Convergences du Droit et du Numérique

François Pellegrini

Convergences
du droit et du numérique

Actes des ateliers de préfiguration

8 – 10 février 2017

Colloque organisé avec le soutien du GIP Mission de recherche Droit et Justice.
En association avec le débat public sur les enjeux éthiques des algorithmes lancé par la CNIL.

Pourquoi des « Convergences du droit et du numérique » ?

En consacrant son étude annuelle de 2014 au thème « numérique et droits fondamentaux », le Conseil d'État avait engagé une vaste réflexion sur des questions complexes jusque-là assez inédites. Dans une société dont tous les champs sont désormais investis par le développement du numérique, il s'agit de prendre l'exacte mesure d'une mutation radicale – de type systémique – qui n'affecte pas seulement le contenu des droits fondamentaux, mais qui oblige à tout repenser : le régime juridique applicable à ces droits, afin d'en assurer la reconnaissance éventuelle lorsque des droits nouveaux émergent, et leur protection effective, lorsque les droits existants sont menacés. Mais cette mutation impose aussi de réinventer la réponse juridique elle-même qui doit pouvoir emprunter d'autres voies que celles de règles rigides, qui peuvent n'être pas suffisamment adaptées au rythme des innovations que le numérique porte et nous impose. Nous sommes en présence d'une révolution agissant sur nos modes de vie, nos comportements, notre univers de communication : le droit doit impérativement être revisité s'il entend toujours réguler les rapports sociaux.

Les pistes de réflexion qu'avait alors dégagées le Conseil d'État s'inscrivaient déjà dans la nécessité de rechercher des formes de convergences : de même que le droit devait éviter, par l'édiction de normes excessives, de faire peser sur le développement du numérique des contraintes aussi inhibitrices qu'inutiles, il était attendu du numérique qu'il se mette au service des droits individuels et de l'intérêt général. Ainsi, le Conseil d'État proposait-il, par exemple, de définir les obligations des plateformes envers les utilisateurs au regard du principe de loyauté, ou de rééquilibrer la gouvernance de l'Internet afin de mieux y faire valoir les intérêts généraux que la société entend protéger.

Le colloque « Convergences du droit et du numérique » se propose de poursuivre cette réflexion, en lui donnant un prolongement original et inédit. Non seulement la communauté des juristes et les acteurs du numérique sont invités à dialoguer ensemble, mais ils sont encouragés à le faire en se remplaçant mutuellement : les juristes parleront informatique, cependant que les informaticiens parleront de droit. Déjà, les ateliers préparatoires qui se sont tenus les 8, 9 et 10 février sur les thématiques « Algorithmes et autonomie » et « Numérique et pratique juridiques » ont rendu possible ce partage des savoirs, cette mise en commun des expériences. Il est attendu du prochain colloque qui se tiendra à Bordeaux des 11 au 13 septembre qu'il franchisse une étape supplémentaire dans le partage entre la communauté des juristes et des acteurs du numérique : à la première, je dirai « appropriez-vous le numérique pour repenser le droit », aux seconds « apprivoisez le droit pour faire avancer le numérique » ! ,

Anne Guérin

Conseiller d'État,
Présidente de la cour administrative d'appel de Bordeaux

Présentation

La « révolution numérique », provoquée par la diffusion massive des technologies numériques au sein de la société, bouleverse tant les modèles organisationnels et économiques que les catégories juridiques. De ce constat découle la nécessité de faire collaborer juristes et acteurs du numérique, en suscitant une réflexion commune sur l'évolution du droit et l'encadrement des pratiques informatiques à l'aune de la révolution numérique.

C'est dans cet objectif que l'université de Bordeaux s'est investie dans la création d'un événement dédié à favoriser cette collaboration. Pour autant, cet événement ne peut prendre une forme traditionnelle ; ce serait nier le bouleversement de la pensée et des modes d'action induits par la révolution numérique. Le format proposé est donc celui d'un événement co-construit en mode collaboratif, destiné à créer des ponts durables entre les communautés juridique et numérique, de façon récurrente.

L'objet numérique que vous tenez entre vos mains est donc original à plusieurs égards, car issu d'un processus itératif, agile et collaboratif.

C'est sur la base des contributions reçues, sans restriction de sujet, qu'ont été dégagés les quatre thèmes des ateliers, qui font émerger les questionnements actuels sur l'informatique : les données et les traitements qui les manipulent. Les ateliers ont été l'occasion pour les participants de présenter leurs sujets de recherche et d'interrogations, en « *speed dating* » de 10 minutes, afin de laisser une grande place aux échanges et interactions. Les synthèses ont été rédigées collectivement, en utilisant un « *pad* », afin que tou/te/s puissent apporter leur contribution, y compris les participant/e/s en visio-conférence. Ces échanges ont permis d'entamer la constitution des binômes de travail, en préparation des interventions au colloque des 11 au 13 septembre prochains.

Ce document doit donc être considéré comme le témoin d'une étape ; celle des prémisses de la construction d'une communauté trans-disciplinaire active et en phase avec l'évolution rapide des techniques et de la société.

François Pellegrini

Vice-président délégué au numérique, université de Bordeaux

Table des matières

Thème A : « Algorithmes et loyauté »

Synthèse p. 8

Pour un droit de l'algorithme p. 11
Céline Teyssier

Comment vérifier les résultats du vote par Internet ? p. 15
Tatiana Shulga-Morskaya

Systèmes inéquitables numériques p. 21
Chantal Enguehard

Transparence des algorithmes : quelles réponses juridiques et techniques ? p. 24
Daniel Le Métayer

The DAO : « code is law » of the jungle ? p. 26
François-Vivien Guiot

Bitcoin et Blockchains : réflexions terminologiques et identitaires p. 29
Adli Takkal-Bataille

Bitcoin, Blockchains et monnaies numériques décentralisées : de l'étude de la technologie et des cas d'usage à l'élaboration d'un cadre juridique adapté p. 31
Benoît Huguet

Les transports intelligents p. 34
Sébastien Martin

La mutation des opérateurs réseaux en fournisseurs de cloud : quels enjeux pour la neutralité du net ? p. 36
Nicolas Herbaut

Thème B : « Systèmes autonomes et décision, droits fondamentaux »

Synthèse p. 38

La robotique autonome face au droit et à l'éthique p. 41
Nathalie Nevejans

Droit + numérique + x = droit des robots. Inventer les inconnues p. 43
Pierre-François Euphrasie

Drones et robots autonomes ou télé-opérés en environnement complexe : tenue de situation, prise de décision, responsabilité et éthique p. 45
Serge Chaumette

Implications juridiques de l'émergence des armements autonomes et semi-autonomes p. 51
Julien Ancelin

Sens et implications des systèmes experts d'aide à la décision (en matières médicale et judiciaire) p. 53
Sonia Desmoulin-Canselier

Quelles limites juridiques aux algorithmes prédictifs ? p. 56
Rose-Marie Borges

Les faces cachées du numérique et de la nouvelle technologie p. 58
Lamia El Bouchtioui

Le contrôle de l'homme par les réseaux sociaux p. 62
Rym Fassi Fihri

Thème C : « Numérique et pratiques juridiques »

Synthèse p. 64

Les professions du droit et la révolution numérique p. 68
Constance Caillaud-Renaud

Les enjeux de l'e-justice en matière pénale p. 71
Aminata Touré

L'informatisation du travail juridique p. 73
Sébastien Platon

Projet d'outil contractuel pour les contrats de services p. 81
Manuel Munier & Xavier Daverat

Projet de qualification juridique des différents types de données p. 83
Manuel Munier & Rose-Marie Borges & Christine Lassalas

Traitement automatique des langues, données légales, système d'information, logique p. 85
Annie Forêt

La constitution de bases de données par la doctrine juridique p. 88
Alex Chauvet

Open data et droit : quelles incidences sur l'administration publique du développement durable ? p. 90
Julien Vieira

Infractions et numérique – quelles réponses du droit pénal ? p. 92
Élisa Baron

Crimes, violences et justice parallèle dans le cyberespace p. 94
Hébert-Marc Gustave

Le méga fichier TES ou la surveillance massive des Français p. 97
Ousmane Gueye

Circulation transnationale et interception des données sur Internet au service des activités de renseignement p. 101
Maxime Kheloufi

L'influence de l'intelligence artificielle sur les métiers de droit p. 102
Florian Laussucq

Les enjeux de l'utilisation de la visioconférence dans le procès pénal p. 112
Anaïs Danet

Thème D : « Droit des données à caractère personnel »

Synthèse p. 114

Moins de 18 mois pour se préparer au Règlement européen sur la protection des données personnelles p. 117
Sarah Cadiot

Comment mesurer l'effectivité du Règlement général de la protection des données personnelles ? p. 120

Olivia Tambou

La sécurité des données à caractère personnel : de l'utopie à la réalité. Approche juridique p. 123

Sophie Gambardella

Anonymisation et droit à la privacy dans le contexte de l'Internet des objets (IdO) p. 127

Valeria Loscri

Géolocalisation et IA p. 128

Linda Arcelin

Télémédecine et sécurité des données de santé p. 130

Pauline Nicolas

Internet des objets et captation de la voix : quelle protection pour une donnée pas comme les autres ? p. 131

Charly Lacour

Traitement automatique de la parole : quelle écoute pour nos systèmes ? p. 133

Félicien Vallet

« Big data » et biens communs p. 135

Christine Lassalas

Thème A

« Algorithmes et loyauté »

Synthèse

Les discussions de ce thème ont porté sur les points suivants :

1. Que signifie la loyauté ?
2. Question de la preuve ;
3. Autonomie de l'usager.

Que signifie la loyauté ?

Les termes d'« algorithme » et de « loyauté » pouvant avoir des sens différents au sein des communautés juridique et informatique, il convient en premier lieu d'en proposer des définitions communes.

Un algorithme est la formulation abstraite d'un traitement informatique. Ce dernier est ensuite exprimé (ou « codé ») sous forme d'un programme (aussi appelé « logiciel », ou « application »), qui sera mis en œuvre sur un système informatique et dans un environnement particulier.

La loyauté est un concept interactionnel faisant intervenir un rapport de confiance entre un fournisseur et un bénéficiaire, dans le cadre d'une relation contractuelle établie et des attentes qui sont formulées dans ce cadre. On l'entend très souvent comme la bonne foi, mais elle ne lui est pas réductible ; elle englobe d'autres notions, telles que la bonne exécution du contrat, le devoir d'information, la théorie de l'imprévision, ou le respect des droits des personnes concernées.

Un algorithme conçu par des personnes est souvent codé par d'autres, puis encore mis en œuvre par d'autres, et utilisé par des personnes encore différentes. Chacun de ces acteurs a ses propres attentes, dont la plupart ne sont pas formalisées. En l'absence de règles de droit ou de système normatif, il faut donc se conformer à une acception générale. La loyauté n'est pas une caractéristique intrinsèque des algorithmes. En revanche, l'éthique de la conception des algorithmes et de leur mise en œuvre pourrait être interrogée, en particulier en ce qui concerne les attentes légitimes des parties.

En revanche, la notion de transparence peut être convoquée dans le cas d'algorithmes en mesure de diagnostiquer et d'énoncer leurs échecs et erreurs, d'expliquer leur fonctionnement et permettant l'exercice du contentieux à armes égales. La transparence justifie alors la mise en place de dispositifs techniques (rétro-ingénierie et décompilation des logiciels), normatifs (normes ISO, CEN, etc.) et/ou juridiques (validité de la décision, responsabilité, sanction) en vue de garantir qu'un algorithme est mis en œuvre, au sein d'un traitement, d'une façon loyale mais aussi éthique, légale, respectueuse des droits fondamentaux, des libertés individuelles et de l'intérêt général. De ce point de vue, il est nécessaire que les finalités d'un traitement algorithmique puissent être énoncées *a priori*, afin de pouvoir évaluer *a posteriori* si ces finalités sont atteintes. Dans le contexte de la robotique, la recommandation européenne 2015/2103(INL) insiste sur le fait qu'il doit toujours être possible de fournir la justification rationnelle de toute

décision susceptible d'avoir une incidence importante sur la vie des personnes. Ainsi la notion de transparence est-elle liée à celle de la compréhension par l'usager.

Les communautés juridique et informatique doivent réinterroger collectivement les définitions et acceptions des termes juridiques existants liés à la notion de loyauté (« concurrence déloyale », « prise d'intérêt », etc.), afin de les confronter aux pratiques numériques.

Question de la preuve

Comment le droit est-il à même de traiter les informations issues de logiciels ? Ces questions ont également été abordées dans le thème C de l'atelier, « Numérique et pratiques juridiques ».

À la différence de l'informatique, le droit permet le débat contradictoire et la contestation. *A contrario*, les traitements informatiques étant généralement associés (à tort) aux notions d'exactitude et de neutralité, la possibilité d'en contester les résultats est peu envisagée. Si des experts peuvent tenter d'analyser le fonctionnement d'un dispositif dans les cas les plus évidents de dysfonctionnements, le caractère fugace des informations numériques rend quasiment impossible la collecte *a posteriori* d'éléments dès lors que ceux-ci ont été supprimés du système. Or, pour des raisons d'efficacité, les logiciels sont conçus de façon à supprimer les informations dès qu'elles ne sont plus nécessaires, sauf obligations légales.

En droit français, le témoignage est le fait de personnes juridiques. Le témoin répond de son acte ; il peut être poursuivi et condamné en cas de faux témoignage car cet acte a des conséquences pour les parties au procès. L'enregistrement d'une opération dans une base de données ou dans un circuit informationnel tel qu'une *blockchain* ne peut donc être juridiquement qualifié de témoignage, mais seulement d'élément de preuve à disposition des personnes.

L'informatique est la science du traitement de l'information, celle-ci constituant la matière manipulée par les programmes. Une rupture d'égalité entre les parties peut donc intervenir dans l'absence de partage des données ou la difficulté d'accès aux données manipulées ou produites par une application. C'est le cas par exemple des traces d'exécution non accessibles aux utilisateurs. Ces derniers sont donc défavorisés en cas de contentieux car ils sont privés des informations dont dispose leur adversaire, ou doivent supporter des coûts élevés pour les obtenir. Il convient donc de réfléchir aux moyens juridiques et techniques permettant de symétriser l'accès à l'information, à l'image du principe d'égalité en droit administratif. Ainsi, la loi « République numérique » inclut-elle des dispositions concernant l'obligation de description des traitements mis en œuvre par les administrations. Cette avancée, qui pourrait être étendue aux traitements mis en œuvre par les acteurs privés, n'est cependant pas suffisante pour rééquilibrer les forces en présence. En effet, la description des traitements constitue une image de « ce qui devrait être » (la spécification) mais pas de « ce qui est » (la mise en œuvre et l'exécution), et ne compense donc pas l'absence d'accès aux traces d'exécution, qui peut s'avérer indispensable en cas de contentieux.

Autonomie de l'usager

L'autonomie de l'usager dans l'environnement numérique est remise en cause de multiples façons : tant par des usages imposés (travail, transports, banques, opérateurs téléphoniques, etc.) que par l'existence d'une population éloignée de la technologie et/ou qui n'est pas ou plus en capacité d'utiliser des dispositifs numériques : population

vieillissante, personnes non équipées de dispositifs électroniques récents, personnes handicapées, etc.

Cette question concerne également les « offres de services » (pollicitation) où la volonté des parties, qui est la base du droit des contrats, ne peut s'exprimer, dans la mesure où les termes du contrat ne sont pas négociables : l'offre ne peut être qu'acceptée ou refusée dans son entièreté. Cette situation est typique des contrats d'assurance, de banque, etc. L'acceptation des conditions générales de vente ou de services est parfois exigée simplement pour accéder à des informations, comme par exemple sur les plate-formes de réseaux sociaux. Certaines clauses peuvent être abusives au regard du droit national ou international sans que l'utilisateur puisse se défendre efficacement. La création de mécanismes d'action de groupe, telles que prévues par la loi « République numérique », constitue un progrès, qui n'est cependant pas de nature à changer significativement, à court terme, les pratiques des responsables de traitements.

Ces offres de service posent aussi la question de la contrepartie. La libre exploitation, pouvant aller jusqu'à la revente, des données des usagers est-elle une contrepartie équitable pour la mise à disposition d'un service numérique, au vu de la valorisation actuelle du marché des données personnelles ?

Synthèse réalisée par Chantal Enguehard à partir des éléments débattus collectivement lors de la table ronde

- Pour un droit de l'algorithme -

-

Ils permettent d'identifier le meilleur candidat lors d'un recrutement ; ils aident les entraîneurs sportifs dans le choix des tactiques de jeux ; sur les marchés financiers, ils passent des ordres d'achat et de vente ; ils vous proposent la musique que vous aimez ; ils calculent l'itinéraire le plus rapide et vous trouvent la partenaire sexuelle idéale. Ce sont les algorithmes.

Inodores, incolores, ils sont pourtant présents à tous les niveaux de la société. Comparables à l'eau, ils sont devenus indispensables à notre vie.

Qu'est-ce qu'un algorithme ? Après quelques recherches, il semble qu'il n'existe pas de définition universelle. J'ai choisi de reprendre la définition proposée par courrier international car elle est compréhensible par tous. L'algorithme est un « ensemble de règles et d'instructions qui permettent de réaliser une séquence d'opérations pour résoudre un problème. L'algorithme peut être traduit en programme exécutable par un ordinateur ».[1]

À la lecture de la revue en ligne « Interstices.info »[2] nous comprenons que la notion d'algorithme est ancienne et s'applique à de nombreux domaines. Ainsi, pour la recherche d'un mot dans un dictionnaire nous utilisons une méthode de tri qui constitue un algorithme.[3] Dans le cadre de notre contribution, nous nous intéresserons aux algorithmes mis en œuvre par un ordinateur.

Il est en effet certain que l'avènement de l'ordinateur a permis d'en décupler l'usage. Les progrès de miniaturisation des processeurs ont permis d'atteindre des puissances de calcul vertigineuses. Les recherches sur l'ordinateur quantique qui permet de dépasser les limites de la physique laissent penser que les vitesses de calcul peuvent encore augmenter.

Il faut conjuguer à ceci l'explosion des données personnelles qualifiée « d'or noir du XXIème siècle ». [4] Nouvelle manne financière certes dont les experts s'accordent cependant à dire qu'elle n'est rien sans une méthode de tri efficace et pertinente, c'est-à-dire rien sans un « bon » algorithme. Ainsi, selon la société de conseil Gartner « les

[1] Courrier international, n°1299 du 24 au 30 septembre 2015
[2] https://interstices.info/jcms/jalios_5127/accueil
[3] https://interstices.info/jcms/c_5776/qu-est-ce-qu-un-algorithme
[4] http://www.challenges.fr/high-tech/20140926.CHA8245/vos-donnees-personnelles-sur-internet-peuvent-valoir-de-l-or.html

données sont intrinsèquement passives. Elles ne font rien sauf si vous savez comment les utiliser, comment agir sur ces données, car la véritable valeur réside dans les algorithmes »[5].

Vitesse de calcul des ordinateurs et explosion des données personnelles ont permis l'arrivée d'une nouvelle catégorie d'algorithme : les algorithmes prédictifs.

Un algorithme prédictif est un programme mathématique permettant de calculer des scores prédictifs en fonction des différents types de données disponibles sur les individus étudiés et sur leur comportement de consommation ou d'usage[6].

Les algorithmes prédictifs sont présentés par les experts comme des outils révolutionnaires et incontournables. Tous les secteurs d'activité sont concernés. Donnons quelques exemples. Les entreprises commerciales s'en servent pour ajuster au plus près l'offre, définir des profils de consommateurs en fonction de leurs goûts, de leurs centres d'intérêt, de leur identification à une communauté. Les banques et assurances les utilisent pour prédire les risques de fraude ou d'impayés. Les réseaux sociaux en font un grand usage pour mettre en relation les amis et « les amis de vos amis ». Les objets connectés dans le secteur de la santé fournissent une manne d'informations permettant tris, recoupements et ciblages en tout genre. Les services de police en font également usage pour prévoir notamment les zones de rassemblement lors de manifestations.

De cette énumération pourtant non exhaustive, il est possible de tirer deux enseignements : il faut d'abord noter que le chiffre a pris une place immense dans notre société ; il faut ensuite relever que la société a une foi inconditionnelle dans le résultat mathématique.

Dans cette société gouvernée par le chiffre, que devient le citoyen ? Quelle liberté de pensée pour le citoyen dont l'information lui parvient en fonction de ses centres d'intérêt eux-mêmes identifiés grâce aux calculs algorithmiques ? Quel libre arbitre pour le consommateur ? Quand l'internet est construit initialement comme un espace de liberté basé sur l'échange collaboratif ; l'algorithme prédictif n'est-il pas susceptible de conduire à l'enfermement de la personne ?

Le droit peut-il être la réponse à ces questions ? Pour comprendre l'intérêt d'un droit de l'algorithme, il faut reprendre les finalités du droit.

[5] http://www.zdnet.fr/actualites/sans-algorithmes-le-big-data-ne-sert-a-rien-explique-le-gartner-39832842.htm
[6] https://www.definitions-marketing.com/definition/algorithme-predictif/

Le droit est un ensemble de règles destiné à organiser la vie en société. Il a pour finalité d'assurer l'ordre social garantissant les besoins de stabilité et de sécurité des individus. Selon Alain Supiot, le droit remplit « une fonction singulière » dans l'histoire des techniques, « celle d'un outil d'humanisation des techniques ».[7] Ainsi, le droit doit permettre d'humaniser la relation homme/machine.

Les algorithmes prédictifs résultent d'une utopie cybernétique : rendre l'être humain transparent. Or, cela revient à le priver de son intériorité. C'est là que le droit doit intervenir pour replacer l'homme en tant que sujet de droit et non objet de calcul.

« Le sujet de droit est la personne envisagée dans sa fonction juridique ».[8] À ce titre, la personne jouit de droits qui lui sont propres dont il convient d'assurer la protection.

En l'espèce, l'algorithme prédictif porte bien sur les personnes puisqu'il est intimement lié aux données personnelles collectées.

Quel est l'état du droit sur la question ?

Pour trouver quelques dispositions il faut regarder du côté du droit à la protection des données à caractère personnel garanti par la loi « informatique et libertés » du 6 janvier 1978 principalement modifiée par la loi n° 2004-801 du 6 août 2004 issue de la transposition de la directive n°95/46/CE du Parlement européen et du Conseil du 24 octobre 1995. Ainsi, lors de la constitution de fichier, l'individu concerné a un droit d'information, d'accès, d'opposition et de rectification. Dans le cadre de l'utilisation des données, l'article 10 de la loi dispose qu'« aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le *seul* fondement d'un traitement automatisé de données destiné à définir le profil ou à évaluer certains aspects de sa personnalité ».

La loi mentionne « les traitements automatisés » mais à aucun moment il n'est clairement fait référence aux algorithmes. De fait, l'algorithme n'est pas défini en droit.

En 2014, le rapport du conseil d'État relatif au numérique et aux droits fondamentaux énonce un certain nombre de préconisations concernant les algorithmes prédictifs. Il préconise une obligation de transparence sur les données utilisées par l'algorithme ainsi que sur le raisonnement suivi par celui-ci. Il préconise également de renforcer les pouvoirs de la CNIL en développant le contrôle des algorithmes par l'observation de leur résultat permettant la détection des discriminations.

[7] A. Supiot, « Homo juridicus, essai sur la fonction anthropologique du Droit », Point, Essais, 2009, p 203
[8] J-L. Aubert, E. Savaux, « introduction au droit et thèmes fondamentaux du droit civil », 14è éd., Sirey, 2012, p201

Comme on le comprend aisément l'algorithme prédictif est un outil au service de l'analyse des données. Il serait donc judicieux que le droit de l'algorithme découle de la protection des données à caractère personnel. Il conviendrait aujourd'hui de reconnaître que chaque individu est titulaire d'un patrimoine informationnel. Quelle qualification juridique lui donne-t-on alors ? Comment accepter que des données personnelles soient analysées par des algorithmes prédictifs sans que la personne concernée n'y ait consenti, sans qu'elle ne soit en mesure d'en comprendre la finalité ? Serait-il judicieux de transposer les droits prévus pour la collecte des données aux algorithmes ? Comment garantir l'effectivité de telles garanties dans un contexte de mondialisation ?

Face au progrès technologique le droit peut adopter deux attitudes. La première consiste à « épouser le fait »[9] à s'adapter. La seconde, plus volontariste, consiste à soumettre les technologies aux valeurs humaines. Ce choix est crucial car il déterminera la place de l'homme et de la machine. Il ne s'agit pas de diaboliser le progrès technologique et bien sûr le droit ne doit pas être une entrave au progrès. Il doit cependant en garantir les dérives.

Je conclurai ma contribution par cette dernière question : que devient le droit s'il ne sert pas de rempart, s'il n'est pas ligne directrice au service de la protection des individus ?

[9] J. Carbonnier, « Flexible droit, pour une sociologie du droit sans rigueur », L.G.D.J, 8è éd., 1995, p315

Comment vérifier les résultats du vote par Internet ?

Tatiana Shulga-Morskaya (CERCCLE - EA 7436)

La possibilité de voter par Internet aux scrutins politiques agite les esprits. Nombreux sont les chercheurs essayant de trouver une solution à des problèmes *a priori* insolubles. Comment concilier le secret du vote avec la possibilité de vérifier que le vote a été correctement pris en compte ? Comment assurer la liberté de vote depuis « l'environnement non controlé » ? Comment faire pour que le scrutin puisse être observé et non seulement par les informaticiens mais aussi par tout citoyen intéressé ? Massives sont les critiques apportées aux solutions existantes du vote par Internet qui est pratiqué à l'Estonie, en Suisse, au Canada et à l'Australie. On peut juste évoquer certains points faibles, notamment la vulnérabilité du système de vote, la possibilité de l'achat des voix et de la coercition, la violation possible du secret du scrutin, les difficultés liées à la vérification de l'identité de l'électeur, ainsi que la possibilité de dissimuler des fraudes massives.

Toutefois, il semble que le vote en ligne soit le futur des scrutins politiques. Dans cette perspective, il faut distinguer ce type de vote du vote électronique en général. Selon le Conseil de l'Europe, le vote électronique est l'« *élection ou référendum électroniques qui impliquent le recours à des moyens électroniques au moins lors de l'enregistrement du suffrage* »[1] alors que le vote par Internet, autrement dit le vote électronique à distance, est le « *vote électronique où le suffrage est enregistré au moyen d'un dispositif non contrôlé par une autorité électorale* »[2]. A l'heure de la révolution numérique, il semble que ce soit le vote électronique à distance qui va se développer dans un avenir proche.

Dans cette perspective, la question centrale qui se pose est de savoir comment vérifier les résultats du vote par Internet tout en gardant le secret de vote ? La majorité des autres problématiques en découlent donc la réponse à cette question pourrait mettre fin aux débats concernant la possibilité de l'utilisation du vote en ligne aux élections politiques.

