3%A9s-b511b5a33117).

5 Cette preuve, publique et vérifiable, garantit que la donnée entrée sur la blockchain est identique à celle qui a été récupérée par l'oracle. Par conséquent, si l'oracle automatisé entre dans la blockchain une donnée non-conforme à la donnée réelle, cette information erronée sera repérée par les participants de la blockchain. https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/

6 https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/ Si tous les oracles automatisés transmettent la même information, alors celle-ci peut être considérée comme pertinente. https://www.mindfintech.fr/files/documents/Etudes/Landau_rapport_cryptomonnaies_2018.pdf

7 Primavera De Filippi, Aaron Wright, Blockchain and the law, Harvard University Press, 2018.

03 SEPTEMBRE 2018

Informatique, éthique et régulation

Un nouvel « Entretien autour de l'informatique ». Serge Abiteboul et Claire Mathieu interviewent Noëlle Lenoir, juriste, magistrate et femme politique. Première femme et plus jeune membre jamais nommée au Conseil constitutionnel, ministre des Affaires Européennes entre 2002 et 2004, elle a occupé de nombreuses fonctions, et en particulier a suivi la mise en œuvre de la loi informatique et libertés française. Elle parle à Binaire des liens entre le droit et l'informatique. Cet article est publié en collaboration avec The Conversation.

Noëlle Lenoir, Wikipédia

Binaire : pouvez-vous nous parler de votre carrière ?

Je suis de formation juridique. En 1982, alors que j'étais administrateur au Sénat depuis près de 10 ans, le sénateur Jacques Thyraud, alors rapporteur du budget de la justice, m'a demandé de venir diriger les services de la CNIL, dont j'ai été pratiquement la première directrice. Si le contexte était radicalement différent de celui d'aujourd'hui, la problématique de l'informatique et des libertés était finalement assez similaire. La protection des données était et est restée rattachée aux droits de l'homme, ce qui veut dire que toute collecte et tout traitement de donnée est vue potentiellement comme une atteinte aux libertés. C'est la marque de fabrique européenne. Toutefois, le « la » a été donné par la France dès les années 80. À la CNIL, j'ai participé à la mise en place des services et de l'institution elle-même. À mon avis, encore aujourd'hui, il n'y a pas assez de techniciens parmi les membres du collège de la CNIL ; par exemple, il devrait y avoir de droit un statisticien et un historien archiviste. Protection des données ne doit pas vouloir dire en effet destruction du patrimoine numérique national.

J'ai ensuite intégré le Conseil d'État, qui était très impliqué dans le droit de l'informatique. J'y ai participé à un rapport sur le sujet. Appelée en 1988 à diriger le cabinet de Pierre Arpaillange, ministre de la justice, j'y suis demeurée deux ans à m'intéresser au droit pénal en pleine transformation avec la préparation du nouveau code Pénal. Puis en 1990, le Premier ministre, Michel Rocard, m'a demandé de conduire une mission sur le droit de la bioéthique dans une perspective internationale et comparative. La France n'avait pas de législation tandis que le programme de décryptage du génome humain et la procréation médicalement assistée posaient des problèmes juridiques entièrement nouveaux. Comme vous le savez, la bioéthique inclut des problématiques liant la génétique à l'informatique comme le décryptage du génome humain ou les tests génétiques prédictifs. Ma mission, qui s'est conclue par un rapport remis au Président de la République et au Premier ministre, a débouché sur le dépôt de la première loi française de bioéthique que j'avais contribué à préparer.

Nommée en 1992 au Conseil constitutionnel, j'ai été confrontée à des lois de bioéthique. Une fois terminé mon mandat en 2001, je suis allée enseigner le droit de la bioéthique et le droit européen à la faculté de droit de Columbia, à New York, en tant que *visiting professor*. Ce fut

pour moi une très belle expérience. J'y ai découvert des méthodes d'enseignement très différentes des nôtres, plus interactives, moins directives, moins savantes, mais plus vivantes.

Ensuite, ce furent deux années passionnantes comme ministre des Affaires européennes (2002-2004), à l'heure de l'élargissement de l'Europe aux États de l'Europe centrale et orientale. Certains de ces pays étaient déjà en avance en matière d'informatisation de la société ; c'était et cela reste en particulier le cas de l'Estonie. J'ai visité en 2002 à Tallinn la salle du Conseil des ministres entièrement informatisée, les ministres ayant chacun leur ordinateur, et au diable les documents papier !

Je suis aujourd'hui avocate dans un cabinet américain, Kramer Levin, dont la maison-mère est à New-York. Après m'être spécialisée en droit de la concurrence, une discipline à la frontière du droit et de l'économie, je développe actuellement mon expertise en droit de l'informatique et de la protection des données personnelles. Ma formation de publiciste me conduit à travailler aussi sur des dossiers en droit public, dont fait partie le droit de la protection des données. Enfin, je suis centrée également sur la *compliance*, c'est-à-dire tout ce qui peut contribuer à aider les entreprises à prévenir, détecter et lutter contre la corruption, en application de la loi dite Sapin II. Ce que permet l'utilisation des *hotlines* par exemple à travers lesquelles tout salarié ou tout tiers à l'entreprise peut faire remonter des informations sur des infractions commises ou en voie de l'être. De même, le contrôle des transactions financières dans le cadre de la lutte contre le blanchiment d'argent passe-t-il essentiellement par des procédures informatisées. Le droit et l'informatique ont beaucoup de points en commun, ne serait-ce que les logiques qui les sous-tendent.

B : vous avez participé aux débuts de la CNIL. Comment voyez-vous cette institution ?