Une telle question a été déjà posée à l'Estonie, où suite aux élections parlementaires de 2011, la chambre de contrôle de constitutionnalité de la Cour d'Etat de la République d'Estonie a rejeté trois requêtes visant l'annulation de leurs résultats en raison notamment de la violation possible du secret du vote[3]. Selon la Chambre, les allégations des requérants n'étaient

1 Council of Europe.Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Strasbourg: 2004. Disponible sur: https://wcd.coe.int//ViewDoc.jsp?Ref=Rec(2004)11&Language=lanEnglish&Ver=original&BackCol%20orInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75. P.3

2 Ibid.

3 The Constitutional review chamber of the Supreme Court of the Republic of Estonia. Constitutional judgement 3-4-1-4-11. Complaint of Paavo Pihelgas for annulment of electronic votes cast in the Riigikogu elections 2011. 2011. [réf.04/02/2015]. Disponible sur: http://www.riigikohus.ee/?id=1243. , The Constitutional review chamber of the Supreme Court of the Republic of Estonia. Constitutional judgement 3-4-1-6-11. Complaint of Henn Põlluaas for annulment of electronic votes cast in the Riigikogu elections 2011. 2011. [réf.04/02/2015]. Disponible sur:

qu'hypothétiques ; ils n'ont pas apporté la preuve que le secret du vote a été effectivement violé alors que selon la législation estonienne, les résultats du vote ne peuvent être déclarés nuls que si la cour conclut que la violation de la loi a influencé ou aurait pu influencer les résultats du vote à un degré significatif. En même temps, il faut noter qu'il n'est pas non plus possible d'apporter la preuve que les élections étaient sincères.

Le cas estonien pose la question essentielle : comment trouver la balance entre la transparence et le secret du vote en ligne ? Tout comme lors du vote papier, le système de vote en ligne ne donne pas au votant de moyens de prouver que son vote a été correctement pris en compte. Toutefois, dans le cas du vote papier, l'observation électorale permet de s'assurer du bon déroulement du scrutin en général et, ce qui est important, l'observateur ne doit pas avoir des connaissances particulières pour le faire. Alors que pour observer le vote en ligne, il faut être informaticien expérimenté avec des connaissances profondes du système de vote utilisé et avec l'accès à ce dernier. *Quid* du droit de tout citoyen d'observer le vote reconnu par plusieurs états démocratiques ? Ce droit n'étant pas négociable, il faudrait trouver une solution permettant au citoyen lambda de vérifier qu'au moins, son propre vote a été correctement compté. Pour l'instant, il semble qu'il n'y ait pas de solution définitive permettant de le faire sans violer le secret du vote, bien qu'il y ait déjà certain progrès là-dessus[4]. Pourtant, il est largement admis que même si une telle solution existait, l'émission par le système d'une confirmation de vote serait dangereuse du point de vue de l'achat des voix[5]. Comment assurer la protection de la sincérité des élections dans ce cas ?

En même temps, il convient peut-être aux juristes de réfléchir sur le concept du secret du vote à l'ère numérique. Lors des élections en ligne norvégiennes, il est devenu évident que « s'il ne s'agit pas *de la coercition ou de l'influence indue, beaucoup de gens sont prêts à accepter que leur vote soit observé par d'autres, même s'il s'agit d'une violation des dispositions législatives. Cela indique que la compréhension populaire du secret du vote diffère de l'interprétation juridique* »[6]. La

---

http://www.riigikohus.ee/?id=1255. , The Constitutional review chamber of the Supreme Court of the Republic of Estonia. Constitutional judgement 3-4-1-7-11. Complaint of Teet Raatsin for declaration of invalidity of the voting results of the Riigikogu elections 2011. 2011. [réf.04/02/2015]. Disponible sur: http://www.riigikohus.ee/?id=1256.

4 V. par ex. les travaux des chercheurs travaillant sur les systèmes d'e-vote bout-en-bout vérifiables : Ben Adida. Helios: Web-based Open-Audit Voting. 17th USENIX Security Symposium (Security '08). San Jose, CA, USA. 2008. [réf. 04/02/2015]. Disponible sur: http://static.usenix.org/events/sec08/tech/full_papers/adida/adida.pdf. ; End-to-End Verifiable Internet Voting Project. Overseas Voter Foundation [réf. 04/02/2015]. Disponible sur: https://www.overseasvotefoundation.org/E2E-Verifiable-Internet-Voting-Project. ainsi que le progrès des systèmes d'e-vote existants 2015 : évolutions du système de vote électronique genevois. La République et canton de Genève Chancellerie [en ligne]. 2015. [réf. 11/02/2015]. Disponible sur: http://ge.ch/vote-electronique/actualites/2015-evolutions-systeme-de-vote-electronique-genevois.

5 Council of Europe.Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Strasbourg: 2004. Disponible sur: https://wcd.coe.int//ViewDoc.jsp?Ref=Rec(2004)11&Language=lanEnglish&Ver=original&BackCol%20orInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75. P.51

6 Jo Saglie, Signe Bock Segaard. Internet voting in Norway in 2013. The principle of the secret ballot in practice. 23rd

question qui se pose est de savoir « *si le secret du vote doit être considéré comme un droit ou un devoir du citoyen, c'est-à-dire si les électeurs et les autorités doivent veiller à ce que tous les votes soient exprimés en secret, ou bien ce sont les autorités qui doivent garantir le scrutin secret, alors que les électeurs ont le droit de voter à bulletin secret mais pas nécessairement le devoir de garder le secret de son vote* »[7].

En tout état de cause, la possibilité de vérifier son vote ne remet pas en question la nécessité de l'observation qualifiée des travaux de la commission électorale avant, pendant et après le vote. Comment une telle observation doit être organisée pour s'assurer de la sincérité du vote et, en même temps, ne pas mettre en danger la sécurité du système ?

Dernière question mais non le moindre est de savoir comment protéger le système de vote contre les attaques de l'extérieur ? Dans le contexte actuel des tentatives d'influencer les résultats des élections depuis l'étranger, l'on peut se demander si le système de vote ne pourrait être utilisé comme un tel moyen et, au bout du compte, comme une menace potentielle pour la souveraineté ? Comment donc assurer sa protection sans perte de la transparence, nécessaire pour son observabilité ?

Vu que cette problématique est à la croisée des disciplines, il faut une collaboration étroite des juristes et des informaticiens pour y répondre. Notamment, on pourrait réfléchir ensemble sur la possibilité d'utiliser la technologie Blockchain et sa compatibilité avec les exigences du vote démocratique, plus précisément : le suffrage universel, égal, secret, libre et direct ainsi que avec les exigences à la procédure du scrutin, à savoir la transparence, la vérifiabilité, la fiabilité et l'authenticité[8].

IPSA World Congress of Political Science 19-24 July 2014 Montréal, Québec. Canada.

7 Ibid.

8 V. les tableaux ci-dessous

Tableau 1. Principes du vote démocratique et exigences au système de vote

Principe	Exigence au système	Définition
Suffrage universel	Accessibilité	Tous les votants autorisés ont la possibilité de voter, c'est-à-dire : 1) ils ont ou peuvent facilement obtenir l'accès au système, 2) son utilisation est facile et n'exige pas de compétences particulières, 3) en cas des problèmes les votants peuvent obtenir des renseignements rapidement et efficacement
Suffrage égal /équitable	Authentification correcte du votant	1) Les votants non autorisés ne peuvent pas voter par le biais du système 2) Le système ne permet pas au votant d'exprimer son vote par plusieurs modes de suffrage 3) Tout bulletin déposé sera comptabilisé et ne sera comptabilisé qu'une seule fois, même si plusieurs modes de suffrage sont utilisés dans le même scrutin
Suffrage secret	Bulletin secret	1) L'impossibilité de lier le votant avec son vote 2) L'impossibilité pour le votant de prouver son vote aux tiers
Suffrage libre et direct	Vote libre et immédiat	3) La manière dont les votant sont guidés lors le vote ne les amène pas à voter dans la précipitation ou de manière irréfléchie 4) Les votants peuvent modifier leur choix à n'importe quelle étape de la procédure de vote aussi que déposer un vote blanc 5) Le système de vote indique clairement au votant que le suffrage a été enregistré avec succès et à quel moment la procédure de vote est terminée Tous les votants peuvent faire leur choix de façon directe, sans intermédiaires de toute sorte, y compris intermédiaires ayant la maîtrise technique ou qui peuvent influencer leur choix

Tableau 2. Garanties de la procédure du vote démocratique et exigences à la procédure de vote en ligne

Garantie	Exigences à la procédure	Définition
Transparence	Transparence	1) Les observateurs doivent avoir la possibilité de suivre les travaux de la commission électorale sur l'organisation du scrutin en ligne ainsi que ses travaux le(s) jour(s) de vote 2) L'organisation du scrutin doit permettre aux observateurs d'observer le processus de recueil et de comptage des voix ainsi que d'avoir accès au code source du système de vote 3) Tout intéressé doit pouvoir s'opposer d'une manière efficace à l'enregistrement d'un vote erroné ou frauduleux par le biais du système de vote
Vérification	Vérifiabilité	1) Avant la mise en service, par la suite à intervalles réguliers et après tout changement du système, l'autorité électorale compétente ainsi qu'un organisme indépendant doit vérifier que le système de vote fonctionne correctement et que toutes les mesures de sécurité nécessaires ont été prises 2) Toutes les caractéristiques du système qui peuvent peser sur l'exactitude du résultat du vote doivent être vérifiables
Fiabilité	Fiabilité et sécurité	Les autorités publiques compétentes garantissent la fiabilité et la sécurité du système par les moyens suivants : 1) La prévention des dérangements, des pannes, des attaques en déni de service, des fraudes ou des interventions non autorisées 2) Les interventions au système de vote et aux données relatives au vote doivent être autorisées par l'autorité électorale, suivant à des règles claires et publiques, notamment la collégialité, la contrôlabilité, la représentativité, la verbalisation. 3) Le respect du principe de confidentialité des données y compris le cryptage et le scellage des données 4) La garantie de la disponibilité et de l'intégrité des suffrages.
Authenticité	Authenticité du canal de vote	Le votant doit pouvoir vérifier que la connexion est établie avec le serveur authentique et qu'un bulletin authentique lui est présenté

Systèmes Inéquitables Numériques (SIN)

Chantal Enguehard
(chantal.enguehard@univ-nantes.fr)

Problématique

L'usage de Systèmes Numériques fait intervenir de multiples parties : les concepteurs, l'administration, les commerçants ou les employeurs ayant choisi de déployer le système numérique, les hébergeurs de données, les utilisateurs finaux, etc. Un Système numérique peut prendre des formes très variées : une plate-forme internet, un logiciel (par exemple une base de données de gestion de personnels), ou encore un système incluant du matériel tels les terminaux de validation de tickets de transport dématérialisés, etc.

Numériques, ces dispositifs ont pour double caractéristique : d'une part, la dématérialisation des échanges d'informations ; d'autre part, le fait que certains acteurs (il s'agit souvent des utilisateurs finaux) ne disposent pas d'accès aux traces de leurs interactions avec le système numérique en question.

Certains systèmes numériques peuvent être qualifiés d'**inéquitables** dans la mesure où, en cas de dysfonctionnement qui lèse les droits d'une des parties, il est possible que cette partie n'ait pas accès aux traces de ses interactions avec le Système numérique et ne puisse donc prouver sa bonne foi.

En voici quelques exemples :

- Dans le secteur des transports il peut arriver qu'un utilisateur oblitère un ticket électronique mais que cette oblitération, mal enregistrée, ne soit pas visible par le contrôleur. Dans ce cas, le contrôleur peut infliger une amende.
- Lors de la location d'un vélo en libre service, l'utilisateur ne dispose d'aucune trace prouvant qu'il a restitué le vélo sur une borne. Si le système a mal enregistré cette restitution, ou a « libéré » le vélo par erreur, l'utilisateur peut être débiteur de frais dû à la non restitution de vélo.
- Dans le domaine des élections, l'usage de dispositifs de vote électronique interdit de fait aux électeurs de participer ou même de surveiller le dépouillement. Bien que les systèmes de vote électronique modifient à plusieurs reprises les informations portant les intentions de vote des électeurs (changement de format, etc.), ces derniers ne peuvent s'assurer que les résultats annoncés sont conformes aux intentions de vote qui ont été exprimées et donc qu'il sont sincères.

Comme l'usage de systèmes numériques est devenu de plus en courant depuis une dizaine d'années et qu'il tend à devenir **obligatoire** dans certains domaines (pour les demandeurs d'emplois par exemple, pour voter, ou au travail), l'insécurité juridique liée à cet usage va se développer. Le risque que des utilisateurs soient lésés sans pouvoir se défendre et perdent confiance dans les outils numériques peut donc s'accroître.

Cette recherche a pour but d'explorer ce phénomène afin de mieux le **définir**. En effet, une première étude sur le sujet a déterminé que le concept de SIN n'est pas immédiatement opérant dans le domaine juridique et qu'il s'agirait d'en cerner les **variantes** en fonction du domaine, des acteurs, de la nature des droits lésés, etc. ce qui permettra d'en dresser une **typologie** Il s'agira ensuite de mener des études fines et transdisciplinaires de chacune des variantes afin de les caractériser. Voici quelques questions qui pourraient être abordées : quelles sont les populations concernées ? quels sont les droits lésés ? Quelle est la jurisprudence dans le domaine ? est-il possible de modifier le système afin qu'il ne soit plus un SIN ? Comment reconnaître un SIN ? Comment concevoir des systèmes numériques qui ne soient pas des SIN ?

Certaines de ces variantes peuvent d'ors et déjà être étudiées car elles ont déjà fait l'objet de recherches disciplinaires sans que leur appartenance à la catégorie, alors inexistante, des SIN n'ait été établie.

C'est le cas des systèmes de **vote électronique** déployés depuis une vingtaine d'années dans le cadre des élections politiques ou professionnelles ou encore des référendums. Les dispositifs de vote électronique utilisés en France sont caractérisés par la dématérialisation des choix exprimés par les électeurs (les « bulletins de vote ») et la multiplicité des transformations qui leur sont appliquées et qui sont susceptibles d'avoir des répercussions quant à la **sincérité** des résultats électoraux. La **liberté de vote** est également en jeu car des électeurs peuvent douter du respect du secret du vote, et donc modifier leur intention initiale de vote.

Or, un processus électoral démocratique doit susciter la **confiance** afin que les électeurs votent librement. La capacité à contester des élections devant la justice, et à obtenir annulation partielle ou totale des résultats électoraux est une composante essentielle de ce processus.

Le fonctionnement des processus électroniques étant inobservables directement, des procédures nouvelles ont été mises en place au sujet de leur fiabilité[1] et de leur sûreté[2]. Ainsi, le ministère de l'intérieur a décrété une procédure d'agrément des modèles de machines à voter, puis a instauré un cahier de suivi de chaque exemplaire de machines à voter, la CNIL demande que les systèmes de vote électronique fassent l'objet d'une expertise préalable, etc. Ces procédures ont déjà fait l'objet de critiques récurrentes quant à leur capacité à effectivement garantir la sécurité des processus électoraux. En revanche, l'articulation entre le non respect de ces procédures et la possibilité de contester une élection et à en obtenir l'annulation n'a pas été questionnée.

Il s'agit de s'interroger sur la capacité des électeurs ou des candidats à exercer un contentieux électoral en fonction du dispositif électoral utilisé et de différentes atteintes au processus électoral ou aux procédures qui l'entourent. La jurisprudence à ce sujet pourra être examinée afin de dresser un état de la situation, des pistes d'amélioration pourront être présentées, examinées et critiquées.

Nous proposons que l'atelier porte, d'une part, sur la définition des SIN et la construction d'une typologie des variantes et, d'autre part, sur l'étude du cas particulier que constitue le vote électronique. Il s'agira d'étudier à la fois différents types de dispositifs de vote électronique et le système juridique dans lequel ils s'inscrivent afin de déterminer si la capacité à contester une élection a été améliorée ou détériorée.

Dispositifs susceptibles d'être étudiés :

- machine à voter et élections politiques en France, en Belgique ;
- vote par Internet et élections politiques en France, en Suisse ;
- vote par internet et élections professionnelles en France ;
- dépouillement par scanner et élections professionnelles en France ;
- machine à voter et trace papier au Vénézuéla, aux États-Unis et en Australie.

Le vote « à l'urne » et le vote par correspondance seront également examinés à titre de comparaison.

Communauté d'appartenance de Chantal Enguehard :

Informatique

Éléments de contribution de Chantal Enguehard

Organisation d'une journée d'étude « Usage imposé de dispositifs électroniques »[3] portant, entre autres sur les SIN (3 novembre 2016 à Nantes).

1 Fiabilité : capacité d'un système à fonctionner sans erreur et sans tomber en panne.

2 Sûreté : ensemble des moyens matériels, humains, organisationnels visant à éviter ou contrer toute attaque malveillante.

3 http://www.sciences-techniques.univ-nantes.fr/1476888818797/0/fiche___actualite/&RH=SET_FR1 .

Connaissances techniques et théoriques des dispositifs de vote électronique (publications scientifiques).

Observations de l'utilisation des machines à voter en France depuis 2007 pour les élections politiques (performances et usages) : des données électorales détaillées par bureau de vote ont été collectées auprès de plus de 500 communes.

Expérience de terrain quant au contentieux électoral.

Vulgarisation sur le sujet du vote électronique (articles et conférences grand public).

Transparence des algorithmes : quelles réponses juridiques et techniques ?

Daniel Le Métayer
Inria
http://www.inrialpes.fr/planete/people/lemetayer/dlemetayer-fr.htm

On s'intéresse ici à une catégorie particulière d'algorithmes, ceux qui sont utilisés pour l'aide à la décision ou dans des traitements qui ont des incidences sur les comportements individuels, qui ont donc un effet normatif. A titre d'exemples, on peut citer :

- Les algorithmes de classement, qui établissent des priorités, des recommandations : on pense évidemment aux algorithmes de présentation des résultats des moteurs de recherche, mais aussi à ceux qui sont utilisés pour classer les candidats à un poste ou les rues d'une ville que la police doit surveiller en priorité (police prédictive : PredPol), etc.
- Les algorithmes de catégorisation, de classification, de profilage comme ceux qu'on met en œuvre pour détecter des profils de potentiels terroristes, de fraudeurs, de clients, de personnes non solvables ou à cibler dans une campagne électorale.

Ces algorithmes présentent quelques caractéristiques communes :

- ils ont une incidence importante sur les vies des personnes concernées (soit leurs vie quotidienne, soit à des moments spécifiques, généralement déterminants: candidature à un poste, demande de prêt, demande de visa, etc.),
- ils ne sont ni neutres (au sens où ils mettent en œuvre des critères de priorité, de catégorisation, etc.), ni forcément corrects (faux positifs, faux négatifs), et
- leur fonctionnement est généralement opaque (certains utilisateurs ignorent même parfois leur existence).

Cette combinaison de caractéristiques plutôt inquiétante permet d'imaginer toutes sortes de dérives : traitements injustes, discriminations, manipulation, etc.

Face à cela, on peut se poser au moins deux types d'interrogations: est-ce qu'on peut distinguer des types d'utilisation, des circonstances, où il faudrait limiter l'usage de ces algorithmes : par exemple jusqu'où souhaitons-nous aller en terme d'individualisation des traitements en matière d'assurances (doit-on passer par pertes et profits le principe de mutualisation ?), de consommation (doit-on pouvoir faire payer n'importe quel bien à la tête, ou plutôt au profil, du client ?). Est-il acceptable que des décisions importantes puissent être prises sur la base d'algorithmes complètement opaques pour le décideur (et qu'en est-il des responsabilités si la décision s'avère mauvaise) ?

Puisqu'un des problèmes provient de l'opacité de ces algorithmes, une question essentielle est celle de la transparence. Tout d'abord, la transparence qui nous intéresse ici ne peut pas se réduire à la simple mise à disposition des codes source des logiciels, que le néophyte (et même parfois l'expert) a peu de chances de comprendre. Ce n'est pas non plus forcément connaître leur mode opératoire dans ses moindres détails. L'important est de pouvoir comprendre certains aspects critiques du

fonctionnement d'un algorithme, notamment les informations qui sont utilisées et leur impact sur le résultat final (favorable, défavorable, dans quelle mesure ?).

Différentes méthodes peuvent être appliquées pour améliorer la compréhension des algorithmes, notamment la rétro-ingénierie de logiciels. Cependant, celle-ci a des limites. D'une part légales, puisqu'elle est parfois interdite par les auteurs des logiciels, mais surtout techniques : en effet, le procédé demande beaucoup d'effort, la réussite n'est pas certaine et de plus certains des algorithmes s'y prêtent mal, notamment les algorithmes qui reposent sur l'apprentissage. La complexité de ces algorithmes provient généralement de la taille des données analysées plus que de celle du code lui-même ; de plus, leur fonctionnement évolue au cours du temps. Par ailleurs certains algorithmes, ou leur paramétrage, peuvent aussi être modifiés régulièrement par les acteurs qui les contrôlent (on sait que c'est le cas pour les moteurs de recherche).

L'inconvénient principal de la rétro-ingénierie est qu'il s'agit une démarche non-collaborative, a posteriori. L'idéal serait en fait de promouvoir une démarche de transparence et de responsabilité par construction – ce qu'on appelle parfois « accountability by design » de la même façon qu'on parle de « privacy by design » – incorporer ces valeurs, ces exigences dès la phase de conception d'un système.

Pour conclure, il faut aussi se poser les questions de ce qu'on peut légitimement exiger en matière de transparence et des limites de cette transparence. Ces limites peuvent être liées à des impératifs de protection de la propriété intellectuelle : quand cet argument est-il recevable ? Est-ce que c'est nécessairement un obstacle à la transparence ? Une autre limite est liée au phénomène de contournement (la connaissance du fonctionnement de l'algorithme permet de s'y adapter) avec les mêmes questions : quand cet argument est-il recevable ? Quand l'exigence de transparence doit-elle l'emporter ? Et, finalement, dans les situations où l'objectif de transparence serait tout à fait hors de portée, peut-on accepter l'utilisation d'un algorithme comme outil d'aide à la décision quand les enjeux sont importants pour les personnes concernées (emploi, prêt, visa, décision de justice, etc.) ?

Le législateur s'est déjà saisi de la question de la transparence des algorithmes, notamment à l'occasion de la loi pour une République numérique qui impose de nouvelles obligations aux administrations et aux plateformes. Le nouveau Règlement européen sur la protection des données personnelles comporte également des dispositions visant à améliorer la transparence mais celles-ci sont très limitées et d'une effectivité douteuse. Comment améliorer la transparence des algorithmes ? Comment règlementer en la matière ? Comment améliorer leur production, leur compréhensibilité ? Nous sommes en présence de défis majeurs pour les années à venir, des défis qui ne peuvent être abordés que dans une démarche interdisciplinaire tant les aspects juridiques et techniques sont entremêlés en la matière.

The *DAO* : « code is law » of the jungle ?

L'expérience des monnaies virtuelles, et plus particulièrement de *bitcoin*, a surtout suscité l'intérêt du monde économique en raison des possibilités qu'offre la technologie Blockchain.

Fondées sur un système de gouvernance décentralisée, les monnaies virtuelles ont soulevées des problématiques nouvelles (déterritorialité, responsabilité dans une gouvernance décentralisée, transparence et données personnelles, lutte contre le blanchiment et le financement des activités interdites, etc.). Face à ces questions, trois attitudes se sont opposés : il y a ceux qui pensent qu'un encadrement juridique spécifique est nécessaire, ceux qui pensent que moyennant leur interprétation les règles existantes sont suffisantes, et enfin ceux qui considèrent que le protocole informatique qui en régit le fonctionnement est suffisant.

Ainsi pour cette monnaie, parfois qualifiée de monnaie de singe, l'incantation « code is law » serait suffisante (L. Lessig, « Code Is Law. On Liberty in Cyberspace », *Harvard Magazine*, 2000 (disponible en ligne : http://harvardmagazine.com/2000/01/code-is-law-html). Alors que dans cet appel, la théorie de Lessig n'en sort pas indemne, l'importance financière croissante de Bitcoin nécessite d'investir cette question. En effet, à l'examen on peut craindre que cette loi informatique soit finalement celle de la jungle.

Investir cette question est d'autant plus nécessaire que le développement de la blockchain démultiplie son importance et que les promoteurs des projets en cours se prévalent généralement de l'idée d'une innovation « hors sol juridique », libérée du contrôle étatique.

Le projet porté par la communauté d'Ethereum semble aujourd'hui à cet égard le plus avancé (le *White Paper* qui accompagne ce projet est disponible à l'adresse suivante : https://slock.it/dao.html). Il consiste à promouvoir une nouvelle forme d'association digitale de partenaires porteurs de fonds. La « *decentralized autonomous organization* » est toutefois conçue comme un conseil d'administration géant, au sein duquel la prise de décision est ouverte et transparente (« auditable ») grâce à l'utilisation du registre d'Ethereum (il est possible de faire des liens entre ce projet et le mouvement « *democracy by design* » – P. de Filippi et D. Bourcier, *op. cit.*, p. 48).. La structure se comporte ensuite comme un fond d'investissement ouvert (il est possible d'y entrer librement), qui répond aux offres présentées par des membres ou des tiers (*TheDAO*, premier essai, a été mis en œuvre à très grande échelle puisqu'il aurait réuni jusqu'à 130 millions d'euros) ou elle peut avoir été créée afin de

répondre à un objectif spécifique (projets de *Slock.it* et de *Freeftopia*). Cette entité est supposée être dépourvue de statut juridique : elle serait davantage un programme qu'un organisme susceptible de se voir reconnaître une personnalité morale (la position des initiateurs de ce projet sur ce point mériterait toutefois d'être discutée, car la qualification de société de fait semble difficilement pouvoir être exclue et il en va de même pour la notion d'entreprise retenue en droit de l'Union européenne). Les participants sont liées entre eux et avec leurs cocontractants par des *smart-contracts*, intégrés à Ethereum, et dont la bonne exécution pourrait être certifiée par des tiers.

Le projet a connu toutefois une crise majeure depuis le 16 juin 2016, à la suite d'un vol de tokens (c'est-à-dire de parts des associés de *TheDAO*) pour un montant de 3,6 millions d'Ether. Les 11,6 millions restants ont été bloqués à la suite d'un *soft fork*, de sorte que ni *TheDAO*, ni les participants ne pouvaient les utiliser. Après un débat difficile, il a été convenu de réécrire le registre d'Ethereum, à la faveur d'un *hard fork*, afin de reprendre les Ether volés au pirate et de les restituer à leurs détenteurs initiaux.

Cette affaire illustre les dangers de l'investissement dans ces nouvelles technologies. Les porteurs de *TheDAO* ont mis en place une procédure de remboursement pour les participants qui souhaiteraient se retirer, et craignent désormais que les régulateurs comme l'*AMF* (*Autorité des Marchés Financiers*) ou la *SEC* (*Securities Exchanges Commission*) américaine ne s'intéressent à la régulation des projets adossés à une Blockchain – venant ainsi couper l'élan d'innovation.

Cette solution, en apparence la plus juste, fut difficile à accepter dans la mesure où elle remettait en cause un principe fondateur de la technologie Blockchain : l'immuabilité[1]. Cet épisode montre que l'immuabilité ne tient que dans la mesure où elle bénéficie du consensus de la communauté. Non seulement, quiconque parvient à convaincre 51% des participants peut induire la réécriture du code qui gouverne le fonctionnement du système, mais en outre quiconque possède ou parvient à réunir 51% de la puissance de calcul du réseau peut bel et bien réécrire le registre des transactions.

[1] Un désaccord a conduit à une scission avec la création d'une chaîne minoritaire (*Etheruem classic*), dans laquelle les tokens volés n'ont pas été retournés. Elle se présente donc comme réellement immuable et affirme faire une exacte application de la maxime « *code is law* » en partant du principe que les investisseurs auraient dû être plus vigilants et découvrir la faille dans le code de *TheDAO*. Cet épisode a plus largement été l'occasion de revivifier le débat sur la portée de cette doctrine (voir, par exemple, http://www.coindesk.com/code-is-law-not-quite-yet/).

Les opposants du *hard fork* ont dénoncé avec cet épisode une violation du principe « code is law ». Selon eux, ceux qui avaient tiré profit d'une faille du code originel étaient les possesseurs légitimes des tokens. Mais à l'inverse ne peut-on pas penser que la possibilité de réécrire le ledger au terme d'une procédure de vote « démocratique » est justement une application du principe précité (le consensus est en effet la source de la confiance dans le système) ? Cependant, cette solution a remis en cause le principe qui semblait jusque là fondamental de l'immuabilité (sur lequel repose normalement la sécurité du système).

En réalité, l'affirmation selon laquelle c'est le code qui définit la loi soulève pour le juriste une infinité de questions. D'abord de quel type de loi parle-t-on ? Est-ce de la soft law, ou faut-il y voir un ordre juridique au sens d'un ensemble de normes doté d'une logique et destiner à régir une institution ? On pourra encore se demander si les critères utilisés par Hart pour identifier un système juridique peuvent être satisfaits (règle d'appartenance, d'adjudication, et de changement). Ensuite, on doit s'interroger sur l'existence au sein du code d'une hiérarchie, d'une distinction entre des règles primaires et des règles secondaires, etc. qui seraient de nature à permettre à le changement des règles de fonctionnement tout en assurant la régularité de ces changements. Enfin, c'est la réalité de la décentralisation de la gouvernance qui doit être examinée (initiative, partage de l'information, transparence, application d'un principe démocratique du type « one computer, one vote », etc.), ainsi que la nécessité d'en assurer via le code ou une autre source de contrainte, le bon fonctionnent.

Si comme le prétend Lawrence Lessig, il est nécessaire de laisser dans un premier temps les innovations du monde de l'Internet se développer loin des rigidités d'une régulation d'origine étatique, il reste possible et souhaitable

BITCOIN ET BLOCKCHAINS : RÉFLEXIONS TERMINOLOGIQUES ET IDENTITAIRES

Réflexions terminologiques à propos du Bitcoin et des systèmes d'échanges décentralisés types blockchains et tentative de définition d'un nouveau paradigme d'identité et de certification.

L'objectif de la présente proposition de contribution est la mise en place d'un lexique précis autour des termes de la sphère Bitcoin et blockchains ainsi que la mise en place d'une réflexion sur les enjeux identitaires de ces nouveaux systèmes.

Le premier axe de réflexion est celui d'une définition claire des termes ayant trait à l'écosystème Bitcoin[1]. En effet le lexique employé découlant principalement des utilisateurs au fur et à mesure du temps, il s'avère que ce lexique n'est pas forcément limpide et similaire pour toutes les parties. Or il est essentiel de se mettre d'accord sur une terminologie précise pour pouvoir échanger entre les différents acteurs des secteurs pouvant être concernés par cet écosystème : l'informatique, le droit, la finance, etc.

L'objectif serait ici de réussir à élaborer un lexique commun avec le moins de décalages analogiques possibles ou du moins de réfléchir à leur pertinence. (mineur, portefeuille, compte, contrat, etc.) Cela permettra aussi de réfléchir par la même occasion à des normes techniques. Dans quelle mesure telle ou telle blockchain[2] pourrait-elle être considérée comme fiable ? Dans quelle mesure les jetons d'une blockchains pourraient-ils représenter des actifs ? Toutes ces questions peuvent être totalement résolues ou partiellement résolues à l'aide d'un lexique commun et d'une définition commune de ce qu'est une blockchain. En effet, dans l'optique, d'un jour peut-être, conférer une valeur probante[3] aux enregistrements dans les blockchains, il est essentiel de savoir lesquelles sont considérées comme telles et selon quels critères.

---

[1] Bitcoin : Système d'échanges décentralisé né en 2009 suite à la publication d'un livre blanc : *Bitcoin a peer-to-peer electronic cash system* de l'anonyme Satoshi Nakamoto. Ce protocole permet la production et l'échange d'actifs numériques non reproductibles (des bitcoins) à l'aide notamment d'un livre de compte dans lequel il est possible d'ajouter des données horodatées de manière fiable et infalsifiable.

[2] Blockchain (ou chaîne de blocs) : Registre de transactions décentralisé, c'est un des rouages permettant le bon fonctionnement des systèmes d'échanges décentralisés. Cependant chaque protocole ayant des spécificités différentes, il est impossible d'employer ce terme de manière défini au singulier sans l'accompagner du protocole qui définit ladite blockchain.

[3] La député Madame Laure de La Raudière a proposé un amendement en ce sens : http://www.la-raudiere.com/lng_FR_srub_39_iart_1327-je-presente-un-amendement-a-propos-du-blockchain-a-l-assemblee-nationale-pour-que-la-f.html

Une telle contribution n'est possible qu'avec la collaboration des acteurs des différents secteurs et de ce fait, l'évènement semble être très approprié pour cela.

Le deuxième axe de réflexion, fortement lié au premier, est celui de la valeur (juridique, économique) qu'il est possible de porter aux écritures au sein d'une blockchain comme celle de Bitcoin. Ce nouveau type de registres décentralisés de transactions permet la constitution d'une identité numérique bien plus fiable que celle des bases de données centralisées. (en raison de leur faiblesse aux attaques et du fait qu'elles impliquent de déléguer son identité à un tiers.) Dans une logique d'anticipation, serait-il possible par exemple de signer un document avec une adresse bitcoin ?

Là où un compte Facebook ou Google appartient à la firme qui propose le service, (en ce sens qu'il est dans ses serveurs et qu'il n'est possible à l'utilisateur de faire des changement qu'à l'aide d'une interaction avec l'entreprise) une adresse sur le réseau Bitcoin appartient totalement à la personne concernée. (en ce sens qu'elle est la seule à connaître sa clef privée.) Ce changement paradigmatique inclut dès lors une remise en question de l'identité numérique qui, dépourvue de toute possession extérieure, se rapproche de plus en plus d'une identité physique (je suis seul détenteur de mes empreintes.) , même si paradoxalement elle n'est délivrée par aucun tiers. (l'état se sert de mes empreintes pour m'identifier.) Cependant la constitution d'une identité claire dans ce territoire à part entière qu'est le cyberespace semble un enjeu capital autant d'un point de vue citoyen (possibilité de vote électronique sans faille.) que d'un point de vue judiciaire. (contrôle d'identité en ligne sans pour autant souffrir d'une atteinte à la vie privée.)

Et cela va de pair avec la certification sur les réseaux décentralisés. Il est possible de considérer que l'empreinte d'un document dans la blockchain Bitcoin est horodatée, fiable et infalsifiable dans le temps. *De facto* nous pensons à de nombreux cas pratiques comme celui de la « preuve d'antériorité ». Dans quelle mesure, l'envoi de l'empreinte d'un document dans la blockchain pourrait être considéré comme ayant la même fiabilité et la même valeur qu'une enveloppe Soleau délivrée par l'INPI ? De la même manière, il est essentiel que l'état puisse « marquer » des adresses pour jouer son rôle de tiers. Ainsi il serait possible d'avoir son âge et son sexe liés à son identité numérique sans pour autant la confier à un tiers. (ici l'état) Toutes ces questions doivent être étudiées car elles constituent une étape intermédiaire et obligatoire pour permettre la création d'une identité numérique respectant les droits fondamentaux du citoyen.

ADLI TAKKAL BATAILLE
Étudiant en master recherche de linguistique / Entrepreneur et représentant associatif dans le numérique

Convergence du Droit et du Numérique - Proposition de Contribution

Benoit Huguet,
benoit.huguet@bitconseil.fr

- Fondateur de BitConseil, média d'actualité et d'analyse à propos de Bitcoin, des monnaies numériques décentralisées, et des blockchains.
- Administrateur du Cercle du Coin, association Francophone à propos de Bitcoin et des blockchains
- Formateur Architecte de Registre Distribué pour Eureka Certification

Bitcoin, Blockchains et Monnaies Numériques Décentralisées : de l'étude de la technologie et des cas d'usage à l'élaboration d'un cadre juridique adapté.

L'objectif de cette proposition de contribution est de présenter aux professionnels du droit le fonctionnement de Bitcoin et de la comptabilité par blockchain à travers des exemples d'utilisation concrets et de permettre aux spécialistes du droit de travailler à la mise en place d'un cadre juridique adapté à ces nouvelles technologies et aux enjeux qu'elles soulèvent, en concertation avec les acteurs du secteur.

Né en 2009, Bitcoin est un système d'échange décentralisé, mondial, libre de droits et d'accès, qui révolutionne notre rapport à la monnaie et aux tiers de confiance.

Chaque jour, le protocole Bitcoin permet à des millions d'utilisateurs partout dans le monde[1] d'échanger de façon sécurisée l'équivalent de plusieurs centaines de millions de dollars, comptabilisés en bitcoins[2], sans passer par aucun intermédiaire financier[3]. C'est également en vertu de ce protocole qu'a été défini et déployé pour la première fois le système de comptabilité publique, décentralisée, horodatée et infalsifiable, nommé blockchain. Ce système comptable ouvre la voie à tout un ensemble de nouveaux services, plus transparents, mieux sécurisés, automatisés et moins coûteux. Il devient notamment possible grâce à la blockchain de Bitcoin d'enregistrer des documents dans un registre public et infalsifiable à tout petit prix[4] ; ou bien

[1] Début 2017, ARK et Coinbase estiment qu'environ 10 millions de personnes dans le monde possèdent des bitcoins, extrait de « Bitcoin : ringing the bell from a new class asset », janvier 2017, paper research by Chris Burniske, blockchain product lead – Ark Invest – and Adam White, Vice president & general manager - Coinbase

[2] L'équivalent de 200 millions de dollars en moyenne ont été échangés chaque jour sur le réseau Bitcoin en janvier 2017 : https://blockchain.info/fr/charts/estimated-transaction-volume-usd?timespan=all

[3] Bitcoin est un protocole pair à pair.

[4] Par exemple, les sites https://bitproof.io/ et https://www.ascribe.io/ permettent d'enregistrer l'empreinte numérique d'un document (son hash) dans la blockchain de Bitcoin pour quelques centimes, ce qui permet par la suite d'en certifier l'existence à une date donnée de façon certaine. Ceci étant la reconnaissance légale de ce genre de preuve reste encore à établir. Notons à ce propos l'initiative de la députée madame Laure de la Raudière qui a proposé un amendement visant à conférer une valeur probante aux enregistrements dans une blockchain : http://www.la-raudiere.com/lng_FR_srub_39_iart_1327-je-presente-un-amendement-a-propos-du-blockchain-a-l

encore d'organiser des procédures de vote électronique sécurisées et vérifiables par tous[5]. De surcroît le protocole Bitcoin, ainsi que les nombreux protocoles qui s'en inspirent[6], permettent la programmation d'instructions sécurisées pouvant être exécutées automatiquement par des objets connectés. On qualifie ces programmes capables de transférer de la valeur de façon autonome et automatisée des « smart-contracts ». En ce sens Bitcoin et tous les protocoles qui s'en inspirent sont remarquablement adaptés à l'internet des objets et aux usages de demain. Au final, pour de nombreux spécialistes, comme Bob Greifeld[7], CEO du NASDAQ, ou encore la société IBM[8], Bitcoin et les registres blockchain ont le potentiel de révolutionner le secteur de la finance et plus généralement l'ensemble des métiers d'intermédiation: banquier, assureur, notaire, pour ne citer que les principaux. A ce propos, Dr Jens Weidmann, président de la banque centrale allemande, a très bien résumé les attentes soulevées par cette innovation de rupture lors du dernier sommet du G20 à Davos en janvier 2017 : « Développée à l'origine pour la monnaie virtuelle bitcoin, cette technologie de comptabilité distribuée, semble-t-il, s'est révélée être un outil très polyvalent. Et même les banques centrales - qui ne sont généralement pas connues pour être les premières à adopter de nouvelles technologies - font actuellement des recherches expérimentales sur l'utilisation potentielle d'une blockchain »[9].

Naturellement, face à une innovation d'une telle ampleur plusieurs questions sautent à l'esprit : comment cette technologie fonctionne-t-elle ? Qui s'en sert et pour quoi faire ? Plus généralement, derrière ces questions se cache en filigrane la problématique des opportunités et des risques liés à cette innovation. Problématique à laquelle est particulièrement sensible le législateur. En effet, comme énoncé dans le rapport d'information du sénat sur les enjeux liés au développement du bitcoin et des autres monnaies virtuelles de juillet 2014[10], il s'agit pour les pouvoirs publics de « travailler à la mise en place d'un encadrement juridique équilibré, afin d'empêcher les dérives sans compromettre la capacité d'innovation » qui résulte de ces nouvelles technologies.

Cette volonté d'adapter le droit à l'avènement des registres distribués dits blockchains et des monnaies numériques décentralisées est d'actualité. Au niveau européen on peut citer la mise en place depuis novembre dernier d'un groupe de travail sur les technologies financières (FinTech) dirigé par la Commission Européenne et composé d'experts en réglementation et d'experts techniques avec pour mission notable d'étudier la technologie des registres distribués (DLT)[11]. On peut également citer au niveau français l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse qui spécifie que l'émission et la cession de mini bons peuvent également être

---

-assemblee-nationale-pour-que-la-f.html

[5] Cf. l'article de Pierre Noizat, fondateur de Paymium, Bitcoin pour des votes gratuits et vérifiables

[6] Il existe actuellement plus de 600 protocoles dérivés de Bitcoin et ce nombre ne cesse de croître, cf. http://coinmarketcap.com/

[7] « I am a big believer in the ability of blockchain technology to effect fundamental change in the infrastructure of the financial services industry », Bob Greifeld, CEO du NASDAQ.Source : https://bitcoinmagazine.com/articles/nasdaq-push-forward-blockchain-applications-1432680278/

[8] "Blockchain technology presents opportunities for disruptive innovation. It enables global business to transact with less friction and more trust." IBM Blockchain : http://www.ibm.com/blockchain/what-is-blockchain.html

[9] "Originally developed for the bitcoin virtual currency, this distributed ledger technology, it would appear, has turned out to be a multi-purpose tool. And even central banks – which aren't typically known for being early adopters of new technologies – are currently doing experimental research on the potential use of blockchain."Source : https://www.bundesbank.de/Redaktion/EN/Reden/2017/2017_01_25_weidmann.html

[10] Par MM. Philippe MARINI et François MARC, Sénateurs : http://www.senat.fr/rap/r13-767/r13-7671.pdf

[11] https://ec.europa.eu/digital-single-market/en/blog/european-commission-sets-internal-task-force-financial-technology

inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations (autrement dit dans une blockchain), dans des conditions, notamment de sécurité, définies par décret en Conseil d'Etat.

En tant qu'acteurs de l'écosystème Bitcoin / blockchains et utilisateurs de ces nouvelles technologies nous sommes concernés au premier plan par l'évolution du droit vis-à-vis de ces innovations. A l'image du législateur, nous souhaitons une évolution du droit intelligente, équilibrée et adaptée aux nouveaux enjeux : favoriser l'innovation, prévenir et lutter contre les abus.

Dans cette perspective il semble opportun pour les acteurs de l'écosystème Bitcoin / blockchain de travailler en étroite collaboration avec les professionnels du droit. Il nous semble en particulier très important de présenter aux professionnels du droit le fonctionnement de Bitcoin et de la comptabilité par blockchain, à travers des exemples d'utilisation concrets, afin de permettre aux spécialistes du droit de travailler à la mise en place d'un cadre juridique adapté à ces nouvelles technologies et aux enjeux qu'elles soulèvent en connaissance de cause.

Dans le cadre de ce travail collaboratif, il pourrait notamment être intéressant d'étudier différents services spécifiques à Bitcoin et aux registres distribués :

- Présenter le fonctionnement d'une plateforme d'échange de crypto-monnaies et les problématiques autant techniques que juridiques qui en découlent, ou encore
- Présenter différents portefeuilles bitcoins et leur fonctionnement.
- Effectuer l'enregistrement d'un document dans la blockchain de Bitcoin, ou simplement l'envoi d'une transaction Bitcoin.

Pour conclure cette proposition, il s'agit de mettre à profit l'initiative des convergences du droit et du numérique, afin de rendre la technologie Bitcoin / blockchain et les usages qui en découlent accessibles à tous les professionnels du droit. Cette mission est d'autant plus critique que les professionnels du droit seront bientôt amenés à faire évoluer la réglementation concernant ce secteur, en plus d'avoir à répondre aux questions d'une base d'utilisateurs et d'acteurs des crypto-monnaies en forte croissance.

"Les transports intelligents "

Sébastien Martin

Maître de conférences en droit public

CRDEI, Centre d'excellence Jean Monnet d'Aquitaine

Université de Bordeaux

Depuis plusieurs années, les nouvelles technologies de l'information et de la communication ont fait leur apparition dans tous les secteurs de la vie quotidienne. Les transports n'échappent pas à cette révolution, cette dernière s'accompagnant, qui plus est, des progrès réalisés dans le cadre des systèmes de géolocalisation.

L'émergence du numérique dans le secteur des transports a apporté des évolutions majeures dans :

- l'optimisation de l'utilisation des réseaux par la multimodalité pour les transports de personnes et de marchandises
- le développement des transports, en particulier des transports publics, par l'information des usagers et la billettique
- la sécurité routière par l'amélioration de la maîtrise des moyens de transport et par l'automatisation des contrôles et la télématique routière
- la réduction des consommations d'énergie et de la pollution par les systèmes de gestion de trafic et les véhicules communicants.

L'ensemble des innovations réalisées au-delà de ces évolutions a nécessairement eu des impacts sur le cadre juridique existant et a poussé les pouvoirs publics à réagir pour adapter ce cadre juridique. En effet, il est possible que les autorités doivent organiser ce qui n'était pas prévu ou, dans d'autres configurations, autoriser ce qui était interdit.

L'étude se propose donc, dans un premier temps, d'étudier les évolutions juridiques apportées par le numérique dans le cadre des transports. A cet égard, on notera qu'elles concernent trois domaines différents :

1. l'encadrement de l'usage des moyens de transport intelligent dans l'espace public (à travers les exemples du drone ou de la voiture autonome)

2. l'encadrement des conséquences juridiques du recours aux transports intelligents, avec en particulier la question des régimes de responsabilité (à travers les exemples du drone ou de la voiture autonome)

3. l'encadrement des activités, notamment professionnelles, qui font appel aux transports intelligents (à travers les exemples de la maraude électronique ou de la gestion des flottes de transport en libre-service)

Une fois les évolutions juridiques mises en exergue, il sera possible, dans un second temps, d'identifier les objectifs poursuivis par les autorités publiques lorsqu'elles interviennent pour tenir compte des conséquences d'une innovation.

A cet égard, l'analyse pourrait faire apparaître que les législations sur le numérique dans le cadre des transports entendent tout à la fois saisir les opportunités qui se présentent et protéger les individus des risques sociaux inhérents au monde des transports. Finalement, on pourra se demander si ces deux objectifs peuvent se concilier et s'ils ne sont pas par trop contradictoires.

La mutation des opérateurs réseaux en fournisseurs de Cloud: quels enjeux pour la neutralité du net?

Nicolas Herbaut
nicolas.herbaut@labri.fr

January 8, 2017

La révolution du Cloud

Ces dernières années ont vu une explosion de l'utilisation du Cloud tant pour la gestion de l'informatique personnelle (stokage dans le cloud avec DropBox ou suite bureautique en ligne avec Google Docs), qu'aux profits des éditeurs informatiques à même de vendre leurs logiciels en tant que services, en louant des serveurs à bas coûts à des entreprises tierces spécialisées dans le Cloud.

L'utilisation du Cloud par les opérateurs de réseaux

Sous l'impulsion des opérateurs de télécommunication (Orange, British Telecom, AT&T,...), la révolution du Cloud est en train de gagner le monde des télécoms, et plusieurs efforts de standardisation sont en cours [ETS] afin de définir les normes de développements du futur "Telco-Cloud". Des études de terrains sont également en cours, afin de valider l'approche [Lab]. Ces initiatives mettent en avant la réduction pressentie des coûts d'achat et de maintenance des systèmes télécom. Les cas d'utilisation décrits dans les normes gravitent autour des fonctions traditionnelles des opérateurs télécoms: fourniture de services de voix, gestions des antennes radios, optimisation du coeur de réseaux etc.

Telco-CDN: un cas d'utilisation à risque

D'autres cas présentent la mise sur le marché de nouveaux services à valeur ajoutée pour les opérateurs de réseaux. Parmis ceux-ci, le cas du Telco-CDN[Wika] est celui qui se plie le mieux aux mutations actuelles d'Internet en réseau de distribution de contenus multimedias. En disposant des moyens de stocker à l'intérieur de leurs réseaux les fichiers les plus lourds, les opérateurs peuvent réduire les coûts liés au rappatriement longue distance des vidéos sur Internet. Un effet corrolaire et celui de la réduction du délai d'acheminement des Vidéos, entrainant une amélioration de la qualité ressentie par l'utilisateur final.

Avec ces avantages techniques et économiques clairs, la tentation est grande pour les opérateurs de trouver un relai de croissance en devenant des fournisseurs de Telco-Cloud. En permettant à des sociétés de louer une partie de leurs ressources réseaux les plus favorables à la livraison de contenu, les opérateurs réseaux s'exposent à un contournement du principe de neutralité du Net[Wikb].

Ceux-ci font profiter des entreprises tierces contre paiement, à un accès privilégié (du point de vue du réseau) à des ressources Cloud permettant d'obtenir une position avantageuse pour livrer leur contenu aux utilisateurs. Ceci s'effectue au dépend de la concurence qui ne pourrait pas payer un tel hébergement. A titre de comparaison,

c'est comme ci une compagnie d'autoroute réservait une voie aux compagnies de transport qui se fourniraient en carburant chez elle.

Objectifs de la contribution

Mes contributions scientifiques[myw] et ma thèse se basent sur ce paradigmne de livraison de contenu d'un point de vue technique et algorithmique. Je souhaiterais prolonger mes recherches par une étude légale concernant la revente par les opérateurs réseaux de services de Telco-CDN à des entreprises tierces. L'étude devrait avoir pour objectif la soumission d'un article, afin de pouvoir la valoriser au mieux dans un cadre scientifique.

References

[ETS] ETSI. ETSI Network Function Virtualization. http://www.etsi.org/technologies-clusters/technologies/nfv.

[Lab] Orange Labs. Point de présence du futur, les NGPOP. https://recherche.orange.com/une-nouvelle-generation-de-point-de-presence-le-ng-pop/.

[myw] Mes travaux de recherche. https://nextnet.top/biblio/.

[Wika] Wikipedia. Evolution des CDN. https://fr.wikipedia.org/wiki/Content_delivery_network#.C3.89volutions. [Online; accessed 8-Jan-2017].

[Wikb] Wikipedia. Neutralité de réseau. https://fr.wikipedia.org/wiki/Neutralit%C3%A9_du_r%C3%A9seau.

Thème B

« Systèmes autonomes et décision, droits fondamentaux »

Synthèse

Les discussions de ce thème ont porté sur les points suivants :

1. Définition du robot ;
2. Qualification juridique du robot ;
3. Traitements algorithmiques et aide à la décision ;
4. Droits et libertés et algorithmes.

Définition du robot

À l'heure actuelle, en dépit de multiples travaux doctrinaux, il n'existe pas de définition légale du robot. Cette tâche de définition est d'autant plus ardue que les représentations mentales du concept ont évolué dans le temps. Initialement, ce terme désignait un dispositif mécanisé pouvant exécuter des tâches de façon répétitive, à l'image des robots peintres dans les usines d'automobiles répétant de façon automatisée les gestes mémorisés, que la carrosserie soit présente ou non. Avec l'émergence des technologies numériques, le concept de robot a été étendue à la réalisation de tâches informationnelles, à l'image des « *crawlers* », ces « *bots* » (contraction de « (ro)bots ») en charge d'analyser le contenu des pages web afin d'alimenter les bases de données des moteurs de recherche. Puis, avec l'émergence de l'intelligence artificielle, le terme de robot a été étendu aux machines embarquant une capacité de décision autonome, bien que la majorité des systèmes de contrôle embarqués soit à l'heure actuelle très rudimentaire (pilotage d'un aspirateur autonome, par exemple). Cependant, commencent à apparaître des systèmes plus évolués, capables de fonctionner de façon collaborative et autonome (flottes de drones, robots collaboratifs dans certaines usines), rejoignant ainsi la vision mythologique du robot, forgée dans les années 1940-1960 par la science-fiction en s'appuyant sur des mythes plus anciens tels que celui du golem.

La qualification de robot dépend grandement des situations. Ainsi, les drones ne peuvent être considérés collectivement comme des robots, car les drones télépilotés n'en sont clairement pas : tout comme une pelleteuse mécanique ou une prothèse articulée, l'objet agit sous le contrôle direct de son opérateur humain. La qualification de robot supposerait donc une capacité minimale d'action autonome, à l'image des voitures et drones autonomes. C'est le parti pris la Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique 2015/2103(INL), qui ne vise que les robots autonomes et exclut donc les autres, évoquant même des concepts issus de la littérature tels que les lois d'Asimov. Pour autant, elle évoque aussi les drones civils, qui ne sont pas des robots autonomes. Comme on le voit, la doctrine n'est pas encore établie.

Il convient également de noter qu'il ne suffit pas de qualifier une machine de « robot » pour lui appliquer le « droit des robots ». Cette terminologie doit être abandonnée, pour deux raisons. D'une part, tout comme pour les données, il n'existe pas un droit applicable aux robots en général, mais plusieurs corpus de règles applicables à des domaines spécifiques : robots industriels, robots médicaux, voitures autonomes, drones, etc. D'autre part, parler de « droit des robots » pourrait suggérer de façon implicite que les robots puissent avoir des droits. Aussi, mieux vaut employer l'expression « droit de la robotique ».

Qualification juridique du robot

Est-il opportun de reconnaître une personnalité juridique au robot ? Une telle reconnaissance emporterait comme conséquence majeure qu'un robot puisse être titulaire de droits et d'obligations. Il pourrait les exercer en passant des contrats (par exemple, un taxi autonome qui règlerait ses frais de carburant et de réparations) ou encore en agissant en justice. À l'heure actuelle, à défaut de cas d'espèce justifiant une telle reconnaissance, il n'existe actuellement aucune raison de s'engager dans cette voie. Une telle qualification ne pourrait être retenue que s'il apparaissait qu'une entité synthétique se voie reconnaître une conscience, susceptible de lui donner une volonté capable d'être exercée en autonomie. Le terme d'« intelligence artificielle » ne doit pas conduire à surestimer les capacités des systèmes existants, ni à leur conférer des attributs tels que la « sensibilité » (qui pourrait les faire entrer dans la catégorie des « êtres sensibles » mise en œuvre dans le droit des animaux) ou des « sentiments ».

Une question de portée plus immédiate concerne les mécanismes de responsabilité qui pourraient être mobilisés en cas de dommage causé par un robot. Dans des situations particulières, on pourrait retenir la responsabilité du fait des choses, la responsabilité du fait des produits défectueux voire la responsabilité pour risque. La question parait plus délicate dans le cas des robots de combat. Ces derniers ne relèvent pas de la même problématique car ils s'inscrivent dans le droit de la guerre et le droit international des droits de l'Homme.