A l'époque, les « autorités administratives indépendantes » telle que la CNIL, dotées de prérogatives règlementaires autant que répressives, étaient toutes nouvelles. Pour moi, ces autorités relèvent d'un concept libéral, venu des États-Unis, qui veut qu'entre l'État et les opérateurs économiques, des institutions étatiques, mais indépendantes, aient le pouvoir de faire évoluer la norme juridique en fonction de l'évolution des technologies et de l'économie. Depuis environ 40 ans, on assiste à l'émergence d'une nouvelle forme de droit, plus ou moins contraignant, qui est négocié ou au moins discuté avec les acteurs économiques. Mais par ailleurs, les normes (recommandations, lignes directrices, règlements etc.) produites par ces autorités sont assorties de sanctions pécuniaires extrêmement lourdes. Elles sont certes le fruit de discussions entre l'autorité et l'entreprise contrevenante qui peut exercer ses droits de la défense ; mais l'autorité dispose d'une force de frappe qui lui donne un pouvoir considérable pour faire respecter ses recommandations. Pensez que la CNIL peut infliger des amendes allant jusqu'à 4% du chiffre d'affaires mondial, ce qui peut littéralement mettre à genoux une entreprise, lorsqu'en plus, l'amende prononcée fait chuter son cours de bourse. Même quand des amendes ne sont pas prononcées à l'encontre des opérateurs défaillants, les avertissements par exemple émis par ces autorités peuvent être rendus publics, à grand renfort de communiqué de presse, avec tous les dommages en terme de réputation que cela implique. Parmi les principales autorités administratives indépendantes, en dehors de la CNIL qui a été précurseur, on peut citer l'autorité de la concurrence, l'ARCEP, le Conseil supérieur de l'audiovisuel ou encore la récente agence anti-corruption.

La CNIL, elle, est exclusivement compétente en matière de protection des données personnelles des personnes physiques, c'est-à-dire de la vie privée. L'informatique constitue un formidable

progrès dans la gestion de l'information des individus, mais peut mettre en danger leurs libertés si elle fait l'objet d'une utilisation pernicieuse. La loi Informatique et Libertés en France, et le Règlement général européen sur la protection des données (RGPD) applicable depuis mai de cette année tentent de réaliser un arbitrage entre développement technologique et économique et protection des libertés.

Je me souviens que les principaux sujets d'intérêt pour la CNIL étaient à l'époque, avant Internet et le web, d'abord les fichiers de police et de renseignements, les fichiers de la sécurité sociale, et les fichiers fiscaux mis en place pour déceler dans les déclarations les anomalies susceptibles de déclencher des contrôles.

René Carmille, créateur du numéro de code individuel et de l'Insee

Le but était avant tout d'éviter l'interconnexion des fichiers administratifs. Cela était tabou et l'est encore. Le numéro de sécurité sociale (le NIR) était et reste considéré comme dangereux en soi, et il fallait éviter à tout prix qu'il ne serve aux interconnexions de fichiers. Permettez-moi en lien avec ce numéro d'évoquer l'histoire dramatique d'une personne exceptionnelle, René Carmille. Il a créé sous l'Occupation le Service National Statistique (qui deviendra l'INSEE en 1946) et le code individuel des citoyens qui deviendra le numéro de sécurité sociale. Seulement ce numéro a été détourné de sa vocation par le ministre de la Justice Raphaël Alibert pour distinguer les juifs et les tsiganes, et organiser les départs pour le STO. Carmille rentre dans la Résistance, cache des fichiers pour mettre au point un dispositif de mobilisation contre l'ennemi, fabrique de fausses cartes d'identité pour les juifs et les résistants. Arrêté à Lyon en 1944, atrocement torturé par Klaus Barbie, il meurt en 1945 au camp de Dachau. L'ENA devrait donner son nom à une de ses promotions, comme l'a fait en 2008-2009 l'EMCTA (Ecole militaire du corps technique et administratif).

Le numéro de code individuel créé par René Carmille est demeuré une sorte d'épouvantail. Ce n'est, à mon avis, plus justifié du fait de tous les autres moyens d'interconnexions de fichiers disponibles aujourd'hui.

Pour revenir à la CNIL, à ses débuts, lorsque j'y travaillais, elle s'intéressait à deux autres sujets qui paraissent préhistoriques aujourd'hui : le premier était celui de la vente par correspondance, car cela scandalisait qu'on puisse s'échanger des fichiers d'adresses. Le vrai sujet était le droit des personnes de ne pas être sollicitées par la publicité et de pouvoir demander à être retirées des fichiers. Ce que la CNIL a acté. Le second sujet avait trait aux travaux statistiques. Je dois dire qu'à mon grand étonnement, l'INSEE était la tête de turc de certains membres de la CNIL. Ceux-ci soulignaient que les chercheurs en général, et les statisticiens en particulier, ne protégeaient pas convenablement la masse de données en leur possession, puisqu'ils ne fermaient même pas leurs bureaux à clé et qu'ils ne rangeaient pas leurs dossiers dans des tiroirs ! Aujourd'hui encore, chercheurs et statisticiens sont en butte à une méfiance injustifiée.

Ce qui, à mon avis, a le plus fondamentalement changé dans les législations de protection des données personnelles, c'est qu'aujourd'hui, elles ont un effet extraterritorial. Ainsi le RGPD s'applique, indépendamment du lieu où sont traitées les données (dans un cloud en Californie, par exemple) dès lors que la personne concernée est en Europe. Cela va très loin et en outre les

conditions d'application de cette disposition ne sont cependant pas évidentes. Comme les Américains préparent eux-mêmes une législation semble-t-il fédérale sur la protection des données, il y aura certainement des conflits de lois ; un véritable casse-tête pour les juristes et les juges.

B : voyez-vous une transposition de ce qui a été mis en place pour la bioéthique dans le cadre du numérique ?

J'ai présidé deux comités de bioéthique [1], l'un auprès de la Commission européenne et l'autre à l'UNESCO. Au niveau européen, on a beaucoup travaillé sur le numérique : tests génétiques, dossier médical informatisé et accès aux données de santé, brevets sur le génome humain, etc. La bioéthique et le droit de la protection des données personnelles ont pour objectif commun d'aider à répondre à des situations concrètes inédites du fait des technologies nouvelles, et qui peuvent poser des questions de libertés individuelles, ou de vie privée. De plus, sans l'informatique, la biologie ne pourrait avancer.

B : maintenant se posent des questions d'éthique numérique qui dépassent le cadre de la médecine et de la biologie. Y a-t-il quelque chose à apprendre de l'expérience bioéthique ?

Le mot « éthique » est ambigu. Il recouvre à la fois une attitude, un comportement relevant de la responsabilité individuelle, et les mœurs, soit une notion sociétale renvoyant à des valeurs collectives. En 1983, François Mitterrand a créé le premier comité d'éthique au monde, non pas contre la science, mais parce que « Science sans conscience n'est que ruine de l'âme », selon l'expression de Rabelais.

Quelle est cette conscience ? Elle ne peut plus être totalement univoque dans un monde où les mœurs, c'est-à-dire les normes morales acceptées par la société, sont de plus en plus diversifiées sur un même espace. Dans un monde ouvert, des individus vivant côte à côte peuvent avoir des systèmes de valeurs différents. Les comités d'éthique n'essaient pas seulement de faire une synthèse. Ils rappellent les valeurs de base communes, mais à l'issue d'un débat ouvert entre philosophies et religions différentes : c'est l'éthique de la délibération. Les membres des comités d'éthique ont à l'origine des opinions et des sensibilités contrastées, et puis à la fin, ils trouvent un compromis acceptable par tous. Leurs décisions sont le fruit de rapports circonstanciés et documentés pour montrer qu'ils n'ont oublié aucun aspect de la question.

Pour autant, un comité d'éthique ne doit pas, selon moi, être relativiste. Il y a des principes intangibles sur lesquels notre société démocratique aujourd'hui grandement fragilisée par les intégristes et les *fake news* ne doit pas transiger : égalité entre les sexes, lutte contre le racisme, respect de la vérité, tolérance, solidarité, absence d'intention de nuire, etc.

En tant que Présidente du comité scientifique et éthique de Parcoursup, je constate que certaines informations au mieux approximatives, au pire tendancieuses ou erronées, circulent sur les réseaux sociaux, voire dans la presse. Tout se passe comme si, pour certains, il fallait systématiquement soupçonner les responsables politiques de vouloir le mal de la population, et en l'occurrence des jeunes. Au-delà de l'éthique de la génétique et de l'informatique, je plaide pour la mise en place d'une éthique de l'information technique et scientifique. Cette éthique

aurait pour but de permettre aux citoyens de juger par eux-mêmes des avantages et inconvénients de systèmes techniques complexes traduisant des choix politiques, au lieu d'être condamnés à s'en remettre à des interprétations dont ils ne sont pas en mesure de vérifier la fiabilité.

B : pensez-vous que la transparence des algorithmes puisse améliorer nos vies ?

Le droit à la transparence, on ne peut pas en avoir une vision absolue. Il est un principe général du droit, ancien et bien connu, suivant lequel « il n'y a pas de liberté générale et absolue ». Ce n'est pas parce qu'on est un citoyen qu'il faut pouvoir être dans le bureau du Premier Ministre pour écouter ce qu'il dit et assister aux réunions auxquelles il participe ; pour moi, ce n'est pas ça, la transparence. Elle est un outil essentiel de la démocratie directe, qui doit coexister avec les outils de la démocratie représentative et ses institutions légitimes. Elle ne peut s'y substituer; précisément pour préserver les équilibres démocratiques.

La loi pour la République numérique du 7 octobre 2016 a introduit, dans le code des relations entre le public et l'administration, une disposition selon laquelle en cas de décision concernant un individu prise sur le fondement d'un algorithme, l'intéressé a droit, s'il le demande, d'obtenir de l'administration communication des principales caractéristiques du traitement.

De prime abord, je me suis demandé quel pouvait être l'intérêt d'obtenir ces données dès lors que l'immense majorité de nos concitoyens n'a pas été formée pour comprendre les algorithmes. Mais finalement, il y a dans ce nouveau droit un présupposé que je trouve intéressant : pour être un citoyen maître de son destin, il faut avoir aujourd'hui de solides notions d'informatique, comme on doit savoir lire et écrire couramment (ce qui n'est hélas toujours pas le cas en France). Pour que le droit à l'algorithme soit effectif, il faut soi-même en comprendre les codes et les mécanismes informatiques.

B : il y a donc un devoir d'enseignement des algorithmes ?

Il est sain que les citoyens veuillent comprendre l'action administrative. Parmi les libertés publiques, il y a pour moi le droit de comprendre les décisions de l'administration qui vous concernent. Le droit de connaître l'algorithme, c'est une manière d'obliger l'administration à expliquer les raisons pour lesquelles elle vous oppose telle ou telle décision. Il est rare que des décisions s'appuient sur un seul critère (par exemple, le droit de vote repose sur un critère essentiel, il faut avoir l'âge de la majorité). La plupart du temps, les décisions individuelles sont multicritères. C'est là qu'intervient l'algorithme qui n'est autre qu'un processus informatique pour appliquer ces critères multiples en fonction des instructions données pour leur application.

S'il est un enseignement à tirer de la récente publication de l'algorithme de Parcoursup assorti d'explicitations parfaitement claires, précises et techniques, c'est que du coup personne n'a plus mis en question cet algorithme et ce qu'il signifie en termes de choix public.

Malgré tout, l'exigence croissante de transparence dans tous les domaines révèle une certaine méfiance vis-à-vis des détenteurs de l'autorité. Autrefois, aucun élève n'aurait eu l'idée de contester ses notes ou l'appréciation de son professeur. A présent, on veut non seulement comprendre, mais remettre en cause. Je ne porte aucun jugement sur cette évolution, qui est ce qu'elle est. D'une certaine façon, il est normal que la gestion de masse à laquelle est conduit un

État de 67 millions d'habitants comme la France ait pour contrepartie un certain éloignement du citoyen. Celui-ci cherche à le compenser en ayant davantage de prise sur les décisions qui le concernent et en se prémunissant contre un éventuel arbitraire administratif, ce qui est positif. Encore faut-il que notre société ne bascule pas dans la défiance entre citoyens, et vis-à-vis des institutions républicaines qui sont le ciment de la société.