Enfin, des qualifications juridiques peuvent être opérées. Si la machine robotisée est assimilé en droit à une chose, cette assimilation peut être reconsidérée dans des situations particulières : lorsque des prothèses bioniques sont incorporées à l'homme, elles deviennent une partie de lui-même et bénéficient de la qualification doctrinale (d'éléments) de personnes par destination.

Traitement algorithmiques et aide à la décision

La question des traitements algorithmiques pour l'aide à la décision, abordée ici dans le cadre des systèmes autonomes, a également fait l'objet de débats lors du thème C de l'atelier, « Numérique et pratiques juridiques ».

La conception de logiciels et systèmes experts capables de prendre des décisions à la place des médecins et juristes, voire à la place des autorités publiques en matière de décision administrative, est ancienne. Cependant, la généralisation de ces systèmes conduit à s'interroger sur les avantages et limites de ces outils, ainsi que sur l'encadrement de leurs conditions d'utilisation afin de garantir l'indépendance du décisionnaire. La transparence dans le fonctionnement du système d'aide à la décision apparaît nécessaire. Son utilisateur doit être en mesure de savoir ce qu'il peut et ce qu'il ne peut pas faire pour plusieurs raisons : optimiser la qualité de la décision ; évaluer la pertinence de suivre ou non la suggestion du système ; contester une décision s'appuyant sur un algorithme décisionnel.

Les mécanismes de responsabilité pourraient être un premier encadrement de cette pratique. Or, ces derniers doivent être redéfinis. Quel régime de responsabilité faut-il appliquer à la prise de décision algorithmique ? Qui, du médecin ou du concepteur du système, sera-t-il tenu responsable ? Cette question nécessite de réfléchir de manière plus générale à l'imputation de la faute. Ces systèmes d'aide à la décision supposent de s'interroger sur la notion d'aide. À partir de quel moment passe-t-on d'une aide à la prise effective de la décision ? Aussi, comment comprendre « l'intelligence artificielle » dans le contexte de l'aide à la décision ?

Droits et libertés et algorithmes

Une forme de contrôle de la machine sur l'humain – ne serait-ce qu'à travers l'effectivité de sa liberté de penser – n'est pas inenvisageable. La hiérarchisation de la présentation de l'information (résultats de moteurs de recherche, recommandations, etc.) influe sur la manière dont l'information nous est accessible. Ce filtrage est apparemment plus développé sur les réseaux sociaux. L'algorithme EdgeRank de Facebook permet de suggérer des pages et des amis en fonction de l'affinité et la fréquentation exprimées par le score « J'aime » et les « Partages », du contenu (photos, vidéos), ainsi que de leur fraîcheur chronologique. En ne retenant que des informations en rapport avec les demandes passées des utilisateurs, et en limitant par contrecoup la possibilité d'avoir accès à des idées opposées, ces algorithmes ne constituent-ils pas un danger pour la démocratie et, plus largement, pour l'État de droit ? Ne risque-t-on pas d'enfermer l'individu dans une bulle algorithmique néfaste à la liberté d'opinion et d'expression ?

Synthèse réalisée par Élodie Annamayer à partir des éléments débattus collectivement lors de la table ronde

Proposition de contribution sur :

« La robotique autonome face au droit et à l'éthique »

Nathalie NEVEJANS

Maître de conférences en droit privé, Faculté de droit de Douai,
Centre de Recherche en Droit, Ethique et Procédures (EA n° 2471),
Membre du Comité d'éthique du CNRS (COMETS).

COMMUNAUTE D'APPARTENANCE PREFERENTIELLE :

Juridique.

PROBLEMATIQUE :

Depuis quelques années, les progrès de la robotique sont tels, que les juristes sont contraints de s'y intéresser.

Si l'ensemble de la robotique, aussi bien civile (robots chirurgicaux, industriels, de services, …) que militaire (robots de guerre, drones de guerre, …) renouvelle les réflexions, il pourrait être judicieux dans le cadre des travaux sur les « Convergences du droit et du numérique » de s'orienter plus spécifiquement vers la robotique autonome. En effet, cette dernière pose de nombreux problèmes aussi bien juridiques qu'éthiques fort délicats à aborder (responsabilité, droits fondamentaux, etc.), et qui méritent analyse au regard de son inévitable influence sur la société. La robotique autonome a d'ailleurs attiré l'attention du législateur européen, comme en témoigne le projet de résolution européenne concernant les règles de droit civil sur la robotique du 31 mai 2016.

Toutefois, l'aspect éminemment technique et scientifique de la robotique fait que, bien souvent, il est très difficile pour un juriste d'aborder ces questions. Or, seule une compréhension véritable de la robotique permet de déjouer les pièges, ainsi que les tentations de la facilité aux relents de personnalité juridique du robot.

ELEMENTS DE MA CONTRIBUTION :

Spécialiste en droit et éthique de la robotique et des technologies émergentes, et ayant participé à des évènements majeurs nationaux et européens, je me propose, dans le cadre de cette contribution, de m'attarder sur l'examen des grandes notions juridiques qui pourraient être bouleversées par l'apparition de la robotique autonome, notamment le problème de la responsabilité, puis d'orienter mon étude vers la dimension éthique qui pose de nouvelles questions, et qui touche au plus près l'homme et les droits fondamentaux.

Ayant acquis des compétences techniques et scientifiques en robotique, à côté du seul aspect juridique et éthique, j'envisage avec plaisir de contribuer aux ateliers du seul point de vue scientifique, lorsqu'il s'agira de travailler sur la notion de robotique autonome avec un langage du scientifique.

Convergences du droit et du numérique

« Droit + numérique + x = droit des robots
Inventer les inconnues... »

1°/ Parler de droit et de numérique conduit-il impérativement à parler de droit des robots ? La réponse sera sans doute nuancée, car s'il est vrai qu'une partie de la robotique repose sur le numérique, le terme de robot renvoie aussi à une réalité qui s'affranchit du numérique.

Il est vrai qu'une partie de la robotique repose sur le numérique.

En effet, le numérique peut s'entendre d'un domaine dans lequel un code, constituant une suite de numéros, sera lu par une machine qui pourra (re)produire une chose sous un format particulier ; image, son, mouvement, code nouveau...

Selon cette définition, un robot peut être compris dans le domaine du numérique car le robot repose bien souvent sur la programmation informatique, qui repose elle même sur le numérique.

Pourtant, tout robot ne repose pas forcément sur la technologie numérique.

Pour accepter cette idée, il faut adopter une définition plus large du robot, en pensant déjà aux automates, inventions mécaniques mues par des forces physiques comme l'eau ou l'air, et qui exécutent des mouvements. Selon leur apparence ; leur utilité ; leur degré de mécanisation…, l'utilisation du terme « robot » pourrait leur être applicable.

De même, il faut aussi songer à l'homme augmenté, concrétisation d'un *Homme qui valait 3 milliards*, greffant des objets à son corps à l'instar du « biohacker » *Tim Cannon* qui se fait déjà implanter des objets pour devenir cyborg. Encore, la médecine regorge d'illustrations dans lesquelles l'Homme utilise des choses articulées pour remplacer des parties de son propre corps. La littérature de fiction est rattrapée par la réalité, puisque nous ne sommes plus très loin des automates d'Héphaïstos ou de la créature du docteur Frankenstein.

Dans ces derniers exemples, les fonctionnements des « robots » s'éloignent du numérique. En effet, le message codifié n'est par toujours numérique puisqu'il peut être mécanique ou électrique[1], alors une première inconnue est déjà de savoir si la convergence du droit et du numérique peut ou non aider le juriste dans la conception d'un éventuel droit du robot ou de catégories de robots ?

2°/ Une autre inconnue s'ajoute toutefois à celle-ci. En effet, que le droit *puisse* ou non adopter une définition du robot, *doit*-il nécessairement le faire ? Autrement-dit, le robot est-il une chose si particulière que le droit doive lui accorder un statut différent des choses communes ?

Si les auteurs s'accordent généralement sur la nécessité pour l'industrie robotique de se doter d'un *charte « roboéthique »* (dont il existe déjà quelques exemples), trois conceptions principales s'affrontent tout de même sur la question des droits reconnus aux robots.

La première voudrait que le robot soit, en droit, une chose comme une autre. Ainsi, elle se

1 Bien qu'en l'état actuel des avancées techniques, le message nerveux électrique qui passe du cerveau à un membre bionique semble toujours relu par un ordinateur implanté dans ce membre.

verrait appliquer les mécanismes traditionnels du droit[2].

A l'inverse, certains auteurs verraient dans l'intelligence artificielle du robot un élément permettant de lui conférer une personnalité juridique, notamment une personnalité robot[3].

En troisième lieu, sans en arriver à une personnalité robot, une autre conception envisagerait de munir les robots de mécanismes juridiques particuliers, notamment en les dotant d'un capital pour répondre des dommages qu'ils causeraient[4].

Pour choisir une de ces solutions, le raisonnement peut alors être double.

D'une part, il faut rechercher si l'acception du robot comme une chose instaure des difficultés au regard des mécanismes juridiques traditionnels. S'il existe des difficultés, il faudra sans doute que le droit évolue, et il sera nécessaire de trouver le vecteur de cette évolution (loi ; jurisprudence...).

Mais d'autre part, si cette conception du robot-chose n'engendre pas de difficulté dans les mécanismes juridiques, le débat n'est pas pour autant clos, car il reste une autre interrogation : faut-il attendre des difficultés juridiques pour doter le robot d'une personnalité juridique, ou doit-on considérer qu'au fond, la capacité « intellectuelle » du robot en vient à le distinguer d'une chose commune, tout comme le droit a voulu distinguer l'Homme de la chose en lui donnant la personnalité juridique. Cela reviendrait à considérer que le robot a réellement une personnalité dans les faits, et de recourir à la *thèse de la réalité*[5] pour lui donner une certaine personnalité juridique.

3°/ De façon plus théorique, il conviendra enfin de trouver une nouvelle inconnue, en procédant à la recherche des fondements de la règle qui inciteraient à recourir ou non à cette thèse de la réalité. Par exemple, lorsque la science estimera le « cerveau » du robot aussi développé que celui de l'Homme, devra-t-on se reposer sur ce fondement scientifique pour le doter de la personnalité juridique, ou devra-t-on à l'inverse privilégier un fondement spirituel en estimant que seule une création divine pourrait être dotée d'une personnalité juridique supplémentaire[6]? Le fondement philosophique pourrait lui aussi être invoqué en se demandant si la conscience ; la morale ; le juste... devraient justifier la personnalité juridique des robots ou l'écarter.

Que ce soit donc du point de vue des définitions, de l'utilité ou encore des fondements, le droit des robots recèle de multiples inconnues, et il n'est pas sûr que celles-ci puissent être trouvées par un raisonnement strictement logique – juridique ou mathématique.

Pierre-François Euphrasie, doctorant en droit

2 Notamment G. Loiseau, M. Bourgeois, *Du robot en droit à un droit des robots :* Semaine Juridique Edition Générale n° 48, 24 Novembre 2014, doctr. 1231

3 A. Bensoussan, *Plaidoyer pour un droit des robots : de la « personne morale » à la « personne robot »* : La Lettre des juristes d'affaires 23 oct. 2013, n° 1134

4 Cédric Coulon, *Du robot en droit de la responsabilité civile : à propos des dommages causés par les choses intelligentes :* Responsabilité civile et assurances n° 4, Avril 2016, étude 6

5 G. Loiseau, M. Bourgeois, *op. cit.*

6 Choix qui écarterait le raisonnement par analogie, puisque ce fondement n'a pas été retenu pour la personnalité morale

Drones et robots autonomes ou télé-opérés en environnement complexe : tenue de situation, prise de décision, responsabilité et éthique

Serge Chaumette, Pr., LaBRI, Université de Bordeaux

serge.chaumette@labri.fr

Table des matières

1 Drones et drones autonomes 1
1.1 Qu'est-ce qu'un drone 1
1.2 Qu'est-ce qu'un drone autonome 2
2 Essaims de drones et essaims de drones autonomes 2
2.1 Les essaims de drones et les essaims de drones autonomes 2
2.2 Mode dégradé – mode nominal 3
3 Trois points clefs 3
3.1 Autonomie 4
3.2 Approximation du monde réel 4
3.3 Dilution de responsabilité/décision 5
Références 5

Cette contribution porte sur les systèmes autonomes communicants de type robots ou drones. Dans leurs versions les plus complexes, ils présentent la spécificité de disposer d'une intelligence embarquée leur conférant non seulement une autonomie de mouvement mais aussi et surtout une autonomie de décision, et c'est ce point qui soulève les interrogations en termes de responsabilité qui sont décrites dans cette contribution. Cette autonomie leur permet de réagir à l'évolution de leur environnement et en particulier à tout événement extérieur non prévu.

1 Drones et drones autonomes

1.1 Qu'est-ce qu'un drone

Un drone est un système sans pilote à bord et plus précisément un système télé-opéré. La notion de télé-opération absente de la terminologie initiale (on parlait de *Unmanned Aerial*

Vehicle – UAV – sans plus de précision) a été réintroduite et est aujourd'hui largement adoptée. On parle ainsi de RPAS (*Remotely Piloted Aircraft System*). On dispose donc bien toujours d'un pilote même si il n'est plus présent à bord mais déporté sur un site de pilotage.

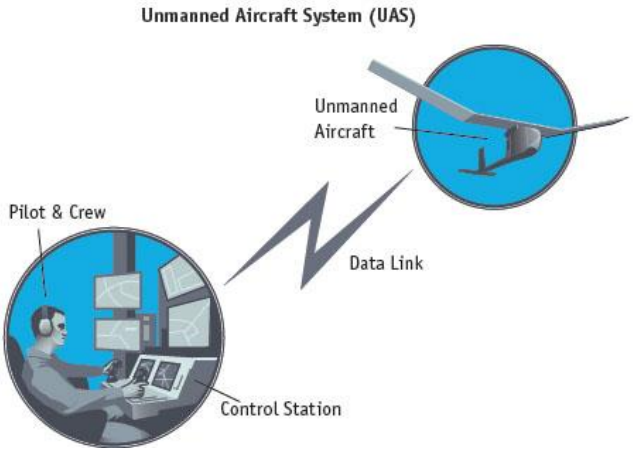


Figure 1. Système de drone

source en date du 24/04/2017 :
http://www.insidegnss.com/auto/popupimage/UAS%20illustration%20FAA%20roadmap.jpg

1.2 Qu'est-ce qu'un drone autonome

Les systèmes décrits ci-dessus sont opérationnels depuis maintenant de nombreuses années et l'étape suivante en terme d'évolution technologique est la notion de drone autonome. C'est elle qui nous intéresse dans cette contribution. Il ne s'agit ici plus seulement de déporter le pilote mais purement et simplement de se passer de pilote. Le drone doit alors disposer d'une intelligence embarquée lui permettant de s'adapter à son environnement et à l'évolution de celui-ci.

Ainsi, le concepteur du système n'est plus nécessairement en mesure de prédire toutes les décisions qui seront prises par l'engin au cours de sa mission.

2 Essaims de drones et essaims de drones autonomes

2.1 Les essaims de drones et les essaims de drones autonomes

Une étape additionnelle consiste à constituer des essaims de drones [3, 4] afin de supporter des fonctionnalités supplémentaires [2] (« *Le tout est plus que la somme de ses parties* » (Aristote)) : résilience, multi-capteurs, vol continu, collaboration multi-autorités, etc. De la même façon qu'un drone peut être autonome, un essaim de drones peut lui aussi être autonome. Cela lui confère une adaptabilité incomparable qui lui permet de réaliser des missions complexes [5, 6, 7, 8].

En revanche, la complexité et la non prévisibilité du comportent vues pour un drone autonome unique prennent naturellement ici une dimension indéniablement plus importante.

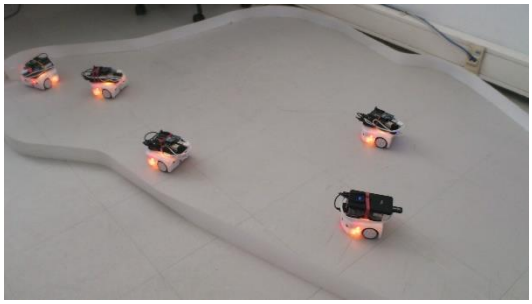


Figure 2. Un essaim de robots autonomes

Figure 3. Un essaim de drones autonomes

2.2 Mode dégradé – mode nominal

Dans une approche de type essaim, le mode dégradé est le mode de fonctionnement standard [1]. Cette opinion est assez largement partagée. Par exemple, Werner J.A. Dahm, de l'*Arizona State University* dans sa présentation à *AIAA Guidance, Navigation, and Control Conference* qui a eu lieu du 19 au 22 août 2013 à Boston , Massachusetts aux Etats-Unis a dit : "*classical separation between "nominal operation" and "faults" becomes untenable; system is continuously operating under faults".* En effet, dans un système d'envergure (on parle de plusieurs centaines de drones), la probabilité de se trouver face à une panne (au sens large) est très importante.

Pour ce qui nous concerne ici, les fautes majeures sont la perte d'un appareil ou des communications entre appareils. Ces pertes ne sont plus des erreurs, mais des événements comme les autres dont la survenue doit être prise en compte dès la conception des systèmes considérés. Une conséquence importante est qu'il n'est pas possible de re-exploiter dans un tel contexte une application non prévue pour ce cadre. Un travail de re-conception et de redéveloppement complet du produit doit être réalisé pour prendre ces contraintes en considération.

Les architectures résultantes prennent en compte cette spécificité en ne faisant aucune hypothèse sur l'environnement de chaque appareil pris individuellement ; pas d'hypothèse sur la présence ou non d'autres engins et sur les capacités éventuelles de communication avec eux. Les missions globales mises en œuvre par un essaim sont ainsi l'émergence d'un ensemble de comportements locaux, « à l'aveugle », des engins qui le composent.

3 Trois points clefs

Trois points clefs semblent fondamentaux pour bien cerner les enjeux de ces systèmes, points dont les conséquences doivent être cadrées juridiquement : autonomie, approximation du monde réel, dilution de responsabilité/décision.

3.1 Autonomie

Le système global résultant est un système autonome. En ce sens il prend lui-même les décisions relatives à son évolution en fonction d'informations collectées dans son environnement et de procédures codées (programmées) en interne. Néanmoins, même si ces décisions ont été programmées, l'espace d'évolution du système (au sens mathématique d'espace de solutions) n'est pas nécessairement connu. L'évolution reste en tout cas non déterministe et il peut y avoir émergence de phénomènes globaux ou de comportements non imaginés par les concepteurs/développeurs d'un tel système.

Ainsi, le système présente un comportement par nature non déterministe en évoluant dans un espace de solutions possiblement non totalement connu. En d'autres termes « il prévu pour fonctionner dans un environnement non prévu ». Qui est alors responsable des problèmes éventuels causés par ce degré de liberté élevé du système ?

3.2 Approximation du monde réel

De sorte à être résilients ces systèmes ne peuvent faire aucune hypothèse sur leur environnement. En particulier ni la présence d'autres engins de l'essaim ni la capacité à communiquer avec eux ne peuvent être supposées. Ainsi, la seule fonctionnalité dont dispose un appareil pour assurer la collaboration est une primitive de communication de type diffusion asynchrone. Il ne peut que diffuser une information alentour, mais en aucun il ne saura si elle a été reçue par un autre engin. Malgré la faiblesse ce cette fonction il n'en reste pas moins possible de construire des applications complexes.

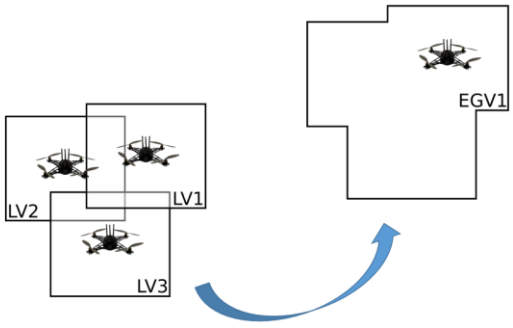


Figure 4. Construction d'une image globale estimée à partie d'images locales

Le principe de base consiste à construire au sein de chaque appareil une représentation (une image) du monde réel. Le processus est le suivant. Chaque engin diffuse alentour l'image qu'il

se fait du monde global (*Estimated Global View - EGV* -). De manière symétrique il peut recevoir un certain nombre d'images globales construites par d'autres engins de la flotte. Dans ce cas, il fusionne (selon un processus qui peut être complexe) les images reçues et la sienne afin de construire une nouvelle image globale. Un point fondamental est que cette image globale est essentiellement toujours fausse (sauf pour la partie locale, *Local View, - LV* -). En effet, entre l'instant où un engin diffuse l'image globale qu'il se fait du monde et le moment où elle est reçue par un autre engin puis fusionnée, le monde a par nature évolué. Les informations assemblées peuvent donc être fausses.

Chaque engin dispose donc d'une approximation du monde réel, possiblement en grande partie fausse et avec laquelle il doit travailler pour réaliser sa mission.

Ainsi, le système est conçu pour fonctionner avec des informations fausses. Quelle est alors la responsabilité de celui qui a consciemment conçu un système dont il sait que les données qu'il exploite sont fausses ?

3.3 Dilution de responsabilité/décision

La chaine de commandement/contrôle d'un système autonome peut être longue et on pourrait penser que la responsabilité des intervenants s'en trouve diluée. Néanmoins, et cela est expliqué dans un article du Général Sartre [9], il y a certes dilution mais pas rupture de chaine comme dans un système plus classique. Concrètement dans un système militaire plus conventionnel (sans drone), un pilote dans un avion de chasse prend *in fine* la décision d'ouvrir le feu ou pas. Dans un système de drones, les informations remontées à distance permettent au politique d'être au plus près de la décision, lui réattribuant la responsabilité par exemple d'ouvrir le feu ou pas, même si physiquement c'est le télé-pilote qui le fait. Dans l'approche drone autonome, que devient cette chaine de responsabilité. Qu'est-ce qui est de la décision humaine et de l'ordre de la décision autonome ?

Ainsi, il y a certes une chaine de responsabilité/décision mais qui se trouve en quelque sorte brisée au denier niveau, dans la prise de décision autonome de l'engin. Quel peut être l'impact de cette rupture au niveau de la responsabilité des intervenants ?

Références

[1] Serge Chaumette. Failure is the nominal operation mode for swarms (of drones): reasons and consequences . *Conference on Complex Systems (CCS2016). Satellite Session - Swarming Systems: Analysis, Modeling & Design.*, Sep 2016, Amsterdam, Netherlands.

[2] Serge Chaumette. A swarm of drones is more than the sum of the drones that make it up. *Conference on Complex Systems (CCS2016)*, Sep 2016, Amsterdam, Netherlands.

[3] Serge Chaumette, Jin Hyun Kim, Kamesh Namuduri, James P.G. Sterbenz. UAV Networks and Communications. Cambridge University Press, 2017.

[4] Serge Chaumette. Chapter 8: Cooperating UAVs and Swarming. Kamesh Namuduri, Jae H. Kim, Serge Chaumette, and James P.G. Sterbenz. *UAV Networks and Communications*, Cambridge University Press, 2016.

[5] S. Chaumette, R. Laplace, C. Mazel, R. Mirault, A. Dunand, Y. Lecoutre, and J. Perbet. CARUS, an operational retasking application for a swarm of autonomous UAVs : first return on experience. In *IEEE Military Communication Conference, 2011. MILCOM 2011*, pages 2003–2010. IEEE, 2011.

[6] Vincent Autefage, Serge Chaumette, Damien Magoni. Distributed Collaborative System for Heterogeneous Swarms of Autonomous Mobile Robots. IEEE. *CFIP-NOTERE 2015*, Jul 2015, Paris, France.

[7] Vincent Autefage, Arnaud Casteler, Serge Chaumette, Nicolas Daguisé, Arnaud Dutartre, et al.. ParCS-S2: Park Cleaning Swarm Supervision System - Position Paper. *Proceedings of the 9th AIRTEC International Congress (AIRTEC 2014)*, Oct 2014, Franfurt, Germany.

[8] Bouvry, Pascal; Chaumette, Serge; Danoy, Grégoire; Guerrini, Gilles; Jurquet, Gilles; Kuwertz, Achim; Müller, Wilmuth; Rosalie, Martin; Sander, Jennifer. Using Heterogeneous Multilevel Swarms of UAVs and High-Level Data Fusion to Support Situation Management in Surveillance Scenarios in *2016 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems, MFI 2016* (2016, September 19).

[9] Patrice Sartre, Général de Brigade. *La télé-opération et l'autonomisation des drones : quels problèmes éthiques ?* Tribune numéro 558, 17 juillet 2014.

Projet de contribution :

Convergence du droit et du numérique

IMPLICATIONS JURIDIQUES DE L'EMERGENCE DES ARMEMENTS AUTONOMES ET SEMI-AUTONOMES

Julien ANCELIN

Les évolutions technologiques dans le domaine de l'armement bouleversent les catégories et méthodes classiquement employées par le droit (qu'il soit interne ou international et européen). L'autonomie des moyens de sécurité et de défense constitue un paramètre nouveau nécessitant l'adaptation de règles souvent anciennes ou adoptées pour faire face à des situations d'urgence.

Le présent projet de contribution vise à la réalisation d'une étude sur les implications juridiques du développement des systèmes d'armements autonomes et semi-autonomes. Cette catégorie émergente, dans le mouvement de développement exponentiel de la robotique, provoquera des **mutations structurelles** de grande ampleur au sein du droit positif.

Les armes autonomes et semi-autonomes soulèvent de nombreux défis (qu'une analyse croisée menée par un spécialiste du droit et un spécialiste du numérique permettra d'éclairer) :

. (1) Les **classifications classiquement** rencontrées en matière d'armement vont apparaitre inopérantes à en saisir les caractères innovants. **L'autonomie**, plus ou moins étendue en fonction de l'évolution envisageable de la technique, des drones et des SALA aboutira au dépassement de la dichotomie armes classiques/armes de destruction massive. Les commentateurs considèrent que nous faisons face aux prémices d'un bouleversement similaire à celui entrainé par la mise au point de la poudre à canon ou encore à celui consécutif au contrôle de l'atome.

. (2) Les options normatives existantes en matière de **réglementation de la conception, de l'usage et de la destruction** des armements témoignent de réelles faiblesses. Le choix d'un encadrement fondé sur des équilibres anciens est limité et défaillant (à titre d'exemple, les opérations de lutte contre le terrorisme ou de maintien de la sécurité publique au soutien de drones soulèvent des difficultés en matière d'application du *jus in bello* ou de protection des droits fondamentaux). L'option de l'interdiction n'est, pour le moment, pas envisageable et seul un petit groupe d'Etat à la Conférence du désarmement de Genève l'envisage. L'étude croisée du droit et du numérique permettra de dégager des solutions

précise aptes à porter des pistes pertinentes d'évolution du droit positif

. (3) Les **garanties d'effectivité** du droit apparaissent inadaptées face aux conséquences de l'utilisation des drones ou des robot-tueurs. L'autonomie amènera à repenser les règles de la responsabilité (tant interne, qu'internationale). Les mécanismes de vérification employés en droit du désarmement devront être adaptés aux spécificités techniques des armes concernées afin d'éviter les pièges susceptibles d'être tendus par des pratiques de contournement informatique (*hacking* notamment).

Ces trois éléments d'analyse constituent une illustration des enjeux posés par l'émergence de la robotisation de l'armement et pourront constituer le cadre d'une analyse croisée. Ils ne sont toutefois pas exclusifs de l'étude d'autres aspects destinés à éclairer la thématique générale choisie dans le cadre du projet de recherche auquel se rattache la présente proposition de contribution.

Atelier « Convergences du Droit et du Numérique » - Université de Bordeaux - 2017

Sens et implications des systèmes algorithmiques d'aide à la décision (en matières médicale et judiciaire) ?

Proposition de contribution de Sonia Desmoulin-Canselier
Docteur en droit, CR CNRS, UMR 6297 DCS (Université de Nantes/CNRS)
Membre du programme **DataSanté : http://bigdatamed.hypotheses.org/**

Les décisions médicales et judiciaires sont le résultat de processus particulièrement complexes, mêlant savoir, savoir-faire et savoir-être. Elles ont notamment pour points communs de nécessité le traitement d'informations très hétérogènes en vue d'une action, mais aussi d'assumer une fonction traditionnellement associée aux qualités d'humanité et d'indépendance. De par leurs caractéristiques, elles paraissent donc éloignées de la pure rationalité algorithmique, surtout lorsqu'elle est intégrée dans un programme informatique. Pourtant, le projet de concevoir des systèmes experts ou des systèmes informatiques capables de se substituer aux juristes et aux médecins est formulé depuis plus de quarante ans (Buchanan & Headrick 1970). Ce projet peut s'appuyer sur deux arguments forts. Le premier est l'importance conférée aux données dans les deux domaines : état de l'art médical d'un côté, état du droit textuel et jurisprudentiel de l'autre servent à étalonner la décision. L'exploitation de ces données est donc un point important du processus décisionnel. Le second argument a trait au souci d'égalité de traitement (des citoyens, des justiciables et des patients) : les inquiétudes vis-à-vis des capacités individuelles de chaque professionnel ou à l'égard des inégalités territoriales (entre juridictions ou entre établissements hospitaliers) conduisent à rechercher des vecteurs d'harmonisation. Les systèmes numériques décisionnels pourraient constituer la solution. Derrière des terminologies changeantes – systèmes experts, systèmes d'aide à la décision, « intelligence artificielle » –, il s'agit de formuler une suggestion considérée comme la solution optimale en l'état des données disponibles (dans les bases de données concernées : médicales ou juridictionnelles). Pour certaines tâches, l'objectif semble désormais techniquement réalisable. Qu'il s'agisse d'établir un état du droit applicable ou un diagnostic, un pronostic sur les chances de succès d'une prétention ou d'une thérapie ou une projection sur les risques de récidive (pénale ou pathologique), les offres de service se multiplient. Le logiciel Waston d'IBM est une illustration édifiante de ces « intelligences artificielles » mises au service de toutes sortes de décideurs sans égard apparent pour la spécificité des champs d'application concernés. Ainsi, l'argument de vente promet, dans le domaine de la santé, « d'analyser toutes les données rassemblées autour d'un patient : symptômes, découvertes, remarques du praticien, entrevues avec le patient, précédents familiaux. L'ordinateur analytique peut ainsi engager avec le professionnel une discussion collaborative dans le but de déterminer le diagnostic le plus vraisemblable et les options de traitement. - Dans le domaine de la radiologie, les capacités analytiques de Watson pourront permettre de repérer sur des IRM des anomalies imperceptibles à l'œil humain. - Dans le domaine de la cancérologie, la technologie de Watson pourra être utilisée afin de trouver un compromis en examinant les avantages et inconvénients d'un traitement contre le cancer et les solutions de dépistage ». La rhétorique communicationnelle témoigne de ce qu'il s'agit de faire jouer à cet outil décisionnel le rôle d'un « partenaire de collaboration ». Le même algorithme est mis au service des décideurs – privés ou publics – dans le domaine juridique. Il s'agit alors de leur permettre de « répondre aux questions posées » quasi instantanément : « Les capacités analytiques de Watson peuvent permettre d'apporter une réponse immédiate à des questions touchant une large gamme de sujets: " Quelles sont les règles de plan d'occupation des sols pour construire un nouveau porche ? ", " Cette taxe s'applique-t'elle à moi ? ", " Quelle est la meilleure façon d'obtenir un Visa ? " ».

De fait, le cerveau humain ne peut concurrencer cette capacité de traitement rapide de données massives. Avec l'avènement du Big Data et les perspectives d'analyses quantitatives offertes par l'accessibilité accrue des immenses bases de données publiques, la force de conviction de ces innovations s'accroît. Les masses de données qui deviennent accessibles et pourraient être utiles sont sans cesse plus nombreuses, tandis que les hommes en charge de soigner, de défendre ou de juger sont contraints par des impératifs de temps et des injonctions de limitation des coûts. Aux perspectives d'optimisation économiques, s'ajoutent des arguments d'amélioration des décisions notamment par leur harmonisation par-delà les capacités humaines individuelles. Cependant, la mise en algorithme de la décision médicale, comme de la décision judiciaire, ne va pas sans susciter doutes et interrogations.

Force est de constater que les expériences passées de développement de l'informatique décisionnelle en matière médicale et judiciaire se sont plutôt soldées par des échecs (Bourcier 2007, Sybord 2016). Ce résultat est-il directement et exclusivement lié aux insuffisances techniques des outils jusqu'alors disponibles ? Dans cette optique, il faudrait parler d'échec relatif des systèmes experts – terminologie datée désignant des outils dépassés – ne présageant nullement du succès des systèmes algorithmiques d'aide à la décision. Ne faut-il pas cependant, aussi, tenir compte de la dimension psycho-sociale de ces professions particulières officiant dans le domaine du soin et de la justice ? Aux arguments valorisant l'innovation au service de l'efficacité juridique et médicale sont opposés la défense de la spécificité des métiers du droit et de la médecine, impliquant des procédures certes expertes mais aussi très humaines. Pourrait-il y avoir un *ethos* du médecin et du juge, irréductiblement résistant à une rationalité exclusivement numérique ? Par-delà l'importance des interactions humaines qui se déroulent en consultation ou en audience, les professions médicales et judiciaires sont indéniablement attachées à leur indépendance, ce qui pose la question de la transparence des algorithmes utilisés pour les aider. Il ne faut pas négliger non plus le contexte dans lequel se déploie les nouveaux outils d'aide à la décision : ils rencontrent en effet les injonctions gestionnaires de management des établissements de soin et des juridictions et leur usage ne peut, de ce fait, prétendre être totalement neutre.

Les questions de responsabilité et de perte d'autonomie du décideur vis-à-vis d'un outil dont il ne comprend que partiellement le fonctionnement, les limites et les capacités se font pressantes. Si les algorithmes logiques (comme formalisation de suites d'étapes en vue de la résolution d'un problème), les barèmes et les échelles sont déjà utilisés, les algorithmes numériques d'aide à la décision semblent représenter un saut qualitatif inédit. Comment les utilisateurs peuvent-ils apprécier la valeur d'une suggestion ou d'un résultat dont ils ne comprennent ni les prémisses ni le fonctionnement ? Comment devront-ils demain justifier ou motiver le fait de s'écarter de la préconisation algorithmique ? Comment pourront-ils motiver cet écart s'ils ne perçoivent pas les véritables apports et limites de l'algorithme et du résultat ?

Dans ce contexte, il paraît crucial de prendre la mesure du sens et des implications du recours aux algorithmes d'aide à la décision en matière médicale et judiciaire. Ceci passe par l'élucidation interdisciplinaire de plusieurs difficultés.

Les premières sont conceptuelles : comment replacer les nouveaux outils d'aide à la décision dans la succession des innovations et des pratiques (pour éviter l'effet de fascination et de perte de repère) ? Peut-on encore parler de systèmes experts ou l'avènement du big data et des systèmes auto-apprenants représentent-ils un saut conceptuel impliquant la création d'une nouvelle catégorie (autonomie ou système expert amélioré) ? « L'intelligence artificielle » est-elle un concept générique recouvrant différentes approches et méthodes de mimétisme et simulation de raisonnement humain ou est-ce une notion fermée renvoyant à une approche précise ? Quelle définition retenir au regard de quel objectif pour des termes et des expressions comme : système expert, algorithme, « aide à la décision », *machine learning* (apprentissage automatique autonome), intelligence artificielle)

Les secondes sont théoriques : Quelle incidence des logiques numériques sur des modes de pensée et des pratiques ? Quelle influence de la logique managériale dans la mise en place des logiciels experts ? Quelle compréhension et quelle réception de la « rationalité algorithmique » par les usagers : professionnels, patients, clients et justiciables?

Les troisièmes sont pratiques : quelle place pour l'acclimatation/l'adaptation de la pensée informatique dans ces champs d'application ? Comment rendre compte du travail de modélisation à l'œuvre, afin de rendre compréhensible les atouts et les limites de l'outil pour un utilisateur non informaticien ? Quelle autonomie du décideur et quelles conditions d'usage pour optimiser les bénéfices et non induire un déplacement impliquant une forme de démission du médecin ou du juriste face à la logique algorithmique ? Quelle

Alors que la Loi n° 2016-1321 pour une République numérique du 7 octobre 2016 a prévu l'adoption d'un décret en vue de faire figurer la « mention explicite de l'utilisation d'un traitement algorithmique dans le cadre d'une décision administrative » et la « possibilité pour l'usager d'en demander les principales règles » et alors que la Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)) souligne qu'il « est nécessaire d'intégrer des garanties et des possibilités de contrôle et de vérification par l'homme dans les processus décisionnels automatiques et algorithmiques » et « insiste sur le principe de transparence, à savoir qu'il devrait toujours être possible de fournir la justification rationnelle de toute décision prise avec l'aide de l'intelligence artificielle qui est susceptible d'avoir une incidence importante sur la vie d'une ou de plusieurs personnes », il est devenu plus que crucial qu'informaticiens, juristes et médecins entrent en discussion pour éclairer les conditions de conception et d'usage des algorithmes d'aide à la décision. Derrière le mot d'ordre de la « transparence », l'enjeu crucial est bien d'assurer une médecine et une justice humaines.

QUELLES LIMITES JURIDIQUES AUX ALGORITHMES PREDICTIFS ?

Rose-Marie BORGES

IRPI, Paris II Panthéon-Assas

Chercheur associé au CMH, Université d'Auvergne

Les algorithmes prédictifs sont aujourd'hui au centre de nombreuses préoccupations d'ordre juridique et éthique. Ils sont en effet présents dans de nombreux domaines du quotidien, qu'il s'agisse de marketing, de sécurité ou de médecine.

Les domaines très divers utilisant des algorithmes montrent un usage également divers de ceux-ci : certains d'entre eux ont une fonction de classement qui gère des priorités (recommandations, moteurs de recherche, logiciels d'affectation de candidats…) alors que d'autres ont davantage une fonction de catégorisation (ciblage publicitaire, recherche de terroristes, malades…). Si ces différents algorithmes ont des usages distincts, ils peuvent cependant avoir une influence importante sur nos vies : nous accorder ou refuser un prêt, nous rendre suspects d'infractions ou nous prédire une maladie que l'on aura peut-être jamais. Ils fonctionnent grâce à la multitude de données auxquelles ils ont accès et qui constituent autant de critères clairs ou cachés, dont l'influence n'est pas neutre. Une grande partie des données utilisées peut être qualifiée de données à caractère personnel. Parmi ces données à caractère personnel, certaines constituent également des données sensibles, dont le traitement est normalement soumis à autorisation. L'utilisation de telles données peut engendrer un détournement de finalité de celles-ci. L'utilisation de données à des fins d'analyse prédictive peut induire une prise de décisions produisant des effets juridiques à l'égard d'une personne, grâce à la détermination d'un profil.

Un encadrement juridique de ces pratiques doit sans doute être envisagé mais se pose alors la question de la forme de cet encadrement. Cette contribution se propose de réfléchir à différents aspects des algorithmes prédictifs pouvant avoir un impact sur leur régime juridique, même si le champ des questionnements est beaucoup plus vaste :

- Tous les algorithmes doivent-ils être traités de façon identique ? Peut-on définir des catégories d'algorithmes et sur quels critères fonder ces catégories ?
- Quel régime de responsabilité appliquer à la prise de décision fondée sur une analyse algorithmique ? Ainsi, un médecin réalisant un diagnostic au moyen d'un outil de prédiction est-il déchargé de toute responsabilité ? Qui est responsable d'une erreur dans la détermination du niveau d'urgence en vue de la prise en charge d'un patient au regard d'une analyse prédictive ? Comment encadrer ou limiter cette responsabilité ?

- Lorsque l'utilisation d'un algorithme conduit à une prise de décision, le professionnel est-il encore tenu d'une obligation de conseil ou la confiance en la technologie prime-t-elle sur tout (en matière bancaire par exemple) ?
- Qu'en est-il de la preuve de la véracité des résultats obtenus grâce à des algorithmes prédictifs : comment assurer la transparence des critères utilisés pour aboutir à ce résultat ? …

Les faces cachées du numérique et de la nouvelle technologie

Il y a 25 ans, le numérique était quasiment inexistant. L'équipement basique des foyers était le téléphone filaire, le domaine de la musique avec le CD et le clavier à touches numériques. A cela s'ajoute les équipements ménagers électriques. Le téléphone mobile existait mais il était réservé à une minorité ou bien aux usages militaires. Sont arrivés les réseaux numériques au cours des années 90. Ils avaient commencé leur essor dans les années 1950 avec la cybernétique, puis, dans les années 1970, des réseaux entre universités ou entre sites militaires s'étaient développés. C'est dans les années 1990 que tout bascula : le premier navigateur internet grand public Netscape Navigator sortit. Il ouvrait les portes d'un monde virtuel encore inconnu. Au départ on comptait uniquement 130 sites. Mais en quatre ans à peine, le nombre de sites explosa : plus d'un million ont été recensés ; Amazon fut fondé en 1999, et le géant Google en 1998. Cela a eu pour conséquences la création de nouveaux produits et applications (géolocalisation,etc...).

C'est à la faveur de ces innovations technologiques que se diffusa progressivement un discours promettant l'émergence d'une nouvelle économie, immatérielle : l'information. Ainsi les technologies de l'information et de la communication (TIC) deviennent dès lors omniprésentes.

Cette tendance du numérique pose plusieurs questions quant à la liberté des utilisateurs et notamment celle de leur vie privée (I). Mais le numérique cache un tout autre problème celui de l'impact sur notre environnement (II).

I- L'impact du numérique sur les libertés fondamentales : la vie privée

En prenant l'exemple d'internet, à chaque clic l'utilisateur laisse des traces, qui sont des données transmises au site en question qui nourrissent le Big Data. Les data sont le pétrole du 21 ème siècles. Elles circulent, elles sont stockées et exploitées. Les données sont enregistrées en permanence et vendues. Ainsi les vitrines sur internet s'adaptent au client : il sera orienté directement vers des publicités se référant aux dernières recherches effectuées. C'est une pratique courante de Facebook et sa principale source de revenu.

Voici un exemple qui permettra de comprendre comment les données sont utilisées: un utilisateur cherche à acheter une commode et consulte plusieurs sites internet, automatiquement dès qu'il se connectera sur internet il recevra des publicités ciblées illustrant des commodes. Aucune publicité n'arrive par hasard. Il est facile de savoir si la personne est un homme ou une femme, son âge. Si les sites internet sont gratuits, c'est que nous sommes le produit ! Cette méthode de collecte de données porte atteinte à la liberté des utilisateurs. Ainsi, il existe de nombreuses condamnations du CNIL pour violation de la vie privée. Le géant Google été condamné pour violation de la vie privée à de nombreuses reprises sur le fondement de la loi informatique et Libertés. En effet, la

société procède depuis plusieurs années à une collecte massive de données sur les réseaux wifi dans le but d'offrir des services de géolocalisation. Toutefois, il a été constaté par la CNIL que des données personnelles sont collectées : courriels, mots de passe, adresses de sites sur lesquels naviguaient les internautes concernés.

Il est évident que l'informatique et les nouvelles technologies intègrent de nouvelles thématiques en matière de droit : celle des fichiers informatiques, de la surveillance, du Biga Data. Il est nécessaire de légiférer très rapidement dans ce domaine pour éviter que les libertés fondamentales soient bafouées. La question de l'ère numérique amène à étudier son autre face cachée : celle de l'impact sur l'environnement.

II- L'impact du numérique sur l'environnement :

En 2008 l'entreprise américaine de conseil et d'analyse Gartner Inc, spécialisée dans les nouvelles technologies, relève que le secteur des TIC est à l'origine d'une quantité de gaz à effet de serre comparable à celle produite par l'aviation. Le secteur contre attaqua rapidement en expliquant que le déploiement des TIC peut permettre de réduire les émissions de gaz à effet de serre de 15 à 30% d'ici 2020. Pourtant, les TIC ont de véritable impacts environnementaux. Et que doit on dire des déchets des équipements électriques et électroniques (DEEE). En effet, en plus de la pollution occasionnée par les émissions de gaz à effet de serre, le secteur des TIC produit aussi d'énormes quantités de déchets. Le Programme des Nations Unies dans son rapport *From Waste to Ressources, 2009* a estimé la production globale de déchets électriques et électroniques à environ 40 millions de tonnes par an. Elle est essentiellement le fait de l'Europe, des Etats Unis, et de l'Australie. Cette masse de déchets représente une file de 20 000 kilomètres, chargés sur des camions de 40 tonnes et de 20 mètres de long. Pour l'Union Européenne l'estimation est de huit kilogrammes de déchets TIC par personne et par an. En France, en incluant certains appareils électroménagers dans les déchets TIC, on arrive à 24 kilogrammes. 80% des déchets de ce type viennent des ménages, 20% des entreprises. En 2020, la quantité de DEEE pourrait être multipliée par un facteur de 2,7 à 7 par rapport à l'an 2000.

Les facteurs principaux de cette croissance sont la pénétration toujours plus forte des produits dans la vie quotidienne, le renouvellement et l'évolution technique qui déclasse les anciens produits, et l'insertion des TIC dans les produits les plus divers : voitures, vêtements etc. Il faut ajouter que les DEEE sont toxiques et difficilement recyclables du fait de leur composition. Les matériaux fréquemment utilisés sont : le mercure, plomb, cadmium, chrome, PVC. Les DEEE représentent un poids dont cherchent à se débarrasser à moindre coût les pays développés. Il est dans cette situation compréhensible que ces DEEE soit exportés dans les pays du tiers monde. Très

tôt des ONG ont pointé du doigt ce phénomène. Un rapport du centre national d'information sur les déchets (CNIID) publié en 2010 résume clairement la situation. *« Environ la moitié des 20 à 50 millions de tonnes des DEEE produits dans le monde chaque année alimentent les économies informelles des pays du Sud, essentiellement l'Asie et l'Afrique, autour du démantèlement des appareils et du recyclage rudimentaire des métaux précieux, avant de finir dans des décharges sauvages. »* Les conditions de recyclage et d'élimination sont souvent désastreuses. Les ouvriers travaillent sans masque et sont souvent des enfants. De nombreuses études attestent d'une pollution importante de nombreux sites dans les pays du sud.

Réchauffement climatique, épuisement des ressources naturelles, pollution, les Etats veulent agir et pourtant les DEEE ne cessent d'augmenter. Face à une politique de croissance il est difficile de pouvoir freiner le nombre de DEEE. Ainsi le recyclage doit être l'élément clé.Le droit international met en avant la volonté de prendre en charge ce problème en mettant l'accent sur le recyclage dans les pays développés. Toutefois, les seules actions internationales ne sont pas suffisantes. Il est nécessaire que chaque Etat établisse des lois régissant ce domaine et met en place des politiques environnementales en faveur de la minimisation des déchets dangereux.

Sources bibliographiques :

FLIPO Fabrice, La face cachée du numérique : l'impact environnemental des nouvelles technologies, L'échappée, Montreuil, 2013.
HENNETTE-VAUCHEZ Stéphanie, ROMAN Diane, Droits de l'Homme et libertés fondamentales, Dalloz, Paris, 2013
PRIEUR Michel, Droit de l'environnement, Paris, Dalloz, 6ème édition, 2016.
WEBER Marc, La gestion des déchets industriels et ménagers dans la Communauté européenne : étude de droit communautaire, Comparativa, Genève, Librairie Droz, 1995.

Rym FASSI FIHRI
Doctorante contractuelle en Droit public à l'Université de Bordeaux (33)
Sujet de thèse : « *La protection constitutionnelle des droits fondamentaux à l'épreuve de la numérisation globale des données personnelles. »,* sous la direction de Mr le Professeur Mélin- Soucramanien et Mme Pauline Gervier.
fassi-fihri.rym@laposte.net

Thème proposé : « Le contrôle de l'homme par les algorithmes ».

L'Internet représente la facette la plus rayonnante de la dimension sociale de l'informatique et de ce que l'on nomme aujourd'hui la « société de l'information et de la communication ». Il s'agit incontestablement d'un nouveau moyen d'exercice des libertés fondamentales : L'Internet est un nouveau moyen d'expression, d'information, de communication, mais aussi de protection de la vie privée dans sa dimension développement des relations avec ses semblables.

Mais les réseaux connectés constituent un instrument à double tranchant : en tant qu'espace de liberté, ils « libèrent », en tant qu'espace algorithmique ils « enferment ».

Le contrôle de l'homme -ou du moins de sa liberté de penser- parait possible grâce aux algorithmes permettant d'attribuer à chaque recherche un score qui va déterminer sa pertinence et sa position dans les résultats de recherche. Le contenu de la recherche étant hiérarchisé, la manière dont nous recevons l'information est ainsi contrôlée. En ne retenant que des informations en rapport avec les demandes passées des utilisateurs, ces algorithmes constituent un danger pour la démocratie et plus largement, pour l'Etat de droit.

Ne risque-t-on pas d'enfermer l'individu dans une bulle algorithmique néfaste à la liberté d'opinion et d'expression ? Ces algorithmes sélectifs anéantissent en effet la possibilité d'avoir accès à des idées opposées aux nôtres, comme l'a exposé la rédactrice en chef du journal anglais The Guardian, Katharina Viner. En effet, les journaux et les politiciens pro-Brexit auraient accumulé les fausses informations pendant la campagne électorale, largement partagées sur la toile.

Ce filtrage est apparemment plus développé sur les réseaux sociaux. L'algorithme EdgeRank de Facebook permet de suggérer des pages et des amis en fonction de l'affinité et la fréquentation exprimées par le score « J'aime » et les « Partages », du contenu (photos, vidéos), ainsi que de la fraicheur chronologique.

Il semble qu'au-delà des données « traditionnelles » (données nominatives) ce sont désormais les traces informatiques qui sont collectées. Les réseaux sociaux et l'Internet permettent une « publicisation de soi » facilitant la collecte massive de traces laissées par les individus du seul fait de leur passage, traces abandonnées avec ou sans consentement. Grâce aux algorithmes, les informations susceptibles d'être traitées sont alors quantitativement et qualitativement plus intéressantes pour les pouvoirs publics et pour les entreprises privées.

Dès lors, il s'agirait de se questionner sur les solutions techniques et juridiques existantes permettant de rompre avec ce fatalisme technologique. Existe-t-il des moyens informatiques pour contrer ces algorithmes ? Est-il possible de les encadrer juridiquement ? Alors que le numérique a envahi nos vies quotidiennes, nombreux sont ceux qui ne disposent pas de connaissances suffisantes pour devenir de véritables « citoyens du numérique ».

Thème C

« Numérique et pratiques juridiques »

Les discussions de ce thème ont porté sur les points suivants :

1. Mécanisation de la décision ;
2. Biais des données ;
3. Liberté du juge et des parties vis-à-vis des technologies numériques ;
4. Pouvoirs des acteurs juridiques vis-à-vis des technologies numériques.

Mécanisation de la décision

La notion de « justice prédictive » peut être abordée sous deux angles : la prédiction de décisions et l'aide à la décision. Un des problèmes majeurs évoqué lors de l'atelier est l'excès de confiance des juristes dans les systèmes numériques, qui leur sont dépeints comme étant des machines merveilleuses, infaillibles, capables de compulser des masses de jurisprudences et d'en ressortir des résultats parfaitement exacts ou, en tout cas, de manière plus fiable et plus rapide que ce qu'un humain serait capable de faire. Or, du point de vue des informaticiens, si l'on examine les technologies qu'il est possible de mettre en œuvre au sein de tels outils numériques (logique floue, *deep learning*, etc.), il est clair qu'une confiance aveugle dans les systèmes numériques peut avoir des conséquences très graves si les résultats produits sont utilisés hors de toute mise en perspective.

La principale raison en est que le comportement de tels programmes échappe à la compréhension de leurs utilisateurs, voire de leurs développeurs. Si ces derniers ont effectivement implémenté des mécanismes d'apprentissage, de déduction, d'inférence, etc., qui sont bien compris, éprouvés et vérifiables, le comportement effectif du programme dépendra en pratique des arbres de décision, des critères, etc. construits et mis à jour lors de la phase d'apprentissage. De fait, le modèle de raisonnement que la machine aura élaboré sera inconnu des humains.

D'une manière plus générale, le fonctionnement de tout système numérique, observé sous l'angle des données produites en sortie, est conditionné par les données qui lui sont fournies en entrée (voir *infra*).

Il faut également noter que le raisonnement juridique n'est pas gouverné purement par une logique formelle. Toute tentative de le transcrire en algorithme implique donc une interprétation de la part des concepteurs et/ou développeurs, ce qui multiplie les sources d'inexactitudes.

Biais des données

Tout système numérique travaille sur une représentation du monde réel : un modèle. Or, par nature, ce modèle ne peut pas être complet. Dans certains cas, ce modèle peut même parfois être inexact. Il faut donc accepter le fait que le système va prendre des

décisions sur la base d'informations incomplètes, voire fausses. De ce fait, quelle confiance peut-on avoir quant à la qualité des résultats produits ? Certes, le (bon) développeur va mettre en place des tests pour vérifier que, sur un nombre, forcément limité, de cas qu'il juge représentatifs, son système fournira le résultat attendu, c'est-à-dire conforme aux spécifications. Pour autant, il ne pourra jamais garantir que son système fonctionnera en toute occasion de la façon attendue, quelles que soient les conditions environnementales d'exécution : machine physique, connexions extérieures, température, champs électromagnétiques, rayons cosmiques, etc.

En ce qui concerne les systèmes fonctionnant par apprentissage, un biais peut être dû aux informations (quantité, qualité, ordre) fournies lors de l'apprentissage. Le système va construire son modèle, qui ne correspond pas forcément à celui auquel un humain fait référence (même inconsciemment). Les conditions d'apprentissage vont donc influer sur le fonctionnement ultérieur du système. Si, en outre, cet apprentissage se déroule en mode collaboratif, il y a un risque réel que certains contributeurs injectent délibérément des informations erronées, avec pour objectif d'influencer le fonctionnement ultérieur du système et donc les résultats produits.

Il est en théorie possible qu'une personne mal intentionnée, ayant déterminé comment se comporte un système, décide de concevoir un second système dans le but spécifique de produire des données à même de biaiser les décisions du premier système. Il s'agit là d'un phénomène connu et largement utilisé dans les relations humaines. Pour autant, il convient d'alerter les utilisateurs quant à la qualité des données résultats produites et des informations qu'elles peuvent convoyer, tant qu'ils n'auront pas à leur disposition des indicateurs leur permettant de juger de la confiance qu'ils peuvent accorder à ces données. Une telle approche relève des processus de gestion des risques liés à la sécurité des informations.