B : que se passe-t-il dans le cas où les décisions sont prises par un logiciel ?

Bien avant l'entrée en vigueur du RGPD en mai dernier, il est un principe qu'a de longue date dégagé la CNIL, à savoir que les décisions administratives produisant des effets juridiques ne peuvent uniquement découler d'un traitement automatisé. Il faut une intervention humaine, encore que des exceptions soient maintenant prévues par la loi du 20 juin 2018 ayant modifié la loi informatique et libertés pour tenir compte du RGPD. Par ailleurs, est toujours ménagée la possibilité d'un recours devant une autorité ou un juge pour contester les fondements d'une décision prise sur la base d'un algorithme. C'est une avancée.

B : vous avez eu une carrière impressionnante. Auriez-vous des conseils en particulier pour les plus jeunes de nos lecteurs ?

Je dirais d'abord et avant tout aux jeunes en particulier qu'ils doivent avoir la curiosité du monde qui les entoure, avoir la soif d'apprendre. Aller à l'école, au collège, au lycée et à l'Université sont des privilèges dont sont privés beaucoup de jeunes à travers le monde. C'est en s'intéressant au monde, en apprenant sans cesse qu'on se construit et qu'on maîtrise du mieux possible sa vie. Je conseille fortement de lire et relire « Souvenirs et Solitude » de Jean Zay, l'un des plus grands ministres de l'Éducation nationale de la France.

Aujourd'hui, apprendre, cela veut dire acquérir des connaissances universelles, en informatique et en maths, autant qu'en relations internationales, histoire, littérature, en art.

Par ailleurs, force est de constater que nous vivons dans un monde où les idées toutes faites pullulent, et où via les réseaux sociaux, n'importe qui peut s'ériger en expert qu'il n'est pas, peut attaquer anonymement, et donc lâchement, n'importe qui pour lui nuire, peut organiser des boycotts contre n'importe quel pays ou n'importe quel organisme en propageant de fausses accusations ou rumeurs etc. C'est dangereux !

Là encore, pour maîtriser la quantité inépuisable d'informations que l'on reçoit de toutes parts, il faut avoir un niveau de conscience et de connaissances suffisant. L'esprit critique est un impératif catégorique dans la société actuelle. Il est l'antidote de l'intégrisme et du sectarisme, qu'il soit religieux ou politique, c'est-à-dire une condition essentielle de la liberté.

Enfin, il faut savoir écouter et ne pas s'enfermer dans des certitudes. J'ai eu des engagements politiques que je n'ai plus. Cependant, je n'ai jamais pensé que j'avais toujours raison contre mes contradicteurs. Bien-sûr, j'ai gardé de très fortes convictions ; ma vision de la société a évolué, mais pas mes principes. Et je n'ai pas l'intention de transiger sur mes valeurs, même si, lorsque je sens que mon interlocuteur est de bonne foi et connait son sujet, je suis prête à changer d'avis !

Entretien réalisé par Serge Abiteboul et Claire Mathieu

[1] Noëlle Lenoir a été présidente du Comité international de bioéthique de l'UNESCO de 1992 à 1999. Elle a ainsi été conduite à élaborer le premier instrument international sur le droit de la génétique — « La Déclaration universelle sur le génome humain et des droits de l'homme » — qui sera adopté en 1998 par l'Assemblée générale des Nations. En 1991, elle est également désignée par la Commission européenne, alors présidée par Jacques Delors, comme membre du Groupe européen d'éthique des sciences et des technologies nouvelles. Puis, en 1994, elle y est élue, puis réélue pour deux fois Présidente, par ses pairs. (Wikipédia 2018)

24 MAI 2018

Libertés numériques, ça va être votre fête !

Le numérique s'est installé dans nos vies ; les lecteurs de binaire l'ont bien compris. Il s'invite de plus en plus au parlement. En ce moment, citons entre autres :

⇒ La proposition de loi sur les « fake news ».
⇒ Le projet de loi Elan, évolution du logement, de l'aménagement et du numérique.
⇒ Le plan d'action pour la transformation des entreprises (des aspects sur leurs transformations numériques).
⇒ Le projet de loi relatif aux violences sexuelles et sexistes (cyberharcèlement).
⇒ Le projet de loi de programmation militaire (cyberattaques).
⇒ Le projet de loi de programmation et de réforme pour la justice (plusieurs volets sur le numérique).
⇒ Le projet de loi sur l'audiovisuel (volets numériques).

Parmi tous ces projets, le projet de loi RGPD va particulièrement transformer nos vies. Nous vous en avions déjà parlé lors d'un précédent billet, ce 25 mai marquera une étape importante au niveau législatif dans l'ensemble de l'union européenne. Le **règlement général sur la protection des données** (**RGPD**) entre officiellement en vigueur. Ce texte de référence européen renforce et unifie la protection des données pour les individus.

Depuis plusieurs mois, le web regorge d'articles sur le sujet. Sur les réseaux sociaux, le hashtag #RGPD affiche complet. Tous les sites web qui collectent ou utilisent nos données sont contraints de se mettre en conformité avec le nouveau cadre légal et nous inondent de messages en ce sens.

Parmi toutes les ressources existantes, nous vous conseillons d'aller visionner cette petite vidéo réalisée par le youtubeur Samson Son – alias *Cookie Connecté* qui nous explique en 6 minutes et en Emoji le RGPD. Elle permet de comprendre ce qui change vraiment pour nous aujourd'hui.

GDPR / RGPD expliqué en emojis

Et une autre vidéo du même auteur a été réalisée en partenariat avec la CNIL qui s'adresse principalement aux professionnels. Si vous n'avez pas encore mis en application ce règlement, il est grand temps !

RGPD / GDPR : FAQ avec la CNIL

Pour célébrer cette journée particulière, nous vous donnons rendez-vous pour faire la fête des libertés numériques lors d'événements organisés dans toute la France.