Dans le cas des mégadonnées (« *big data* »), apparaît un problème supplémentaire, lié au caractère transitoire des données. Au vu des quantités de données traitées, il n'est techniquement pas possible de les stocker indéfiniment. Elles sont donc purgées régulièrement. Pour autant, les inférences construites à partir de ces données d'entrée (c'est-à-dire, les données de paramétrage calculées par le processus d'apprentissage) vont persister et seront à leur tour intégrées aux données qui seront traitées par la suite. Elle pourront ainsi, par effet de cascade, influencer de futures déductions. L'intérêt des mégadonnées est double : travailler sur de gros volumes de données et disposer de données récentes. Néanmoins, il est du coup souvent impossible de retracer le processus de décision jusqu'à son origine. Si, à un moment donné, le système a calculé une donnée erronée, cette erreur peut perdurer bien après la disparition de la cause. La conséquence d'une erreur peut donc être temporellement très distante de sa cause.

Il convient également de s'interroger sur la qualification des différents types de données que les systèmes numériques sont amenés à traiter : données « initiales », données « calculées », métadonnées, etc Lors de cet atelier, ce questionnement a plutôt été abordé dans le thème D, « Droit des données à caractère personnel ».

La liberté du juge et des acteurs juridiques vis-à-vis des technologies numériques

Face à la débauche de puissance et la réputation d'infaillibilité des systèmes numériques, on peut légitimement craindre qu'il deviendra de plus en plus difficile pour un juge ou une partie d'aller à l'encontre de l'avis calculé par de tels systèmes experts. Quand bien même ces acteurs seraient conscients des vulnérabilités de ces systèmes (voir *supra*), la force de persuasion due à l'autorité de la chose calculée peut faire craindre

à terme une confiscation du processus judiciaire par les programmeurs. Le logiciel dicterait ce qui est juste ou pas, renforçant le caractère prémonitoire de l'adage de Lawrence Lessig : « *code is law* ». Cela soulève plusieurs questions :

- En premier lieu, on peut s'interroger sur l'acceptation sociale d'une telle confiscation. Cette dernière est vraisemblablement contingente de la culture juridique et du contexte politique et social. C'est ainsi qu'en Chine, l'aide automatisée à la décision des juges mise en œuvre dans certaines provinces rassure les populations, dans un contexte de défiance envers ceux-ci, réputés peu compétents ou peu impartiaux. Sur ce point, il serait d'ailleurs intéressant de comparer la place du juge et de la jurisprudence dans les systèmes de *Common Law* par rapport aux pays de droit romano-germanique.
- Il conviendrait également d'étudier les risques de stagnation de la jurisprudence et de fixation de certains stigmates sociaux induits par la mécanisation des décisions.

Dans ce contexte d'utilisation de plus en plus fréquente de systèmes numériques dans le domaine juridique, il apparaît indispensable de former les juristes aux outils numériques pour qu'ils en connaissent non seulement les avantages mais également les limites et les biais. Ceux-ci sont à l'heure actuelle moins connus et acceptés que ceux des humains.

En tout état de cause, un tel système devrait a minima :

- mettre en œuvre un algorithme transparent, sachant qu'il ne sera pas forcément toujours possible d'en prouver le comportement (au sens de la preuve logique formelle) ni donc d'en garantir les résultats ;
- fournir les éléments d'argumentation permettant aux humains, en dernière instance, de juger de la pertinence des arguments ayant conduit à la décision proposée et éventuellement de s'en écarter. Comme il a été discuté, ces systèmes s'appuient sur un modèle du monde réel (donc partiel et pouvant éventuellement contenir des erreurs), et de nombreuses connaissances des humains (parfois inconscientes) ne sont pas modélisées.

Il serait d'ailleurs sûrement judicieux de s'interroger, nous êtres humains, tant d'un point de vue juridique que d'un point de vue purement sociétal, afin de savoir jusqu'où mettre en œuvre les technologies du numérique en justice :

- simple aide décisionnelle, en conservant à l'humain la maîtrise du processus ; ou
- automatisation totale, avec recommandations / propositions plus ou moins imposées.

Cette question est bien évidemment en lien direct avec le thème B de l'atelier, « Systèmes Autonomes et Décision, Droits Fondamentaux ».

Quels pouvoirs pour les acteurs juridiques vis-à-vis des technologies numériques ?

Le dernier point évoqué au sein de ce thème, mais que nous n'avons pas eu le temps de développer, concerne les moyens dont pourraient disposer les acteurs juridiques vis-à-vis des technologies numériques. Les enquêteurs se trouvent effectivement de plus en plus fréquemment confrontés à de nouveaux outils tels que l'anonymisation ou l'usage du *darknet*. Afin de remplir leur mission, quels sont les pouvoirs techniques et juridiques des enquêteurs pour contourner ces outils, les infiltrer, etc. ? La question n'est pas fondamentalement nouvelle. La téléphonie, par exemple, a elle aussi suscité en son temps

les mêmes interrogations. Cependant, la puissance des technologies numériques impose d'aborder le sujet de façon différente.

Synthèse réalisée par Manuel Munier à partir des éléments débattus collectivement lors de la table ronde

Constance CAILLAUD-RENAUD
Doctorante en 3ème année
Faculté de Droit de La Rochelle
Ecole Doctorale Pierre Couvrat
Centre d'Etudes Juridiques et Politiques (CEJEP)
Directrice de thèse : Linda ARCELIN LECUYER

Les professions du droit et la révolution numérique

Le XXIème siècle sera certainement retenu dans l'histoire comme celui de la révolution numérique. En effet, le développement d'une technologique sans précédent a bouleversé l'ensemble de notre civilisation : l'Internet.

Nous sommes tous dorénavant connectés par le biais de nos smartphones, de nos ordinateurs, de nos tablettes ou encore de nos télévisions.

Leboncoin, *eBay*, *Cdiscount*, *Amazon* sont devenus en moins de dix ans des sites marchands de référence, connus de tous et utilisés régulièrement par un grand nombre de consommateurs.

Face à ce chamboulement, l'ensemble des acteurs de notre société ont changé leurs habitudes, modifiant par la même la nature des rapports entre les individus.

Les professionnels du droit, qu'ils soient avocats, notaires, huissiers ou membres d'une autre profession réglementée ne peuvent pas faire exception à cette tendance.

La dématérialisation a fait une entrée discrète dans le monde du droit et plus particulièrement du procès, à la fin des années 90 avec la loi « *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique* »,[1]suivie quelques années plus tard par la loi de 2004 sur « *la confiance en l'économie numérique* »[2]. Le droit français est ensuite resté silencieux presque une décennie jusqu'à ce qu'une loi et un décret[3] décident d'accompagner dans cette révolution numérique les professions judiciaires et juridiques, ainsi que certaines professions réglementées.

---

[1] Loi n°2000-230 du 13 mars 2000.

[2] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[3] L. n° 2011-331, 28 mars 2011 de modernisation des professions judiciaires ou juridiques et certaines professions réglementées (JO 29 mars 2011, p. 5447)a instauré la dématérialisation des actes de procédures collectives- transcrite dans le code de commerce. Le décret d'application de cette loi du 28 décembre 2012 prévoit quant à lui que, dans un futur proche, le jugement pourra être établi sur support électronique (art. 456 c. pr. civ.), selon des procédés garantissant l'intégrité et la conservation, et qu'il sera signé

La volonté législative de faire rentrer l'Internet au cœur des métiers du droit s'est accentuée durant le dernier quinquennat avec la promulgation de trois lois faisant une part belle au numérique. Tout d'abord, la Loi « *Macron* »[4] est venue définir la notion de plateforme numérique, tout en obligeant dans un soucis de protection du consommateur, à la transparence quant à la tarification[5] des actes d'huissiers et notariés, ou des honoraires d'avocat avec la signature d'une convention. Puis, ce fut au tour de la loi « *pour une République Numérique*[6] » de continuer le processus en imposant à tous les professionnels dans leur ensemble : la notion de loyauté des plateformes, un renforcement de l'information du consommateur, et une protection accrue de ses données à caractère personnel. Cependant, la loi de modernisation de la justice du XXIème siècle est celle qui amène réellement le numérique au cœur des professions juridiques et réglementées en incitant ces professionnels à proposer à leur clientèle une « relation numérique » c'est-à-dire totalement dématérialisée répondant à l'ensemble des critères garantissant une interopérabilité[7] efficace. Cette disposition s'inscrit dans une volonté globale de faciliter l'accès du citoyen à la justice.

électroniquement dans le respect des exigences légales, qui seront précisées par un arrêté du garde des Sceaux.

[4] Loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques.

[5] Grille tarifaire concernant tous les actes classiques fixée par décret.

[6] Loi 2016-1321 du 7 octobre 2016 (JO 8 texte n°1). Ce texte pose également le principe de la neutralité d'Internet, celui de la portabilité et récupération des données, et l'encadrement des avis en ligne.

[7] Art3 : « I.-Les huissiers de justice, les notaires, les commissaires-priseurs judiciaires, les avocats, les avocats au Conseil d'Etat et à la Cour de cassation, les commissaires aux comptes et les experts-comptables proposent à leur clientèle une relation numérique dans un format garantissant l'interopérabilité de l'ensemble des échanges.

II.-Les professions mentionnées au I rendent librement accessibles les données figurant dans leurs annuaires et tables nationales de manière à garantir cette interopérabilité, notamment au moyen d'un standard ouvert et réutilisable, exploitable par un traitement automatisé.

III.-Les professions mentionnées au même I peuvent recourir à la sollicitation personnalisée, notamment par voie numérique, et proposer des services en ligne.

Les conditions d'application du présent III, notamment les adaptations nécessaires aux règles déontologiques applicables à ces professions dans le respect des principes de dignité, de loyauté, de confraternité et de délicatesse, sont fixées par décret en Conseil d'Etat.

IV.-Les administrateurs judiciaires et les mandataires judiciaires proposent aux personnes intéressées, dans les limites de ce que leur permet leur mandat de justice et pour les besoins de celui-ci, une relation numérique dans un format garantissant l'interopérabilité de l'ensemble des échanges.

V.-….

Les professionnels du droit doivent donc continuer à relever ce défi pour finaliser leur « transformation numérique », tout en tenant compte de l'ensemble des dispositions législatives venant protéger les consommateurs tant du côté du devoir d'information que du respect de sa vie privée avec les dispositifs relatifs à la protection des données à caractère personnel[8].

Une réflexion conjointe entre informaticiens et juristes sur la matière pourrait être menée afin d'identifier les besoins de chaque profession du droit et de leur proposer des solutions numériques concrètes et adaptées à leur métier pour les faire devenir des acteurs à part entière du numérique.

[8] Un nouveau règlement européen en date du 27 avril 2016 (Règl.UE 2016/679) est venu défendre le droit à l'oubli mais surtout en ce qui nous intéresse ici le consentement clair et explicite de la personne concernée quant à l'utilisation de ses données personnelles ou encore le transfert de ces dernières. La loi pour une République numérique citée ci-dessus prône également la protection de la vie privée en ligne en affirmant des principes comme le secret des correspondances privées, le droit à l'oubli ou encore la mort numérique.

Aminata Touré
Enseignant chercheur

LES ENJEUX DE L'E-JUSTICE EN MATIERE PENALE

Les nouveaux procédés d'information, de recherche, de rédaction et de communication écrite ou orale ont une place grandissante dans le paysage judiciaire. Depuis le début des années 2000, l'institution judiciaire française tente de s'approprier peu à peu ces outils technologiques et leurs diverses fonctionnalités, franchissant une première étape dans un long processus de transition technologique encore balbutiant. Cependant, à la différence des technologies qui les ont précédées, ces instruments du travail judiciaire touchent aujourd'hui le cœur de la mission juridictionnelle, affectant par exemple le contact humain ou la construction du raisonnement judiciaire. Du traitement de texte au système expert, de la présence réelle à la présence virtuelle à l'audience, l'enjeu n'est pas le même et les difficultés ne se résument plus à l'équipement de toutes les juridictions et la formation des personnels. Il est donc certain que la nature et l'action de ces outils ne sont pas simplement techniques ; ces nouveaux procédés transforment les conditions d'exercice de la justice, amorçant une nouvelle façon de mener le travail judiciaire dont la neutralité n'est qu'apparente.

A l'évidence, l'emploi de ces nouveaux outils contraint les acteurs du procès à en adopter de nouvelles pratiques ou habitudes. Toutefois, certaines d'entre elles tranchent fortement avec l'exercice traditionnel de la fonction de juger, jusqu'à faire poindre le risque d'une atteinte à des garanties procédurales classiques telles que la publicité, les droits de la défense, le contradictoire, ou encore l'individualisation des peines. De ce fait, l'on se demande si ces nouvelles pratiques, induites par les technologies et susceptibles de se développer à l'avenir, ne constituent pas les germes d'une forme d'asservissement de la justice face à la modernité, emportant le risque de provoquer des changements conséquents au sein même de la mission juridictionnelle. L'indépendance du juge, qui constitue une caractéristique essentielle sinon fondamentale de l'institution en charge d'interpréter la loi et d'en assurer l'application, lui permettant de bénéficier d'une totale autonomie en sa qualité d'auteur d'un acte juridictionnel, est aujourd'hui menacée. Inhérente à son office, elle figure parmi les principes fondateurs de l'État de droit et donne sens à la justice ; pour autant, elle semble altérée par la diffusion d'outils et procédés modernes à des fins judiciaires, laissant alors planer la menace d'une justice pénale qui accorde une place maîtresse à la technique, et en devient alors tributaire.

L'on fait effectivement le constat d'un fléchissement de certains principes procéduraux devant les contraintes technologiques. La visioconférence par exemple, a une emprise conséquente sur la conduite de l'audience, restreignant le principe fondamental de la publicité des débats – le public n'étant admis que d'un seul coté de l'écran – ou encore les droits de la défense, lorsque prévenu et avocat sont éloignés physiquement. Aussi et surtout, la production des actes de procédure et des décisions de justice voit ses modalités transformées, tant sur la forme que sur le fond. D'une part, les interactions virtuelles ont une influence sur la manifestation de la vérité, le fruit d'une audience à distance ne pouvant nécessairement pas être le même qu'une audience en coprésence. D'autre part, les nouvelles techniques d'information, et notamment les banques de données juridiques et judiciaires, bien que constituant une aide adéquate pouvant guider le juge dans sa réflexion, sont dans le même temps susceptibles de représenter un carcan invisible,

source d'inertie jurisprudentielle ou de désindividualisation du traitement pénal. L'on peut en effet craindre que la facilité d'accès à cette information juridique et procédurale, ainsi que la diversité des contenus, incitent le juge, de façon presque inconsciente, à davantage construire son raisonnement autour de ces données, et corrélativement, à moins solliciter sa réflexion et son analyse personnelle de la situation, voire son imagination. Par ailleurs, afin de gagner en célérité, la technologie intervient progressivement sur ce terrain de l'écriture du fond de la décision. Source de normalisation, la modélisation de la décision de justice peut tout autant constituer un enfermement dans un cadre rédactionnel prédéfini par la machine ; or, cela n'est pas sans questionnement quant à la qualité de la décision et sa réception par le justiciable, car de telles pratiques peuvent difficilement témoigner d'un rapport personnalisé, pourtant nécessaire au sentiment de justice. Ajoutons enfin que la technologie est également aujourd'hui capable de fournir une réponse à un problème de droit ; du moins, d'apporter une aide décisive dans sa résolution. Se pose alors la question de la place du juge dans ce contexte modernisé, et précisément, des places respectives de la technologie et du juge dans l'activité décisionnelle. Assurément, cette assistance technique plus conséquente est radicalement différente de la conception traditionnelle, voire de la nature même de la *juris dictio*. Sous l'effet des technologies, le procès pénal se transforme, non seulement d'un point de vue juridique, mais également d'un point de vue sociologique, quant à l'esquisse d'une justice pénale technologisée qui se dessine.

Le scepticisme immodéré à l'égard de l'introduction des technologies processuelles est pour autant à proscrire, l'emploi de ces moyens technologiques pouvant être au service tant de l'efficacité des processus de production de la justice, que de l'efficacité procédurale. Si le lien imposé qui s'est tissé entre le praticien et la technologie « *s'est construit sur un modèle de dualité : le juridique d'une part, le technique de l'autre* »[1], l'enjeux est alors d'effacer progressivement cette dualité car justement, l'absence de neutralité procédurale et processuelle de la technologie atteste du fait que juridique et numérique sont imbriqués. Il convient alors de dépasser le constat d'un ascendant irrésistible de la technologie sur la justice, source de mutation de cette dernière, pour se concentrer davantage sur la possible et même l'indispensable adaptabilité des technologies face aux exigences d'une bonne administration de la justice. En la matière, la coopération avec avec les techniciens est fondamentale dès la phase de conception de l'outil, seul moyen de parvenir à l'aboutissement d'un produit adapté aux contraintes procédurales et aux « besoins métiers », afin que la technologie devienne un auxiliaire substantiel des professionnels du droit et de la justice, et non un synonyme de l'effacement progressif de ces derniers.

[1] S. ELKAÏM, « Justice, NTIC et office processuel du juge », *in* A. Garapon, S. Perdriolle, B. Bernabé*, La prudence et l'autorité : l'office du juge au XXIe siècle,* préc., p. 211.

L'informatisation du travail juridique

Introduction

Comme toutes les activités humaines, le travail juridique est affecté par la révolution numérique. Récemment, un phénomène tout à fait notable s'est fait jour en matière de droit : la « justice prédictive », c'est-à-dire l'utilisation des nouvelles technologies, et en particulier du Big Data et de l'intelligence artificielle, pour prédire une décision de justice par l'analyse automatisée de la jurisprudence.

L'origine de l'expression n'est pas facile à tracer, et ne fait pas l'unanimité, certains préférant parlant de « justice quantitative ». L'expression « justice prédictive » est indéniablement piégeuse. On aurait pu parler de « prédiction judiciaire », en inversant les termes, et cela aurait probablement été plus juste. Pourquoi « justice prédictive » ? Probablement par volonté de montrer la parenté de ces techniques avec l'analyse prédictive et la médecine prédictive. L'analogie est plaisante à l'oreille, mais elle a des limites. L'analyse est l'opération effectuée par l'analyste, qui est observateur des faits qu'il tente de prévoir. La justice est quant à elle une opération effectuée par le juge, qui est non pas l'observateur mais le « producteur final », pourrait-on dire, du processus judiciaire. Une « justice prédictive » serait celle qui verrait le juge ou le processus judiciaire déterminer la probabilité qu'un évènement advienne sur la base des éléments qui lui sont connus : c'est d'ailleurs en ce sens que Mireille Delmas-Marty emploie l'expression « justice prédictive » dans un article de 2011 dans lequel elle critique la prise en compte de la dangerosité des individus, telle que déterminée par leur comportement antérieur, en droit pénal[1]. Ce n'est pas du tout de cela qu'on parle quand on parle aujourd'hui de justice prédictive : dans la justice prédictive, le juge n'est pas celui qui prédit le comportement mais celui dont le comportement est prédit. Il n'est pas le sujet de la prédiction, il en est l'objet.

Le développement de la justice prédictive est une réalité au niveau mondial. Aux Etats-Unis, la start-up Legalist a développé un modèle économique fondé sur un algorithme capable de déterminer en quarante-huit heures les chances de succès d'un client et la durée probable des procédures à partir d'une base de données de quinze millions de dossiers sur les vingt-cinq dernières années. Des logiciels sont utilisés par des juridictions américaines pour

[1] Delmas-Marty M., « Sécurité et dangerosité », Revue française de Droit administratif, 2011, p. 1096.

évaluer les risques de récidive des prévenus. Dans certaines provinces chinoises, des systèmes d'intelligence artificielle proposent même des décisions aux juges.

La technique progresse aussi : le 24 octobre 2016, la revue PeerJ a publié un article intitulé "Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective", dont les auteurs affirment qu'ils ont élaboré un modèle numérique capable de prédire les décisions de la Cour européenne des droits de l'homme avec un taux de réussite de 79 %.

En France, le phénomène est pris suffisamment au sérieux par les pouvoirs publics pour que les principaux acteurs du secteur aient été auditionnés par le Sénat le 12 décembre dernier. En effet, plusieurs sociétés, comme Case Law Analytics, Tyr Legal ou Prédictice, proposent des outils permettant, par exemple, d'estimer le montant de dommages et intérêts ou d'une pension alimentaire, d'obtenir des statistiques sur les chances de gagner une procédure, d'afficher graphiquement l'état d'un contentieux ou les arguments les plus souvent utilisés, etc. Le barreau lillois travaille, en partenariat avec une startup au développement d'un logiciel qui sera non seulement un moteur de recherches spécialisées mais aussi une moulinette à données permettant « d'enrichir la stratégie judiciaire ». Et les possibilités s'accroitront nécessairement avec la loi du 7 octobre 2016 pour une République numérique. Celle-ci prévoit en effet une « mise à la disposition du public à titre gratuit » des décisions de justice « dans le respect de la vie privée des personnes concernées » - c'est-à-dire avec obligation préalable d'anonymisation. Il en résultera une augmentation considérable des données disponibles, et donc, *a priori*, de la fiabilité des analyses.

Ce phénomène soulève bien évidemment une grande quantité de questions liées à une éventuelle « déshumanisation » de la justice et du travail juridique, et appelle une étude détaillée et pluridisciplinaire.

Identification du phénomène

L'expression « informatisation du travail juridique » renvoie en réalité à un large spectre de phénomènes, allant de la simple consultation d'une base de données juridiques à la prise éventuelle d'une décision juridique par une intelligence artificielle. Il conviendra donc de distinguer, au sein de cette gamme de situations, celles qui ne constituent finalement qu'une évolution des moyens mis à disposition du juriste pour effectuer les tâches nécessaires à son art ou à sa recherche (typiquement par l'informatisation du travail de recherche documentaire) de celles qui, plus profondément, substituent véritablement le travail de la

machine au travail humain. Où placer, par exemple, les sites internet qui génèrent automatiquement des actes juridiques sur la base des données renseignées par l'utilisateur ? Pour le présenter autrement, il convient de se demander à quel moment l'évolution technologique en matière de travail juridique cesse de générer un simple changement de degré (le même travail est effectué plus efficacement) et devient un changement de nature.

Ceci étant fait, le phénomène devra faire l'objet d'une étude aussi bien théorique que pratique.

Analyse théorique

Sur le plan théorique, il conviendrait de développer une réflexion sur les convergences et les divergences intrinsèques entre les processus juridiques et les processus numériques. Ainsi, du côté des convergences, il conviendra de se demander dans quelle mesure la structure logique qui sous-tend le processus décisionnel juridique peut se rapprocher d'un algorithme dont le code serait la règle de droit. Du côté des divergences, il faudra se demander au contraire dans quelle mesure le processus décisionnel juridique contient une part inéluctable de discrétion humaine non modélisable, et ce non seulement d'un point de vue descriptif mais également normatif :

- Descriptif : est-il vrai que la décision juridique est toujours dépendante d'une part de discrétion humaine imprévisible, et si oui à quel degré et sous quels aspects ?
- Normatif : est-il souhaitable que la décision juridique soit toujours, in fine, dépendante d'une part de discrétion humaine imprévisible ?

Cette deuxième question est liée en réalité à une autre : celle de la confiance qu'accorde le système social considéré à la personne même du juge. Il y a là certainement un élément contingent lié à la culture nationale. Ainsi, le système juridique anglo-saxon est fondé sur une grande confiance accordée à la personne même du juge et à son sens de l'équité, mais en même temps le poids du précédent dans les systèmes de *Common Law* rend suspect l'écart par rapport aux solutions précédentes, et rend donc pertinente l'exploitation massive de bases de données jurisprudentielles. Le système français est au contraire caractérisé depuis la Révolution française par une méfiance envers les juges, qui doivent être cantonnées à un rôle de « bouches de la loi ». Comment mieux dire qu'ils sont, finalement, assimilés à des « machines » à appliquer la loi ? L'automatisation de la décision de justice est-elle alors susceptible d'y être mieux acceptée ? Il y a pourtant en droit français des éléments qui prennent en compte le facteur humain, comme le principe de l'intime conviction en droit

pénal. Dans les provinces chinoises ou le « jugement assisté par ordinateur » s'est développé, les juges sont réputés ne pas être compétents ou impartiaux : cela rassure que ce soit la machine qui prenne les décisions. La confiance dans la machine est-elle inversement proportionnelle à la méfiance envers l'humain ? La question, on le voit, est complexe.

Analyse pratique

Sur le plan pratique (et en insistant sur le fait que la « théorie » et la « pratique » ne sauraient s'opposer de façon aussi tranchée qu'elles ne sont présentées dans cette brève contribution), il conviendra d'opérer une analyse des opportunités et des risques sociaux que génèrent ces phénomènes ainsi que des paramètres de bonne opération.

Opportunités

Les opportunités sont nombreuses. On ne parlera pas ici des opportunités économiques – le marché potentiel est probablement énorme – mais des opportunités sociales, en termes de bien commun. Un traitement plus efficace et plus massif des données juridiques est de nature à réduire le temps passé par les professionnels du droit sur chaque affaire et, partant, à diminuer le coût de la justice pour les justiciables. Une évaluation objective et fiable du « pronostic » judiciaire est également de nature à dissuader les justiciables et leurs auxiliaires de s'engager dans des procédures à « mauvais pronostic » et de recourir alors à d'autres formes de résolution de leurs affaires. Les tribunaux en seront désengorgés d'autant.

Risques

Le risque le plus évident est celui d'une certaine déshumanisation de la justice – auquel il pourrait être éventuellement répondu que, tout à l'inverse, de tels outils permettent précisément aux professionnels du droit de se concentrer sur les aspects humains en passant moins de temps sur le travail automatisable.

On peut relever également le risque de « prophétie auto-réalisatrice » ou d'effet « performatif » de la prédiction. Est-il en effet possible que la prédiction influence le jugement autant qu'elle ne le prédit ? Les juges ne risquent-ils pas d'être montrés du doigt en raison de leur éventuelle sévérité ou laxisme s'ils ne tiennent pas compte, dans leurs jugements, des statistiques établies ? C'est alors le logiciel qui fait le jugement, et donc le concepteur de l'algorithme qui confisque le pouvoir de juger. Cet effet performatif n'est d'ailleurs pas nécessairement accidentel : pour citer Antoine Garapon, magistrat et secrétaire général de l'Institut des hautes études sur la justice, « les legaltech ne doivent pas être

seulement appréhendés comme de simples facilitateurs pour les justiciables et les avocats, ou comme de nouveaux auxiliaires d'une fonction judiciaire qui demeurerait intacte ; ils nourrissent une ambition plus large, celle de devenir eux-mêmes une nouvelle forme de justice »[2]. L'expression « justice prédictive » prendrait alors cette fois tout ce sens, celui d'une nouvelle forme de justice par les nombres.