Marie-Agnès Enard et **Serge Abiteboul**

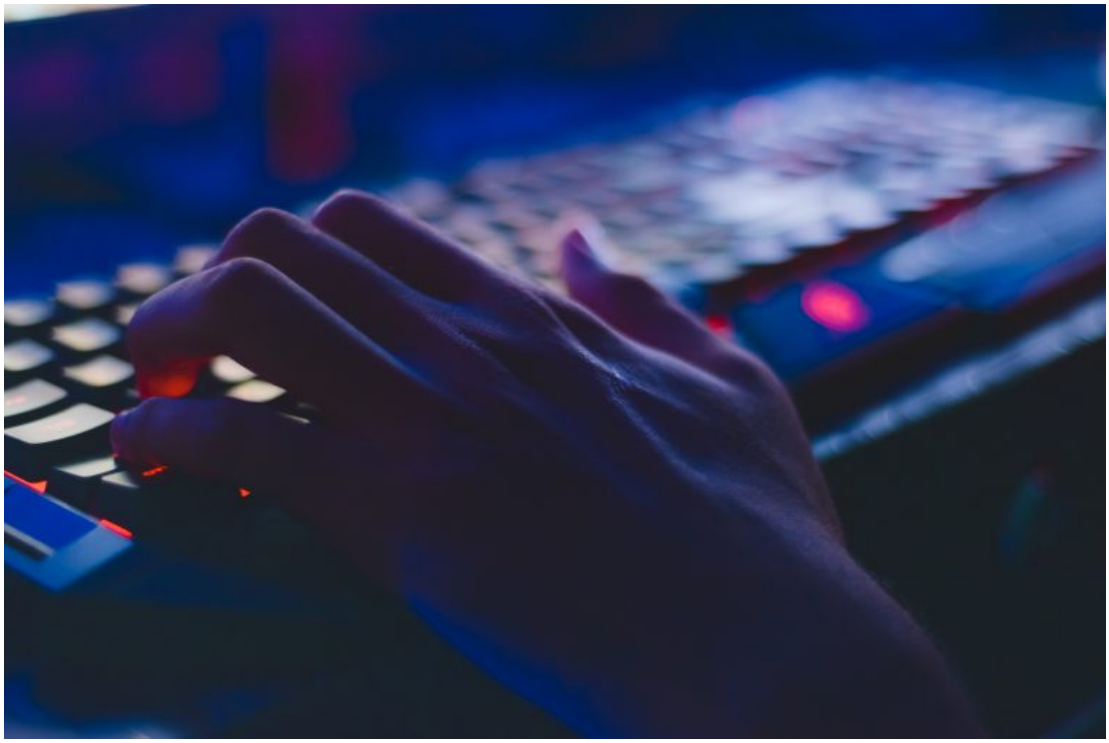
18 MAI 2018

Code et droit : le mariage du siècle

Les rapports entre le code informatique et le droit sont intimes. Le code n'est pas là pour se substituer au droit, mais pour en faciliter l'application. Une spécialiste du droit du numérique, Lêmy Godefroy, explore pour Binaire ces interactions. ***Serge Abiteboul****.*
Ce texte est basé sur un article paru dans la revue juridique Dalloz N°14, 12 avril 2018, p.734

Lawrence Lessig déclare que « le code [informatique] régule. (…) Il implémente des valeurs ou pas. Il permet les libertés ou les désactive. Il protège la vie privée ou favorise la surveillance » (1). Or, des atteintes aux droits risquent de se multiplier si les codeurs s'accaparent le pouvoir de « choisir nos valeurs pour nous » et imposent leurs normes pour privilégier leurs intérêts particuliers. Le code entre alors en opposition avec le Droit. En revanche, si le code régule en accord avec le Droit, il s'y réfère et peut le servir dans le sens d'une meilleure effectivité et efficacité.

Code versus Droit



Le code s'affranchit du Droit : des affaires semblables à celle de Cambridge Analytica révélant des failles dans la protection par Facebook des données personnelles de ses utilisateurs sont susceptibles de se répéter dès lors que le code engendre des normes hors du Droit. Pour éviter ces dérives, il importe que le Droit s'empare davantage du code.

Cela passe, notamment, par la détermination de valeurs éthiques juridiquement garanties. (Voir le rapport récent de Cédric Villani.) Ces valeurs s'agrègent autour d'une exigence de transparence afférente à la logique du code. Cette explicabilité est techniquement envisageable pour le code dont le fonctionnement a été programmé *ab initio*. Il en va différemment pour le code qui se construit par application de procédés d'apprentissage. Le cheminement menant des intrants aux sortants est souvent opaque.

Les codeurs sont également tenus de veiller à la protection de la vie privée. Le règlement général sur la protection des données (RGPD) du 27 avril 2016, applicable à compter du 25 mai 2018, met l'accent sur la prévention des répercussions potentiellement dommageables du traitement massif de données. Outre les obligations déjà prescrites par les textes antérieurs (consentement à la collecte, mention de l'identité du responsable du traitement, de la finalité du traitement, des droits dont disposent les individus, etc.), le RGPD entérine les règles de la *privacy by design* et de la *privacy by default* (2). Au regard de ces impératifs techniques et organisationnels relatifs à la conception du code, le responsable du traitement devra vérifier que les opérations auxquelles il se livre sur les données préservent suffisamment les droits et libertés individuelles et enclencher éventuellement les actions nécessaires. Par exemple, un traitement engendrant des risques élevés pour la vie privée implique la réalisation d'une analyse d'impact destinée à spécifier des mesures de gestion de ces risques.

Enfin, la violation du Droit par le code doit conduire à engager la responsabilité de son auteur (3). Il convient de définir les régimes juridiques appropriés pour pallier les difficultés à tracer la chaîne des causalités, faciliter la désignation du débiteur de l'obligation de réparation et éviter une dilution des responsabilités.

L'appréhension juridique du code est donc essentielle à son acceptation par ceux qui auraient à en subir le retentissement au quotidien (usagers des services publics, consommateurs, patients, justiciables, etc.). Il incombe aux autorités publiques d'éprouver la conformité du code au Droit. Un organe de contrôle mènerait périodiquement des audits afin de tester le code et de pointer les biais de programmation comme une discrimination salariale, un refus injustifié de prêt bancaire ou une pratique anticoncurrentielle. Des signalements seraient transmis par les utilisateurs du code (plateformes numériques, professionnels de santé, administration, professionnels du droit et de la justice, etc.) et par les usagers (consommateurs, patients, administrés, justiciables, etc.).

A ces conditions, le code pourrait alors servir le Droit, ce que nous allons voir ci-après.

Code cf. Droit

Le code se réfère au Droit : réplique informatique du Droit, il apparaît comme un nouveau mode d'expression de la régulation juridique avec, en ligne de mire, un renforcement de l'efficacité et de l'effectivité du Droit grâce à une automatisation de son application. Dans cette tâche programmée, le code observe le Droit.

C'est de cette manière que peut être lu le code du *smart contract*. Un *smart contract* (en français, « contrat intelligent ») est un protocole informatique qui facilite, vérifie et exécute la négociation ou l'exécution d'un contrat, « Rattaché aux effets du contrat, [son code] se présente comme un modalité d'exécution » (4). Pour ce faire, il traduit le Droit en instructions conditionnelles. Par exemple, il serait paramétré pour que, passé une certaine durée précisée par les cocontractants, si le débiteur n'a pas démontré l'existence d'un cas de force majeure, la sanction convenue en cas d'inexécution s'applique. De même, le code contiendrait l'instruction selon laquelle s'il y a un manquement suffisamment grave – par exemple le non-paiement du loyer d'un contrat de location d'un matériel connecté – le créancier sera dégagé de sa propre obligation – en l'occurrence la mise à disposition du bien loué en le bloquant physiquement.

Associé à une blockchain, il provoque une action qui affecte la situation factuelle à chaque saisie d'informations enregistrées par l'Oracle (5). Par exemple, dans le secteur de l'assurance, « des systèmes de Blockchain permettraient de valider des conditions de déclenchement de primes et de les régler sans délai. À titre d'illustration, il pourrait être proposé de prévoir une indemnité automatique des assurés dès qu'ils seraient victimes d'un retard de train ou d'avion et ce sans formulaire et sans que du personnel de l'assureur ne doive traiter les demandes » (6). Dans tous les cas, le code laisse aux parties la faculté d'en appeler au juge qui demeure l'émanation du tiers de confiance étatique.

Il en est de même du code qui concrétise la reconnaissance judiciaire de droits en produisant un chiffrage des indemnités ou des dommages-intérêts. Par exemple, dans le cadre de la procédure de divorce, l'outil « PilotePC » est une méthode d'analyse multicritères de calcul de la prestation compensatoire qui retranscrit les critères légaux en code (7).

En définitive, le code régule mais il revient aux autorités publiques – en concertation avec l'ensemble des parties prenantes (concepteurs, utilisateurs, usagers) – de gouverner cette régulation pour que le code œuvre ainsi au service du Droit et participe à la préservation efficace et effective des droits.

Lêmy Godefroy, Maître de conférences, Université Côte d'Azur

Pour aller plus loin

1 Code is law. On liberty in cyberspace, Harvard Magazine, janvier 2000.
2 Célia Zolinski, Philippe Pucheral, Alain Rallet et Fabrice Rochelandet, « La Privacy by Design : une fausse bonne solution aux problèmes de protection des données personnelles ? », Légipresse, n° 340, juillet-août 2016).
3 Serge Abiteboul, Gilles Dowek, Le temps des algorithmes, Le Pommier, 2017, p. 8. Adde p. 177 et s.
4 Gaëtan Guerlin, « Considérations sur les smart contracts », Dalloz IP/IT 2017, 512).
5 V. Mustapha Mekki, « Les mystères de la blockchain », D. 2017, 2160.
6 Yaël Cohen-Hadria, « Blockchain : révolution ou évolution ? », Dalloz IP/IT 2016,

26 AVRIL 2018

La justice prédictive et l'égalité devant la loi

Un nouvel « Entretien autour de l'informatique », celui de Louis Boré qui est président de l'ordre des avocats au Conseil d'État et à la Cour de cassation. L'informatique transforme profondément la justice. Serge Abiteboul et Claire Mathieu l'interrogent pour Binaire sur la justice prédictive. Cet article est publié en collaboration avec TheConversation.

Louis Boré, photo personnelle

B : Vous êtes président de l'ordre des avocats au Conseil d'état et à la Cour de cassation. Pouvez-vous nous expliquer en quoi cela consiste ?

LB : Je suis effectivement avocat au Conseil d'État et à la Cour de cassation : le Conseil D'État est notre cour suprême administrative, et la Cour de cassation, notre cour suprême judiciaire. Ce

sont des juridictions qui ont pour mission d'unifier l'interprétation des règles de droit sur toute l'étendue du territoire de la République. Elles ont pour point commun de tendre vers cet objectif avec une technique spécifique qu'on appelle la technique de cassation. On ne juge que les questions de droit, pas les questions de fait qui sont tranchées antérieurement et doivent être considérées comme des éléments définitivement acquis aux débats.

Comme nous plaidons presque exclusivement devant ces deux juridictions et pratiquons quotidiennement cette technique particulière, nous avons une vision du droit un peu différente de celle d'un avocat à la Cour d'appel. Lui fait corps avec son client. Nous, nous devons passer sans arrêt du particulier au général, c'est-à-dire voir si dans la situation individuelle qui nous est soumise, il est possible de déceler une erreur de droit qui a forcément une dimension plus large puisque la règle de droit est toujours générale et impersonnelle.

Quand on trouve un moyen de cassation, on le soutient. Est-ce qu'on est chicanier ? Non, ce n'est pas de la chicane, mais la défense de l'article 6 de la Déclaration des Droits de l'Homme et du citoyen : la loi doit être la même pour tous, soit qu'elle protège, soit qu'elle punisse. Pour cela, elle doit être interprétée de la même manière partout, sinon cela signifierait que l'on en revient aux coutumes régionales de l'ancien régime. Cela signifierait qu'on abandonne le principe d'égalité devant la loi qui est un principe républicain essentiel.