Il existe également un risque de stagnation du droit : en accédant à une moyenne, en grandeur nature, des positions jurisprudentielles et des montants d'indemnisation dans tous les domaines du droit, les professionnels de la justice pourraient être tentés de s'aligner sur ce qui existe déjà, laissant de moins en moins de place au raisonnement et à la prise en compte des facteurs humains et limitant les possibilités d'évolution du droit. Un risque voisin est la fixation des stigmates : un logiciel estimant la peine devant être imposée à un individu sur la base des statistiques américaines aboutirait probablement, quels que soient les critères retenus par la machine, à reproduire le modèle carcéral américain caractérisé par une surreprésentation des afro-américains.

Enfin, il y a également le risque que le pronostic de réussite surdétermine, chez les avocats, le choix d'un client. Qui pourront-ils aller voir, ceux à qui l'ordinateur assigne une faible chance de réussite ? Notons que ce problème existe déjà, mais que cette sélection est aujourd'hui relativement intuitive, voire, oserait-on dire, « pifométrique », ce qui fait que le client rejeté a encore une chance ailleurs.

Paramètres de bonne opération

Ce que nous appellerons ici les paramètres de bonne opération, faute d'une meilleure formule, décrit l'ensemble des éléments et interrogations qui doivent être pris en compte pour que ces nouvelles technologies du droit soient socialement acceptables et juridiquement fiables. Il faudra notamment s'interroger sur le degré de transparence qui devra être accordé aux algorithmes utilisés, afin que les utilisateurs soient conscients des « biais » qui peuvent être générés.

Une réflexion est également nécessaire sur la fiabilité et de la pertinence des bases de données utilisées, notamment jurisprudentielles. Il est vrai que les questions de fiabilité des opérations de prédiction sont, *a priori*, de la responsabilité des concepteurs de ces outils. Mais si l'effet performatif que l'on a signalé comme risque se réalise, ou bien si ces outils sont à

[2] « Les enjeux de la justice prédictive », Revue pratique de la prospective et de l'innovation n° 1, Octobre 2016, dossier 4.

terme utilisés non seulement par les auxiliaires de justice mais également par les juges, n'y a-t-il pas également un intérêt social à ce que ces instruments soient fiables ?

Comment gérer notamment le fait que toutes les décisions de justice ne sont pas publiques ? La loi pour une République numérique devrait *a priori* résoudre ce problème – encore faudra-t-il que soient adoptés les décrets d'application et que soient dégagés les moyens financiers et humains nécessaires. Et même alors, il y a plusieurs réserves. D'une part, la loi précise que « la mise à disposition du public est précédée d'une analyse du risque de ré-identification des personnes ». Or, c'est là une réserve potentiellement importante, selon comment elle est interprétée : n'est-il pas finalement quasiment toujours possible d'identifier les protagonistes, même après anonymisation, sur la base des éléments du litige ? Et si l'anonymisation « réelle » aboutit à gommer des éléments du litige qui sont pertinents pour la prédiction, comme par exemple les fonctions des protagonistes, ne perd-on pas alors en fiabilité ? D'autre part, toutes les juridictions ne sont pas concernées : les juridictions administratives spécialisées, par exemple, semblent exclues. Or, pour certaines – on pense notamment à la Cour nationale du droit d'asile – un outil prédictif serait tout à fait précieux et protecteur de la sécurité juridique d'une catégorie de justiciables particulièrement vulnérables, à savoir les demandeurs d'asile. Pour autant, en cassation, les décisions des juridictions administratives spécialisées sont examinées par le Conseil d'Etat, dont les décisions, elles, seront rendues publiques. Est-ce que cela peut générer un biais ? Faut-il exclure le contentieux des juridictions administratives spécialisées de la justice prédictive dans la mesure où ce contentieux ne sera pas parfaitement public ? Peut-on aménager cette asymétrie vraisemblable de données ?

Autre question : faut-il se concentrer sur les décisions des juridictions suprêmes ou intégrer toutes les décisions de justice – y compris celles par exemple qui vont à l'encontre de la jurisprudence mais qui n'ont pas été contestées ? Comment intégrer les revirements de jurisprudence ? Comment intègre-t-on les décisions qui ont été annulées en appel ou en cassation ? Comment intégrer les « décisions d'espèce », ces « one shots » placés en dehors de toute continuité jurisprudentielle ? Jacques-Henri Stahl, Président de la 2ème chambre de la section du contentieux du Conseil d'Etat, a ainsi pu estimer que « pour la bonne compréhension et l'intelligibilité de la jurisprudence, ce qui compte n'est pas l'exhaustivité, mais au contraire la sélection »[3].

[3] « « *Open data* » et jurisprudence », Dr. adm. 2016. Repère 10

Certaines questions sont à la fois techniques et éthiques. Faut-il pour prendre en compte l'historique individualisé de chaque juge ? Pour certaines juridictions, comme la Cour EDH, ce n'est pas vraiment un problème : les décisions sont acquises par vote, dont le résultat est public. Et si on ne sait pas qui a voté pour ou contre, on peut le deviner grâce à la pratique des opinions séparées. En revanche, dans les juridictions qui sont marquées par la collégialité du verdict et le secret du délibéré, comme en France, il y a plus de problèmes. On peut éventuellement corréler le sens des décisions avec la présence de tel ou tel juge, mais ce ne sera qu'une corrélation, plus ou moins forte. Par ailleurs, une telle corrélation individuelle ne nous fournirait pas nécessairement une prédiction fiable des délibérations collégiales. Cela pose problème. D'un côté, si l'on ne peut pas prendre en compte ce facteur, a-t-on vraiment un outil fiable ? La personnalité des juges, leur leadership, peut influencer le sens des décisions, notamment en première instance voire en appel. De l'autre côté, si on arrive effectivement à accoler des « probabilités de sens d'une décision » à la personnalité des juges, n'aboutit-on pas à remettre en cause le secret du délibéré ?

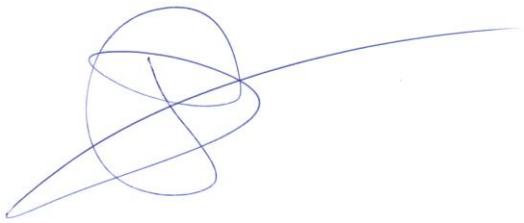
D'autres questions mériteront d'être soulevées, notamment celle de l'encadrement légal (dans quelle mesure une intelligence artificielle peut-elle fournir un conseil juridique, en contradiction avec le monopole des avocats), celles des applications possibles non seulement en matière de pratique juridique mais également de recherche juridique et bien d'autres encore qui émergeront probablement des discussions.

Besoins de compétences dans l'autre discipline :

- Quelles sont les ressemblances et quelles sont les différences entre le raisonnement juridique et la structure d'un algorithme ?
- quelle est la portée et quels sont les limites des systèmes de traitement des données en langage naturel ? Dans quelle mesure peuvent-ils produire une « décision » à partir de « faits » ?
- quels sont les biais que peut générer une base incomplète et comment les gérer ?

Mots-clés : Big Data / Open Data, analyse prédictive, traitement automatisé des données

S. Platon
Professeur de droit public
Université de Bordeaux



Projet d'outil contractuel pour les contrats de services

MUNIER Manuel
(informatique – LIUPPA)
Univ. Pau & Pays Adour

DAVERAT Xavier
(droit privé)
Université de Bordeaux

CONTEXTE

Les paradigmes orientées service ont considérablement changé la façon de concevoir les applications et l'organisation des entreprises. Tant l'approche SOA[1] que le Cloud ont permis l'émergence de nouveaux modèles basés sur des collaborations dynamiques. Du point de vue des utilisateurs finaux, les services offrent un accès simplifié aux fonctionnalités et aux données. Quant aux organisations, la délégation de certains processus métier représente une opportunité de générer des avantages concurrentiels en réduisant les coûts, en augmentant la visibilité sur le marché et en exploitant l'expertise de leurs partenaires en offrant à ses clients des produits et des services avec de la valeur ajoutée.

Malgré les attraits des technologies basées sur les services, la perte de contrôle sur les ressources échangées est un inconvénient bien connu qui freine leur large adoption. Essentiellement, au sein des organisations différents types des règles sont associés aux ressources afin de garantir qu'elles soient correctement utilisées. De telles règles sont associées à n'importe quelle condition visant à prévenir d'éventuels dommages organisationnels, dont nous pouvons citer les conditions assurant la prévention de la perte de réputation ou la garantie de la conformité avec une norme juridique. Cependant, à partir du moment où la ressource sort du périmètre de l'organisation, il n'y a plus aucun moyen de savoir si la ressource est utilisée en respectant les règles établies. Les conséquences d'une telle perte de contrôle sur l'utilisation ne sont pas négligeables puisque la façon dont les ressources partagées sont utilisées peut affecter l'organisation en entraînant des pénalités, la perte de clients ou des poursuites. Les impacts de ces dommages justifient la nécessité d'avoir des méthodes visant à contrôler l'utilisation des ressources partagées lors d'une prestation de services. Dans ce scénario, le défi est de garantir que le partenaire externe se comporte comme prévu lorsque la ressource est dans son domaine et et que les intérêts de chaque organisation doivent être préservés.

Dans nos travaux nous avons proposé que la prestation de services soit régie par un contrat de service. Ce contrat diffère de SLA[2] traditionnels de plusieurs façons:

- Il augmente l'expressivité des garanties de service SLA, traditionnellement basées sur la sécurité et la performance, avec des termes contractuels représentant les exigences opérationnelles sur l'utilisation prévue des ressources.
- Il est basé sur une sémantique formelle qui évite des erreurs d'interprétation des clauses contractuelles grâce à une compréhension commune de leur signification.
- La conformité avec les exigences de l'entreprise en matière d'usage des ressources est déduite de la connaissance disponible recueillie au cours de l'exécution du contrat.

Notre méthode de contrôlabilité est basée sur deux éléments. Le premier a trait à la modélisation des politiques, et la second consiste en un processus qui opère avec ces politiques. En ce qui concerne la modélisation, deux modèles complémentaires sont proposés. Un premier pour formaliser la sémantique d'un contrat de service, y compris un vocabulaire de contrôlabilité. Un second pour définir les politiques de contrôlabilité, utilisant le modèle sémantique pour donner une signification claire au comportement attendu des parties. Au cours du processus, un journal qui contient la connaissance disponible sur le comportement des parties contractuelles est utilisé pour vérifier la conformité et évaluer le comportement des partenaires. Les contrats sont créés en OWL pour être lisibles par la machine et les règles des politiques sont écrites en XML.

Cette méthode, couplée au raisonnement basé sur la connaissance, offre de nouvelles perspectives quant aux techniques d'Intelligence Artificielle appliquée aux services web. D'autre part, ces travaux ouvrent des perspectives de travaux futurs, tels que la négociation de la politique contractuelle pour les contrats multipartites.

1 SOA : Service Oriented Architecture
2 SLA : Service Level Agreement

Problématique

Nos travaux de recherche ont abouti à la définition d'un outil technologique permettant de formaliser les politiques de sécurité (via des contrats) et d'évaluer la conformité du comportement des acteurs par rapport à ces politiques (via les logs et le processus de contrôle).

La perspective de cette proposition commune informatique (M.Munier) et juridique (X.Daverat) est orientée vers un outil contractuel. En effet, l'utilisation des ressources partagées ramène à une question d'exécution loyale du contrat, laquelle est assorties de clauses contractuelles ad hoc. Dans le cadre de la prestation de services informatiques, on ne peut pas se passer des SLA : il faut bien qu'un client de service cloud, par exemple, dispose d'un engagement contractuel du prestataire sur son offre avec des éléments objectifs : disponibilité, maintenance, assistance, crédits de service en cas de non-tenue des SLA (puisqu'il paie le service !).

Mais on peut parfaitement envisager de développer les contrats s'agissant de garantir le comportement des partenaires. Cette perspective coïncide d'ailleurs avec la toute récente réforme du droit des contrats, et particulièrement : les règles relatives à la conclusion du contrat, au consentement des parties (attention à la dépendance technologique qui fait partie intégrante du vice de violence)… Dans ce cadre, il faut d'ailleurs repenser, à l'aune de la réforme, la clause de suspension du service dans les contrats de services d'externalisation informatique tels que ceux d'infogérance ou de cloud conclus sur le mode SaaS. Pour l'heure, il s'agit d'exceptions d'inexécution palliative. Peut-on prévoir une exception d'inexécution préventive, qu'autorise désormais la loi, comme un axe possible de garantie du comportement du partenaire ?

Il faut aussi envisager les règles relatives aux contrats d'adhésion (ceux dont les conditions générales sont soustraites à la négociation, étant pré-déterminées par l'une des parties) – toutes les CGU et CGV sur Internet sont des contrats d'adhésion – et relever les clauses qui pourraient être abusives (la commission des clauses abusives avait déjà, en 2014, listé 45 clauses suspectes pour les contrats électroniques).

La sémantique d'un contrat de service est bien sûr à envisager : l'écriture du contrat et accord sur les définitions techniques est essentiel.

Un journal rapportant la connaissance sur le comportement des parties est possible. Le reporting est classique et on peut le faire évoluer avec un journal. En fait, tout élément entrant dans le processus de contrôle est à envisager dans le contrat : logs, métadonnées, blockchains…

En résumé, cette étude aurait pour objectif, à terme, de proposer une ingénierie contractuelle adaptée, comprenant à la fois l'architecture des contrats et des principes de rédaction.

Références Bilbiographiques

- **Thèse Elena Jaramillo** – « *A Semantic Contract Model and Knowledge-driven Process for Supporting Controllability in Service-oriented Approaches* » – dir. P. Aniorté, M. Munier (soutenue le 12/12/2016)
- **INFORSID 2016** – « *Service Contracts: Beyond Trust in Service Oriented Architectures* », E. Jaramillo, P. Aniorté, M. Munier – 34ème Congrès INFORSID, atelier SSI (Grenoble, France, 31/5-6/6 2016)
- **Thèse Vincent Lalanne** – « *Gestion des risques dans les architectures orientées services* » – dir. A. Gabillon, M. Munier (soutenue le 19/12/2013)
- **PASSAT 2013** – « *Information Security Risk Management in a World of Services* », V.Lalanne, M.Munier, A.Gabillon – 2013 ASE/IEEE International Conference on Privacy, Security, Risk and Trust (Washington D.C., USA, September 8th-14th, 2013) – pages 586-593
- **DPM 2013** – « *Legal Issues about Metadata: Data Privacy vs Information Security* », M.Munier, V.Lalanne, P.Y.Ardoy, M.Ricarde – 8th International Workshop on Data Privacy Management (in conjunction with ESORICS 2013) (Egham, UK, September 12th-13th, 2013) – LNCS 8247, pages 162-177, ed. Springer (ISBN 978-3-642-54567-2)
- **WOSIS 2013** – « *Information Security in Business Intelligence based on Cloud: A Survey of Key Issues and the Premises of a Proposal* », E.Jaramillo, M.Munier, P.Aniorté – 10th International Workshop on Security in Information Systems (Angers, France, July 5, 2013)

Projet de qualification juridique des différents types de données

MUNIER Manuel

(informatique – LIUPPA)
Univ. Pau & Pays Adour

BORGES Rose-Marie
LASSALAS Christine
(droit privé)
Univ. Clermont-Auvergne

CONTEXTE

Les paradigmes orientées service ont considérablement changé la façon de concevoir les applications et l'organisation des entreprises. Tant l'approche SOA[1] que le Cloud ont permis l'émergence de nouveaux modèles basés sur des collaborations dynamiques. Du point de vue des utilisateurs finaux, les services offrent un accès simplifié aux fonctionnalités et aux données. Quant aux organisations, la délégation de certains processus métier représente une opportunité de générer des avantages concurrentiels en réduisant les coûts, en augmentant la visibilité sur le marché et en exploitant l'expertise de leurs partenaires en offrant à ses clients des produits et des services avec de la valeur ajoutée.

Malgré les attraits des technologies basées sur les services, la perte de contrôle sur les ressources échangées est un inconvénient bien connu qui freine leur large adoption. Essentiellement, au sein des organisations différents types des règles sont associés aux ressources afin de garantir qu'elles soient correctement utilisées. De telles règles sont associées à n'importe quelle condition visant à prévenir d'éventuels dommages organisationnels, dont nous pouvons citer les conditions assurant la prévention de la perte de réputation ou la garantie de la conformité avec une norme juridique. Cependant, à partir du moment où la ressource sort du périmètre de l'organisation, il n'y a plus aucun moyen de savoir si la ressource est utilisée en respectant les règles établies. Les conséquences d'une telle perte de contrôle sur l'utilisation ne sont pas négligeables puisque la façon dont les ressources partagées sont utilisées peut affecter l'organisation en entraînant des pénalités, la perte de clients ou des poursuites. Les impacts de ces dommages justifient la nécessité d'avoir des méthodes visant à contrôler l'utilisation des ressources partagées lors d'une prestation de services. Dans ce scénario, le défi est de garantir que le partenaire externe se comporte comme prévu lorsque la ressource est dans son domaine et et que les intérêts de chaque organisation doivent être préservés.

Dans nos travaux nous avons proposé que la prestation de services soit régie par un contrat de service. Ce contrat diffère de SLA[2] traditionnels de plusieurs façons:

- Il augmente l'expressivité des garanties de service SLA, traditionnellement basées sur la sécurité et la performance, avec des termes contractuels représentant les exigences opérationnelles sur l'utilisation prévue des ressources.
- Il est basé sur une sémantique formelle qui évite des erreurs d'interprétation des clauses contractuelles grâce à une compréhension commune de leur signification.
- La conformité avec les exigences de l'entreprise en matière d'usage des ressources est déduite de la connaissance disponible recueillie au cours de l'exécution du contrat.

Notre méthode de contrôlabilité est basée sur deux éléments. Le premier a trait à la modélisation des politiques, et la second consiste en un processus qui opère avec ces politiques. En ce qui concerne la modélisation, deux modèles complémentaires sont proposés. Un premier pour formaliser la sémantique d'un contrat de service, y compris un vocabulaire de contrôlabilité. Un second pour définir les politiques de contrôlabilité, utilisant le modèle sémantique pour donner une signification claire au comportement attendu des parties. Au cours du processus, un journal qui contient la connaissance disponible sur le comportement des parties contractuelles est utilisé pour vérifier la conformité et évaluer le comportement des partenaires. Les contrats sont créés en OWL pour être lisibles par la machine et les règles des politiques sont écrites en XML.

Cette méthode, couplée au raisonnement basé sur la connaissance, offre de nouvelles perspectives quant aux techniques d'Intelligence Artificielle appliquée aux services web. D'autre part, ces travaux ouvrent des perspectives de travaux futurs, tels que la négociation de la politique contractuelle pour les contrats multipartites.

---

1 SOA : Service Oriented Architecture
2 SLA : Service Level Agreement

Problématique

Nos travaux de recherche ont abouti à la définition d'un outil technologique permettant de formaliser les politiques de sécurité (via des contrats) et d'évaluer la conformité du comportement des acteurs par rapport à ces politiques (via les logs et le processus de contrôle).

D'une certaine façon, les mécanismes de supervision et de prise de décision que nous avons proposés entrent dans la catégorie plus générale des algorithmes prédictifs. En effet, ceux-ci pourront par exemple déclencher des pénalités à l'encontre de certains acteurs, calculer des indicateurs de confiance et/ou fiabilité pouvant donc par la suite impacter le choix de tel ou tel provider,...

L'idée sous-jacente de cette contribution est d'étudier les différents types de données intervenant dans ces systèmes numériques :

- données fournis « en entrée » du système
- données produites « en sortie » par le système : résultats, décisions,... À noter que ces données pourront à leur tour être intégrées en tant que « données d'entrée » pour de futurs traitements
- métadonnées, i.e. « données sur d'autres données » ; il y a non seulement les métadonnées collectées par les technologies du numérique pour enrichir les données d'entrée ; il y a aussi les métadonnées ajoutées aux résultats produits, à des fins de traçabilité par exemple. Toutes ces métadonnées sont même souvent porteuses d'informations encore plus « intéressantes » que les données fournies (explicitement) en entrée !

S'agit-il de données de types différents ? Comment les qualifier d'un point de vue juridique ? Tous les algorithmes doivent-ils être traités de façon identique ? Quel régime de responsabilité appliquer à la prise de décision fondée sur une analyse algorithmique ? À qui appartiennent les données, influence du statut juridique du propriétaire ? Comment partager les fruits résultant de l'exploitation de données fournies gratuitement ?

Autant de questions qui nous amènent à cette proposition commune informatique (M.Munier) et juridique (R.M.Borges et C.Lassalas) avec comme point central la notion de donnée.

Références Bilbiographiques

- **Thèse Elena Jaramillo** – « *A Semantic Contract Model and Knowledge-driven Process for Supporting Controllability in Service-oriented Approaches* » – dir. P. Aniorté, M. Munier (soutenue le 12/12/2016)
- **INFORSID 2016** – « *Service Contracts: Beyond Trust in Service Oriented Architectures* », E. Jaramillo, P. Aniorté, M. Munier – 34ème Congrès INFORSID, atelier SSI (Grenoble, France, 31/5-6/6 2016)
- **Thèse Vincent Lalanne** – « *Gestion des risques dans les architectures orientées services* » – dir. A. Gabillon, M. Munier (soutenue le 19/12/2013)
- **PASSAT 2013** – « *Information Security Risk Management in a World of Services* », V.Lalanne, M.Munier, A.Gabillon – 2013 ASE/IEEE International Conference on Privacy, Security, Risk and Trust (Washington D.C., USA, September 8th-14th, 2013) – pages 586-593
- **DPM 2013** – « *Legal Issues about Metadata: Data Privacy vs Information Security* », M.Munier, V.Lalanne, P.Y.Ardoy, M.Ricarde – 8th International Workshop on Data Privacy Management (in conjunction with ESORICS 2013) (Egham, UK, September 12th-13th, 2013) – LNCS 8247, pages 162-177, ed. Springer (ISBN 978-3-642-54567-2)
- **WOSIS 2013** – « *Information Security in Business Intelligence based on Cloud: A Survey of Key Issues and the Premises of a Proposal* », E.Jaramillo, M.Munier, P.Aniorté – 10th International Workshop on Security in Information Systems (Angers, France, July 5, 2013)

Traitement automatique des langues et systèmes d'information logique pour les données juridiques

Annie Foret (foret@irisa.fr)
Université de Rennes 1 et IRISA, informatique

Mots-clé : traitement automatique des langues, données légales, système d'information, logique.

1 - Présentation du projet de recherche

A - Situation du projet

Dans un contexte de volume croissant de données et de connaissance, à la fois en quantité et en diversité, un des objectifs de l'équipe SemLIS (groupe porteur du projet) (« *Semantics*, *Logics*, *Information Systems for Data-User Interaction* ») est de **redonner du pouvoir à l'utilisateur**. Par ce terme nous entendons un individu ou un groupe avec un intérêt fort pour certaines données (personnelles ou collectives), et le besoin de les exploiter pour en déduire de nouvelles connaissances ou prendre des décisions.

Dans le domaine du droit, il s'agit d'envisager en particulier des systèmes d'aide à un usager et une chaîne de traitements allant des textes bruts ou partiellement structurés, à des représentations formelles et à facettes logico-sémantiques, pour traiter et valoriser des données, en lien avec des règles du droit.

Ce type de projet requiert des compétences complémentaires, dans les domaines suivants : droit, linguistique computationnelle et informatique ; et plus précisément pour ce dernier: génie logiciel, logique, traitement automatique des langues naturelles et fouille de données.

B – Jeu, de données, cas d'étude

Divers cas d'étude peuvent être envisagés. Comme sous-domaine, nous pourrons considérer celui des élections, en collaboration avec d'autres équipes ; ce sous-domaine a pour avantage d'être régi par un corpus juridique réduit. Le respect de certains articles de loi peut être vérifié par l'analyse conjointe de données hétérogènes (exprimées sous forme numériques ou en langage naturel).

Un autre type d'analyse concerne aussi les règles (la procédure d'une élection par exemple).

C - Système d'information, portant sur des données du droit

La vision de l'équipe SemLIS est plus celle d'une collaboration homme-machine que d'une automatisation complète, pour l'expert comme l'utilisateur sans connaissances a priori, confronté à une masse d'informations.

Un objectif essentiel des LIS (Systèmes d'information logique) est de combiner des logiques et des étapes d'explorations pour briser des limitations de systèmes existants pour retrouver et mettre à jour l'information (hiérarchies, recherches booléennes). Cette approche a aussi été appliquée à plusieurs domaines dont des données linguistiques.

Un aspect distinctif de l'équipe est l'application de méthodes formelles provenant du génie logiciel, d'informatique théorique (grammaires formelles, logique, théorie des types, langages déclaratifs, preuves) à des tâches d'intelligence artificielle (représentation des données et raisonnement, extraction de données, interaction).

Dans ce projet, notre champ d'étude sera celui des données à caractère règlementaire, sous diverses formes : textes bruts, semi-formelles ou formelles et logiques.

2- Méthodologie

A - Spécificité des textes et type d'analyse

Une première spécificité à prendre en compte est la langue utilisée. De nombreux travaux existent pour l'anglais. À notre connaissance peu de travaux concernent le traitement automatique des langues dans le domaine du droit en français. Des approches et des outils généraux existent, mais il faudrait les adapter à plusieurs niveaux :

- terminologie ;

- analyse syntaxique ;

- analyse sémantique ;

- marqueurs du discours.

À ces niveaux correspondent des ressources, des formalismes et des outils informatiques pour représenter et analyser des connaissances du domaine et l'information contenue dans un texte. Mais de ce point de vue, les textes du domaine du droit ont certaines particularités, allant de la terminologie à la structure des textes. Améliorer la couverture des phénomènes linguistiques spécifiques au français et au domaine du droit, intégrer une ontologie du domaine sont aussi souhaitables. Ces analyses automatisées devraient faciliter l'exploitation informatique de ces textes, fournir des représentations utiles et pertinentes, facilitant leur exploration (recherche d'information) et leur maitrise.

Des travaux en logique (et philosophie) peuvent être utiles dans ce cadre, pour les appliquer notamment à certains types de textes présentant des règles ou des argumentations.

B - Approche SemLIS

Nous décrivons dans cette section une des approches possibles pour la partie système d'information. L'approche LIS intègre naturellement des facettes sémantiques multiples et permet en cela d'appréhender deux problèmes essentiels en qualité des données : celui de l'hétérogénéité des données et celui de la sémantique.

Redonner du pouvoir à l'utilisateur se traduit par plusieurs objectifs :

O1: rendre l'utilisateur autonome et agile en évitant des intermédiaires (e.g., administrateur de base de données) pour exploiter les données et la connaissance ;

O2: faciliter l'interconnexion de données hétérogènes et multi-sources ;

O3: apporter de la flexibilité en autorisant l'acquisition de données hors schéma et l'évolution continue d'un schéma de données ;

O4: apporter un niveau de contrôle et de confiance dans le système en favorisant la transparence et la prédictabilité d'un système d'actions ;

O5: permettre une acquisition collaborative et la vérification des données et des connaissances.

Ces objectifs sous-tendent des défis concernant l'extraction d'information (structurée par exemple avec RDF), l'expressivité, la représentation des connaissances, l'interaction données-utilisateur.

L'équipe SemLIS a développé des outils : des systèmes de gestion de contexte LIS. Les données y sont caractérisées par des propriétés logiques permettant une exploration riche et sans connaissance a priori. L'utilisation du système peut être orienté pour la tâche du repérage d'erreurs et d'incohérences (et la proposition d'amélioration). Un autre avantage de l'approche LIS est celle de permettre une forme de sérendipité.