Il est certain que ce travail particulier influence ma vision de la justice prédictive.

B : Tout ce qui va dans le sens de coder la loi de façon algorithmique, de préciser la loi, vous intéresse ?

LB : Exactement, c'est pour cela que la justice prédictive m'intéresse. Les avocats à la Cour craignent un rouleau compresseur qui va empêcher le juge de faire du sur-mesure, en imposant du prêt-à-porter à la place. Ils se battent pour que le juge se livre à une appréciation humaine, et donc pour eux tout ce qui égalise porte atteinte à cette appréciation au cas par cas. Pour ma part, j'y suis moins hostile, car je pense qu'au-delà de chaque cas particulier, il y a une règle générale qui est en cause.

Ainsi, en matière pénale, pour l'appréciation de la peine, la loi ne fait que fixer un maximum, et c'est le juge qui apprécie, selon les circonstances : le prévenu peut être jeune ou âgé, l'un manifeste un repentir mais pas l'autre… Le juge doit tenir compte de la situation spécifique du prévenu pour déterminer la sanction. Mais pour savoir si l'infraction est constituée ou pas, on n'est plus vraiment dans une appréciation au cas par cas, et là, la cohérence entre ce qui est jugé à Paris et à Bordeaux me semble essentielle. Si demain on est capable de mettre en place des instruments facilitant le travail des juges et des avocats pour appliquer la loi de façon plus cohérente et plus uniforme sur l'ensemble du territoire national, ce sera un progrès.

L'imprécision des lois : une porte ouverte à l'imagination humaine

B : Y a-t-il une tension au sujet de l'attitude du juge, avec d'un côté le désir d'avoir une justice plus humaine et plus empathique, et de l'autre côté le risque d'avoir une justice plus biaisée parce que le juge fait ce qu'il veut ?

LB : La tension existe entre le droit et l'équité. La base du droit, ce sont des règles générales. S'il n'y a pas de généralité, il n'y a pas de droit et il suffit alors d'un juge sous un chêne qui apprécie au cas par cas, sans être contraint par des règles. Mais la règle juridique implique, dans une certaine mesure, la généralité. L'équité, au contraire, c'est le cas par cas, car aucune personne n'est absolument identique à une autre. Mais l'équité pure est extrêmement dangereuse. Il existe un vieil adage de la révolution française, « Dieu nous garde de l'équité des parlements ! », signifiant que les décisions des parlements étaient totalement imprévisibles, ce qui créait une insécurité juridique considérable. C'est contre cela que la révolution française a voulu réagir. Mais, dans la généralité de la règle, il y a aussi une dimension totalitaire. Elle peut aboutir à des décisions injustes parce que trop rigides, trop mécaniques, et donc, inhumaines.

Alors, quel est le rôle du juge ? Il est, selon le doyen Ripert, « le législateur des cas particuliers » : il s'agit d'adapter sans la trahir la règle générale. Entre la règle générale et le cas particulier, il subsiste toujours une marge de manœuvre, une part de souplesse, qui permet au juge d'adapter la règle aux situations particulières, et c'est une très bonne chose.

Et puis l'avocat peut faire preuve d'imagination juridique. Il peut plaider une interprétation totalement nouvelle des textes. Si un juge est convaincu, il transformera cette proposition en jurisprudence. De fait, l'imagination juridique aura déjoué la répétition mécanique de la règle et aura fait avancer le droit. Cela fait partie du travail des magistrats et des avocats.

© Itai Benjamini

B : La loi est bien trop imprécise. Si elle était plus formalisée, il serait plus facile de donner des réponses précises et cela simplifierait le travail des algorithmes. Est-ce que ce serait mieux que la loi soit plus précise ?

LB : Le degré de précision de la loi est une question juridique. Constitutionnellement, la loi ne doit pas être trop précise. Ce sont ultérieurement les décrets et arrêtés pris pour son application qui vont en préciser le sens. Il y a une structure hiérarchique : la constitution, les lois, les décrets, les arrêtés. C'est une structure pyramidale. Ainsi, la loi n'a pas forcément vocation à être précise. En France, il y a pléthore de textes ; on a tendance à en avoir dans tous les sens. Mais en cherchant à être trop précis, on en devient incompréhensible.

L'imprécision d'une loi peut avoir des avantages. Par exemple la loi disant que « tout fait quelconque de l'homme qui cause à autrui un dommage oblige celui par la faute duquel il est arrivé à le réparer » donne les trois éléments de la responsabilité civile. L'imprécision du texte a laissé une capacité créatrice et d'adaptation au juge. Le prix à payer est un certain aléa judiciaire que pourront en partie compenser les algorithmes prédictifs.

La justice au quotidien avec les machines

B : L'avocat se sent-il dépossédé par les machines ?

LB : C'est vrai qu'il y a une véritable inquiétude dans la profession et la majorité voit cela comme une menace considérable. Ils se sentent menacés par le risque d'être remplacés par des machines. Une minorité voit cela, au contraire, comme une opportunité.

Il est certain que la justice prédictive va remplacer ce qui est mécanisable dans l'exercice de la profession juridique, et il y a effectivement certaines choses répétitives dans notre travail. Par exemple, la gestion des infractions telles que les excès de vitesse est de plus en plus remplacée par des décisions automatisées.

Il y a une très vieille tradition dans l'Ordre que je préside, c'est celle de la consultation préalable avant de saisir le Conseil d'État et la Cour de cassation. Sous l'ancien régime, il fallait deux consultations préalables. Maintenant, ce n'est plus obligatoire, mais beaucoup de justiciables nous consultent encore avant de saisir ces deux hautes juridictions. Ils nous contactent soit directement, soit par l'intermédiaire de leur avocat à la cour. Ils souhaitent mieux apprécier leurs chances de succès. Nous ne donnons pas un pourcentage précis mais une appréciation.

Mon expérience de « justicier prédictif » me conduit à constater que certains justiciables, quand on leur dit que leurs chances de gagner sont très faibles, veulent quand même y aller. Mais il y en a aussi beaucoup d'autres, les plaideurs institutionnels en particulier, qui ne veulent y aller qu'avec des chances assez fortes. Les logiciels de justice prédictive ne feront qu'étendre cela à tous les avocats. Cela aidera mes confrères à la cour à exercer plus facilement leur devoir de conseil pour dire si cela vaut, ou non, la peine de saisir le juge. Cela ne tuera pas le métier car le devoir de conseil fait partie des devoirs des avocats. Un logiciel qui aidera à exercer cette obligation professionnelle constituera donc un progrès.

B : Quand on met des algorithmes dans le système juridique, aujourd'hui ce sont des algorithmes relativement simples, qui n'ont pas la capacité de raisonnement d'un juge, et donc de manière presque automatique ils vont plutôt se situer du côté de la règle juridique. Cela vous semble-t-il un risque ?

LB : Non, cela me paraît un progrès, car cet effort d'uniformisation, c'est nous qui le faisons nous-mêmes actuellement, en allant sur le site de Légifrance. Nous mettons des mots-clés pour avoir accès, grâce à un logiciel, à des cas précis, dix ou quinze décisions de la Cour de cassation ou du Conseil d'état sur des sujets similaires à notre affaire et ensuite, nous analysons nous-mêmes les décisions et nous faisons le travail d'abstraction pour déduire de ces éléments la règle générale.

Les logiciels pourront sans doute nous aider à effectuer ce travail d'analyse, mais nous aurons toujours un pouvoir et un devoir de contrôle sur le résultat qu'ils ne feront que nous proposer. Et actuellement, ils sont encore très loin de parvenir à un résultat fiable et utile.

B : Mais si un logiciel dit au juge : « cette personne va récidiver », comment le juge peut-il se sentir capable d'aller contre cet avis et de libérer la personne ?

LB : Il est vrai que cela crée une pression considérable sur le juge. Mais là, la machine ne définit pas de règle de droit. Il n'y a pas de règle de droit pour la libération conditionnelle. Il y a un minimum incompressible d'exécution de la peine, mais une fois cette date passée, la loi donne quelques critères généraux extrêmement souples et vagues, et laisse le reste à l'appréciation du juge. Ce que la machine va faire, ce sera de la prédiction, un travail sociologique plus que juridique, une sorte de version numérique du criminologue Lombroso (*).

B : Et si l'algorithme prédictif donne une probabilité de récidive, après étude de données massives, mais sans expliquer sa prédiction ?

LB : De toute façon tout cela n'est envisageable qu'après un contrôle de l'État. Les juges ne peuvent pas s'emparer de ces outils sans un organe de contrôle, le Ministère de la justice ou la Chancellerie, un organe central qui ira voir l'informaticien et lui demandera les critères utilisés.

B : À quel point est-il important que le résultat du programme soit accompagné d'une explication ?

LB : Il faut une transparence de l'algorithme. L'autorité de contrôle doit comprendre comment le programme fonctionne. Si l'algorithme utilisait des critères prohibés tels que la race, le sexe, ou la religion par exemple, ce serait illégal. De ce point de vue, les pays anglo-saxons sont essentiellement utilitaristes. Notre société n'est pas ainsi. Nous restons attachés à des principes non négociables, et on refusera des algorithmes, même très efficaces, s'ils utilisent des critères prohibés. Les principes, ce sont les racines, c'est la sève, et le résultat, c'est le fruit. Il y a des racines constitutionnelles à notre droit, et à partir de celle-ci on essaiera d'être les plus efficaces possibles. Un projet de société où il n'y aurait plus aucun crime est utopique et totalitaire.

De plus, avant de condamner quelqu'un, le juge voudra vérifier que la machine n'a pas raconté n'importe quoi, et voudra donc regarder l'interprétation livrée par la machine. L'acte en cause, mettre ou non quelqu'un en prison, est un acte grave et un juge ne peut le déléguer à une machine.

Je dois pouvoir regarder dans les yeux celle ou celui qui m'envoie en prison.

B : Même si mon ordinateur-juge fait moins d'erreurs, est moins souvent contredit par les cours supérieures, et envoie moins souvent des innocents en prison, vous continuez à dire que pour des questions de principe la justice doit quand même rester sous le contrôle du juge ?

LB : Je ne vois pas les humains confier totalement leur destin à des machines. Je ne vois pas les français confier la décision d'envoyer quelqu'un en prison à une machine. Si cela devait arriver, j'y serais profondément hostile. Pour accepter que quelqu'un m'envoie en prison, j'ai besoin de le regarder dans les yeux. C'est parce que c'est mon semblable qu'il a le droit de me sanctionner. Une machine n'a pas ce droit. D'une manière curieuse, ce qui rend acceptable la sanction pénale, c'est que le juge peut être lui aussi puni s'il commet une infraction. Le juge et l'assassin sont tous les deux des êtres humains. Comme tu es mon frère, tu as le droit de me juger, de me dire que ce que j'ai fait est horrible et mérite la prison. La machine n'est pas mon frère et ne peut pas me juger car elle est incapable de faire ce que j'ai fait

Propos recueillis par **Serge Abiteboul** et **Claire Mathieu**

(*) Marco Ezechia Lombroso, dit Cesare Lombroso (1835-1909), est un professeur italien de médecine légale et l'un des fondateurs de l'École italienne de criminologie. Il est célèbre pour ses thèses sur le « criminel né » : à partir d'études phrénologiques et physiognomoniques, il tentait de repérer les criminels en considérant qu'il s'agissait d'une classe héréditaire qu'on pourrait distinguer par l'apparence physique. *Wikipédia 2018. (*Note des interviewers : Louis Boré est ici ironique ; le reste de son discours laisse penser qu'il voit les prédications des algorithmes plus scientifiques que les thèses de Lombroso.)