Un autre facteur de qualité concerne les données inconnues ou incomplètes : l'approche LIS fonctionne justement dans ce cadre-là.

Les algorithmes de calcul employés sont principalement issus de l'analyse de concepts formels, de la logique et du traitement automatique des langues.

Nous proposons d'exploiter les données en utilisant les méthodes de l'analyse de concepts logiques [Ferré et Ridoux (2003)] via des outils de l'équipe LIS : Camelis http://www.irisa.fr/LIS/ferre/camelis/ ou Sparklis http://www.irisa.fr/LIS/ferre/sparklis/.

Des expérimentations avec le système de gestion de contexte et le contexte obtenu permettront d'améliorer l'approche et la construction des facettes sémantiques à mettre en avant.

La constitution de bases de données par la doctrine juridique.

Depuis une trentaine d'année, l'étude du droit a affaire à un défi considérable : celui du développement quasi exponentiel de la jurisprudence, que d'aucun appel jurisprudence massive[1]. En un sens, c'est une chance car chaque arrêt ou décision constitue une petite expérience qui permet à la doctrine juridique d'affiner ses modèles, de les modifier ou de les valider. Encore faut-il savoir appréhender ces masses importantes de données. Or à cet égard, il nous semble que la doctrine juridique n'est pas suffisamment armée.

Premièrement, en dépit de la diffusion numérique croissante des arrêts et décisions, la doctrine juridique ne s'est pas dotée d'outils lui permettant de les analyser finement. En particulier, il n'existe pas de base de données critique *construite par (et pour) la doctrine*. Il existe certes des bases de données mais qui sont toutes produites soit par les juridictions elles-mêmes, soit par les éditeurs juridiques et elles ont des inconvénients quant à l'exploitation des arrêts et décisions.

Lorsqu'elles sont critiques et commentées, elles posent un problème épistémologique : celui d'orienter le chercheur sans qu'il connaisse les critères de classification. Lorsqu'elles sont brutes, elles manquent généralement de précision, obligeant à recourir à la recherche textuelle.

En outre, ces bases de données ont toutes la propriété de rendre leur utilisateur captif car les critères de recherche n'y sont généralement limités et restrictifs. Par exemple, le site Légifrance, bien qu'extrêmement complet, ne permet pas de faire une recherche simultanée sur les décisions du Conseil d'Etat, de la Cour de cassation et du Conseil constitutionnel. L'utilisateur sera donc obligé de faire trois recherches consécutives.

Globalement, il en va d'une forme d'indépendance, d'autonomie et d'efficacité de la recherche

Deuxièmement, il nous semble que d'un point de vue strictement pratique, la doctrine juridique aurait tout intérêt à adopter ce type d'outil.

Il y a un intérêt assez évident qui est celui de permettre la *transmission* des données d'une étude. En effet, les études juridiques contentieuses comprennent souvent dans leur appareil critique un tableau et/ou un index permettant de recenser et éventuellement de classer les arrêts étudiés. L'inconvénient de ce procédé à l'heure de la jurisprudence massive est qu'il oblige le chercheur qui voudrait se fonder sur une précédente étude, à chercher à nouveau les arrêts cités, à les relire, et à reconstituer un nouveau tableau et/ou index. L'usage de bases de données permettrait donc un gain de temps considérable car elles pourraient directement intégrer les données sources, soit textuellement, soit à travers de liens.

Au surplus, l'usage de bases de données permettrait la *superposition* et la *rémanence* des analyses. Et là est selon nous l'intérêt principal de créer des bases de données critiques pour la doctrine en Droit. En effet, un même objet peut être abordé avec des perspectives différentes selon les auteurs et plusieurs objets peuvent être connexes, avec toutes sortes d'articulations possibles (complémentarité, divergence, compatibilité). Toute ces configurations peuvent s'articuler dans une base de données relationnelle ou dans des bases de données liées permettant de conjuguer les analyses.

La constitution de base de données permettrait aussi l'alliance d'études quantitatives et qualitatives. Bien qu'il soit à la mode de considérer le Droit à travers des statistiques, ce type

[1] FRISON-ROCHE M-A et BORIES S., « La jurisprudence massive », Rec. Dalloz, 1993, n° 39, p. 287 ;

d'approche est d'un intérêt scientifique assez faible dès lors qu'il n'est pas mis en relation avec des données qualitatives fines. Une base de données critique, permettrait donc de faire le lien entre l'étude de la jurisprudence et la *jurimétrie*, discipline qui peine encore à se faire une place mais qui inspire indirectement la démarche de certains juristes[2].

Reste cependant la question de la possibilité de la constitution d'un tel outil. Il nous semble que cette démarche est possible.

Concernant les arrêts et décisions juridictionnels, il a été récemment adopté un identifiant européen de jurisprudence[3] qui attribue un numéro unique à chacun, de sorte que la question de la constitution de la base de données matrice est quasiment réglée.

Ensuite, bien que de forme littéraire, les arrêts ou décisions juridictionnels sont des textes naturellement structurés. On y distingue des divisions nettes, des expressions régulières, des informations récurrentes et standardisées. Par l'utilisation du langage *xml*[4], il est donc possible de s'appuyer sur cette architecture pour extraire et organiser les données contenues. Et cette structuration est même partiellement automatisable à l'aide de programme écrit dans des langages de programmation relativement accessibles comme le *VBA*[5]. Reste qu'il faudrait s'accorder sur une normalisation de cette structure et des données collectées, d'abord en raison d'appellations ou de formulations légèrement différentes entre juridictions, ensuite pour permettre la portabilité et liaison des bases.

Notre contribution vise ainsi à ce que soit abordée la question de la constitution de bases de données propres à la doctrine juridique et celle de la recherche d'une normalisation d'une structure permettant les recherches croisées entre juridictions et entre études doctrinales.

[2] Voir notamment LOEVINGER L., « Jurimetrics : the methodology of legal inquiry », Law And Contemporary Problems, 1963, n° 28, p. 5 spéc. p. 8 qui indique que la jurimétrie (jurimetrics) « *s'intéresse à des problèmes tels que l'analyse quantitative du comportement judiciaire, à l'application de la théorie de l'information et de la communication à l'expression légale, à l'usage de la logique mathématique en Droit, à la collecte de données légales par des moyens électronique et mécaniques et à l'élaboration de formules de probabilité légales* » (traduction par nos soins) ; BORIES S., « Les décisions de justice à l'aune de la jurimétrie ou proposition pour une analyse du contenu de la communication », Communication Commerce Electronique, 2006, n° 7-8, avec une définition un peu différente qui classe la jurimétrie comme une science de l'information et une science de la communication.

[3] ECLI : European Case Law Identifier

[4] Extensible Markup Language

[5] Visual Basic for Applications

Open data et droit : quelles incidences sur l'administration publique du développement durable ?

Julien Vieira

Doctorant en droit public à l'Université de Bordeaux
Membre du centre Léon Duguit
Juriste en droit de l'environnement et de l'urbanisme

jvieira@hotmail.fr

Mots-clés : droit de l'urbanisme, droit de l'environnement, droit du numérique, *open data*, gouvernance environnementale, diffusion et partage des données.

Face à un constat de « maladministration » impliquant lourdeur des procédures et opacité informationnelle, les institutions publiques ont été amenées à modifier leur comportement mais également leurs modalités d'action. Démocratisation et efficacité des procédures publiques sont devenues des notions incontournables du fonctionnement de l'État, des collectivités territoriales et de leurs établissements publics.

Dans cette modernisation de l'action administrative, le numérique détient désormais une place indéniable. Loin d'être un gadget, les TIC (technologies de l'information et de la communication) ont acquis une place de choix dans les dispositifs juridiques encadrant les modalités d'amélioration des prestations de services publics et de rapprochement entre l'administration et l'usager.

Sans pour autant lui attribuer un monopole dans la mise en œuvre de ces procédés, le droit inscrit au cœur de ses réformes cet *aggiornamento* des outils techniques de l'administration comme un objectif impérieux. À ce titre, la pratique de l'*open data* a été saisie de manière conséquente par la matière juridique dans le cadre de l'administration institutionnelle. Ce procédé consistant à diffuser via le numérique des données libres d'accès et d'usage répond à de nombreux impératifs juridiques.

Les droits de l'urbanisme et de l'environnement illustrent particulièrement bien les enjeux de cette technique numérique pour une administration publique efficace et démocratique. Il s'agit des secteurs juridiques qui consacrent le plus la diffusion et le partage des données numériques : cela peut notamment concerner la transmission des données géographiques, des informations météorologiques ou encore des textes règlementaires.

Dans ce contexte, le thème de la confluence entre le numérique et le juridique est particulièrement pertinent tant le droit de l'environnement et les TIC sont dans une situation d'interrelation. En effet, d'une part l'*open data* permet de mettre en œuvre efficacement le droit à l'information et plus généralement le principe constitutionnel de participation du citoyen. L'accès aux données environnementales et urbanistiques via les TIC permet d'apporter des informations aux gouvernants ainsi qu'à la société civile qui concernent leur santé et leur sécurité. D'autre part, les consécrations

juridiques successives de la mise en place de différents portails numériques, rendant accessibles ces données essentielles à la connaissance de la population, légitiment cette pratique et facilitent son assise au sein du droit formel.

L'évolution du droit européen, du droit français ou encore d'autres droits nationaux atteste d'un réel intérêt de l'utilisation de ce procédé dans un contexte de mutation et de redynamisation de l'action publique. Cependant, le recours à l'*open data* n'est pas sans poser des questionnements du point de vue du respect de certaines libertés fondamentales comme le droit à la propriété intellectuelle, le droit à la vie privée ou encore le droit à l'égalité dans le cadre de la fracture numérique.

Cette communication a pour objet d'étudier plus en détails les conséquences de ce point de rencontre entre numérique et juridique. Quelles sont les implications de la consécration par le droit de l'urbanisme et de l'environnement de la pratique de l'*open data* ? Quels en sont les écueils ?
Quelles sont les obligations des gouvernants face à la consécration de cette nouvelle modalité ? Quelles difficultés la mise en œuvre de cette dernière peut-elle précisément soulever ?

Infractions et numérique – Quelles réponses du droit pénal ?

Elisa BARON, Maître de conférences en droit privé, Université de Bordeaux

Le développement du numérique va de pair avec celui des infractions commises grâce à cet outil ou à son égard. En tant que moyen de communication, le numérique permet de développer de façon exponentielle les activités illicites « traditionnelles » comme le trafic de stupéfiants ou encore l'escroquerie, et d'accroître le nombre de leurs victimes. Par ailleurs, la naissance et le développement du numérique ont nécessairement entraîné la naissance de comportements répréhensibles propres à la matière, tels que le piratage informatique. Comment le droit pénal appréhende-t-il ces phénomènes ? Dispose-t-il d'armes efficaces ? Autrement dit, a-t-il su s'adapter à la « révolution numérique » ?
Ces différents comportement sont autant de défis pour le droit pénal, défis qui touchent aussi bien à l'incrimination des comportements répréhensibles en la matière, qu'à la mise en œuvre de la répression pénale.

S'agissant en premier lieu du principe de la répression, le droit pénal utilise d'abord les infractions classiques, de droit commun, pour sanctionner nombre de comportements. Par exemple, les vols de données informatiques sont appréhendés par l'intermédiaire du vol de l'article 311-1 du code pénal, et les messages outrageants ou injurieux postés sur les réseaux sociaux peuvent être sanctionnés à travers la diffamation et l'injure prévus par la loi de 1881. Plus généralement, l'escroquerie, l'abus de confiance, l'usurpation d'identité, les falsifications ou les atteintes à la vie privée sont fréquemment employés pour réprimer des comportements commis informatiquement. Cette utilisation des incriminations de droit commun soulève des questions importantes. Est-elle efficace ou laisse-t-elle place à des vides juridiques privant de sanction des comportements pourtant choquants ? Ne conduit-elle pas à adapter ces incriminations, quitte à les dévoyer et mettre ainsi à mal le principe de légalité criminelle ? De plus, ces textes sont loin d'épuiser tous les comportements répréhensibles commis informatiquement.

C'est pourquoi ensuite, le droit pénal a prévu des infractions spécifiques pour lutter contre les comportements propres au numérique. Ainsi, il appréhende le piratage informatique à travers l'incrimination des atteintes aux systèmes de traitement informatisé de données (STAD) aux articles 323-1 et suivants du Code pénal. Y sont sanctionnés par exemple, l'introduction et le maintien dans ces STAD. Dans le même ordre d'idées, le Code de la

propriété intellectuelle sanctionne la négligence caractérisée consistant notamment à ne pas avoir mis en place un moyen de sécurisation de son accès internet[1], afin de protéger la propriété littéraire et artistique. Là encore, ces textes posent la question de leur efficacité et de leur complétude avec les infractions de droit commun précédemment évoquées.

En second lieu, au-delà du principe même de la répression, reste à s'interroger sur sa mise en œuvre. En effet, même s'il était acquis que ce dispositif permet d'appréhender tous les comportements envisageables commis par la voie informatique, l'anonymat rendu possible grâce à internet fait véritablement s'interroger sur les outils dont dispose le droit pénal pour débusquer les coupables et mettre en œuvre la répression. A cet égard, le Darkweb est révélateur. Le Darkweb, également appelé Deepweb, est une partie du net non référencée sur les moteurs de recherche traditionnels tels que Google ou Firefox, à laquelle tout un chacun n'a généralement pas accès. Cet internet « masqué » permet de garantir l'anonymat de ses utilisateurs et se révèle ainsi être une véritable plateforme pour les activités illégales. Pédopornographie, trafic de drogue, trafic d'armes, trafic d'êtres humains ou encore blanchiment y sont légion. Les cyberperquisitions mises en place par la loi LOPPSI II[2] sont-elles une réponse suffisante de la législation française ? Par ailleurs, ces activités posent nécessairement la question de l'application de la loi pénale dans l'espace et plus généralement de la coopération internationale en la matière.

Voici ainsi rapidement quelques-unes des questions qui feront l'objet de notre étude.

[1] Art. R. 335-5

[2] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, qui crée un article 706-102-1 dans le Code de procédure pénale rédigé de la sorte :
« Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction. ». L'article a été plusieurs fois modifié depuis.

Hébert-Marc GUSTAVE est docteur en Science politique et chercheur associé au Centre d'Études Juridiques et Politiques (CEJEP) de l'Université de La Rochelle. Ses travaux de recherche portent sur les implications sociales, politiques et juridiques du cyberespace.

CRIMES, VIOLENCES ET JUSTICE PARALLÈLE DANS LE CYBERESPACE

Le cyberespace désigne un « ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs[1] ». Pendant longtemps, ce milieu de communication faisait le lien entre les hommes et les machines et entre les machines elles-mêmes[2]. Mais, depuis l'apparition du Web 2.0, le cyberespace est devenu notamment un lieu d'interactions entre les hommes et les hommes[3]. Ainsi, toutes sortes d'interactions peuvent y avoir lieu : des relations amicales aux relations amoureuses, des relations familiales aux relations professionnelles, des relations criminelles spontanées aux relations criminelles organisées.

L'histoire du cyberespace a montré qu'il était un terrain fertile pour la commission de crimes et de violences ; crimes et violences contre les données, les infrastructures mais aussi contre les personnes, les biens et toutes sortes d'activités qui s'y déroulent. Depuis les activités cybercriminelles de Kevin D. Mitnick dans les années 1990 aux États-Unis, crimes et violences se sont considérablement accrus dans le cyberespace. La recrudescence mondiale des législations contre la cybercriminalité témoigne avec force ce développement.

Cependant, l'inadéquation entre la rapidité et le dynamisme de ces phénomènes et la lourde mécanique institutionnelle des systèmes judiciaires favorise le développement d'une justice parallèle dans le cyberespace. Il faut entendre par cela la répression de cybercrimes et de cyberviolences par les « webacteurs ». Ceux-là sont des « justiciers du Web », sorte de redresseurs de torts faits aux ressources essentielles du Web, à ses infrastructures, aux activités qui y ont lieu et à ses usagers. Ces gardiens autoproclamés du cyberespace sont caractérisés par leur anonymat et l'asymétrie de leurs actions. Le groupe les Anonymous[4] qui s'est distingué dans l'art de la justice expéditive en ligne, constitue une bonne illustration de ce mode de justice parallèle.

Pourtant, certaines difficultés sont liées à la nature des opérations de justice parallèle ainsi qu'au statut de ceux qui les mènent dans le cyberespace. Le caractère clandestin de ces actes de justice constitue le principal obstacle à l'établissement de leur nature. Selon l'observateur

[1] Définition tirée du Dictionnaire Le Robert. Voir aussi, ICHBIAH Daniel, *Les mots de l'informatique,* Paris, CampusPress, 3e éd., 2007, p. 80.
[2] PISANI Francis, PIOTET Dominique, *Comment le Web change le monde : des internautes aux webacteurs,* Paris, Pearson, 2011
[3] Ibid
[4] Voir, GICQUEL Camille, *Anonymous, la fabrique d'un mythe contemporai*n, FYP éditions, 2014, 96 pages

considéré, ces actes sont dits clandestins ou légitimes, criminels ou citoyens[5]. Quant à ceux qui les conduisent, leur anonymat et la clandestinité de leurs actes font balancer leur statut entre ceux de justiciers et de héros ou ceux de criminels, de hors la loi et de terroristes[6].

Qu'en est-il réellement de la nature des activités de justice parallèle en ligne ? Quel pourrait être le statut de ceux qui conduisent ces activités ?

Même si on peut reprocher aux opérations de justice parallèle en ligne leur caractère clandestin et asymétrique, il n'en demeure pas moins vrai que ces opérations poursuivent des causes justes. Considérant leur finalité, est-il convenable d'envisager une reconnaissance des activités de justice parallèle en ligne et une protection de leurs auteurs ?

- ⇨ La problématique que je souhaite voir aborder dans le cadre de cet atelier est celle relative à la nature des activités de justice parallèle en ligne (sont-elles des activités citoyennes ou criminelles ?) et au statut de ceux qui mènent ces activités (héros, justiciers, criminels, hors la loi ou terroristes ?).
- ⇨ Cet atelier intéresse au premier chef la communauté des juristes car il s'agit de savoir comment qualifier et traiter juridiquement des activités de justice parallèle en ligne ayant une juste finalité. Cet atelier fait également appel aux informaticiens car il s'agit d'activités qualifiées généralement de hacking. Les informaticiens peuvent aider à comprendre les procédés de ces activités caractérisées par leur forte complexité technique.

[5] GUSTAVE Hébert-Marc, *Géocyberstabilité : Pacification cyber-conditionnée des conflits en Relations internationales.* Thèse de doctorat : Science politique. Toulouse : Université Toulouse 1 Capitole. 2016, 540 pages.
[6] Ibid.

OUSMANE GUEYE

Doctorant en droit du numérique à l'université de La Rochelle

Thématique : Droit des données à caractère personnel

Contribution Convergences du Droit et d Numérique

Sujet : Le méga fichier TES ou la surveillance massive des Français

La révolution numérique a considérément modernisé les pouvoirs d'action de l'administration publique en offrant des possibilités insoupçonnées de traitements sur les données à caractère personnel des administrés. La crainte d'une surveillance généralisée du « Bug Brother » n'a jamais été aussi réelle qu'aujourd'hui depuis la naissance de l'informatique.

Le décret du 28 octobre 2016 relatif au fichier des Titres électroniques sécurisés (TES), illustre parfaitement la volonté de l'Etat d'instaurer une surveillance ingénieusement organisée à distance des populations. Le gouvernement, le 30 octobre 2016, un dimanche, la veille de la toussaint, a sorti un décret qui décide de ficher tout citoyen détenteur de passeport ou de carte nationale d'identité âgé de + 12 ans avec toutes leurs informations biométriques.

Le décret envisage la centralisation sur un même fichier les données biométriques de plus de 60 millions de citoyens Français. Concrètement, Il va collecter et enregistrer dans une base unique les données relatives à la filiation (noms, prénoms, dates, lieux de naissance et nationalité des parents), l'adresse, le courriel et le numéro de téléphone, ainsi que plusieurs données biométriques : la couleur des yeux, la taille, les empreintes digitales, mais aussi l'image numérisée du visage.

Considérant la nature et la quantité des données personnelles collectées, on peut facilement imaginer les vrais dangers de ce fichier qui constitue selon les experts un véritable recul de nos libertés fondamentales les plus élémentaires et surtout une remise en cause des fondamentaux de la loi Informatique et Libertés.

En effet, rappelons-le, l'adoption de la loi informatique et libertés était intervenue des suites de la controverse déclenchée en 1974 par le projet «Safari». Ce projet poursuivait une ambition comparable : la création d'un fichier centralisé dont la finalité serait le fichage des Français et l'interconnexion de tous les fichiers de l'administration. Les révélations qui avaient été faites par Philippe Boucher, alors journaliste au Monde, dans un article, intitulé « Safari ou la chasse aux Français«, qui, de fait, firent scandale, avaient permis l'instauration d'un arsenal juridique, afin de renforcer la protection des Français contre le fichage administratif, et policier. Le projet Safari fut ainsi suspendu, la loi «Informatique et Libertés» du 6 janvier 1978 adoptée et la Commission nationale de l'informatique et des libertés (Cnil) instituée.

Pour autant l'opiniâtreté des gouvernements successifs depuis ces dernières décennies n'ont pas fini de jeter le discrédit sur le rôle et les compétences de l'autorité de contrôle (la CNIL). En effet, l'Etat avait déjà manifesté sa volonté s'octroyer des prérogatives exorbitantes en se passant de l'avis de CNIL (son avis

n'est que simplement consultatif), depuis la réforme de la loi informatique 2004. Il s'en est suivi l'adoption de la loi (n°2011-267) du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI II) qui consacre un "principe général d'échanges d'informations entre administrations".

Sous prétexte de rationaliser la gestion des titres délivrés et de combattre la fraude et l'usurpation d'identité, le ministre de l'intérieur avait tenté de justifier la nécessité du fichier monstre, en écartant tout débat au fond malgré l'avis défavorable de la CNIL. Les réactions ont été vives : Axelle Lemaire, la secrétaire d'Etat chargée du numérique, avait critiqué dans les colonnes de l'Opinion sa publication, dénonçant "un décret pris en douce" et "un dysfonctionnement majeur"[1]. Le Conseil national du numérique (CNNum) quant à lui, a appelé le gouvernement à suspendre la mise en œuvre du décret.

Le président du conseil national du numérique, Mounir Mahjoubi, dans une interview accordée à MEDIAPART, a indiqué dans ce sens que « le gouvernement n'avait pas parfaitement conscience que les enjeux technologiques ont des enjeux démocratiques », poursuivant son raisonnement, il affirme également que « les élus et les hommes politiques sont complétement déconnectés des enjeux et des réalités du numérique». Une façon de dire que le gouvernement ne mesure pas la dimension hautement sensible de l'existence de ce méga fichier.

L'article 1 de la loi et libertés dispose que « l'informatique doit être au service de chaque citoyen… Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. » Or l'existence d'une base centrale aux mains de l'administration est en opposition avec les fondamentaux de la République[2].

Bien que les objectifs indiqués par le gouvernement soient parfaitement légitimes, il est techniquement prouvé qu'ils peuvent être atteints par d'autres voies. Dans une lettre ouverte intitulée «Méga fichier» : une centralisation «inutile et dangereuse», signée par une trentaine de personnalités reconnues des mondes du droit et de l'informatique et des défenseurs des droits de l'homme, il est proposé le stockage des données biométriques dans le document. Ce procédé existe déjà depuis quelques années pour certains documents administratifs notamment les titres de séjour. Depuis juin 2011, est mis en service le Titre de Séjour Européen Electronique qui est un document uniformisé au niveau européen. Ce titre est conçu avec les mêmes spécifications techniques et sécuritaires que le passeport biométrique. Il est équipé d'une puce sur lequel est enregistré une image faciale ainsi que les données inscrites sur le Titre. Grace à sa puce, le titre offre également les fonctions d'authentification et de signature électronique qui permettront d'utiliser des e-services.

Cette alternative, largement à la portée du gouvernement en termes de coût, de garantie de sécurité et de confidentialité, a été rejetée le 2 novembre par Bernard

[1] http://www.lejdd.fr/Politique/Creation-du-mega-fichier-de-tous-les-Francais-Axelle-Lemaire-critique-un-dysfonctionnement-majeur-822703

[2] LETTRE OUVERTE «Mégafichier» : une centralisation «inutile et dangereuse»
Par Un collectif de parents — 16 novembre 2016 à 14:11

Cazeneuve, au nom d'une prétendue "simplicité du fichier unique". Le ministre de l'Intérieur n'a pas manqué de préciser qu'il n'y aura "aucune puce dans la CNI"[3]. De nombreux experts informaticiens ont proposé plusieurs autres moyens de simplification, Mr François Pellegrini[4] avait laissé entendre qu'il est toujours possible d'arriver au même résultat sans effort ni sans coût, grâce à une fonction de hachage cryptographique. Ces techniques présentent l'avantage d'être extrêmement difficile à pirater, ce qui permettrait de lutter contre les contrefaçons tout en faisant obstacle à toute forme de fichage généralisé.

La question qui demeure sans réponse est de savoir pourquoi cette obstination du gouvernement sur le choix technique de la centralisation ?

L'examen des arguments évoqués par les détracteurs du fichier TES, permet de déceler deux principaux facteurs qui plaident en faveur d'un rejet pur et simple du fichier : un facteur politique et un facteur sécuritaire.

- Sur le facteur politique

La crainte de potentielles dérives est légitime comme se fût le cas dans les années 1940 avec le gouvernement de Vichy qui avait créé un fichier général de la population à des fins de surveillance. A partir du moment où le fichier existe, rien n'empêchera un futur gouvernement peu scrupuleux de s'en servir pour d'autres finalités que celles qu'on nous expose aujourd'hui (authentification). De même, le décret TES, prévoit lui-même, l'accès des services de renseignement ou sur réquisitions judiciaires, des services de police à la base de données centrale à des fins d'identification des individus. Le député Lionel Tardy avait indiqué à ce propos : "Ce simple décret pourrait être modifié au gré des majorités gouvernementales. Il n'est donc pas exclu que ce fichier, puisqu'il existera, soit détourné à des fins bien plus inquiétantes pour nos libertés publiques".

- Sur le facteur sécuritaire

Ce fichier en raison de la nature et de la quantité des données sensibles qu'il contient, va incontestablement devenir une cible de choix pour les hackers notamment ceux financés par les services de renseignement étrangers des pays très portés sur le cyber-espionnage. Sachant qu'aucun système informatique n'est infaillible comme le démontre Edward Snwoden, le risque de piratage va demeurer une menace permanente à laquelle le gouvernement devra faire face.

Cette contribution vise au-delà de tout débat au fond sur les implications juridiques et techniques qui résultent de la mise en œuvre du fichier TES, à favoriser une prise de conscience collective aussi bien dans la communauté des juristes, que dans celle des informaticiens.

[3] http://www.latribune.fr/technos-medias/mega-fichier-d-identite-pourquoi-le-gouvernement-s-est-tire-une-balle-dans-le-pied-613502.html

[4] Professeur des universités et vice-président délégué au numérique à l'université de Bordeaux, et chercheur au Laboratoire bordelais de recherche en informatique et à Inria

Pour les juristes, il s'agit surtout d'alerter sur la nécessité de réfléchir sur un dispositif juridique qui permettrait des limiter les ambitions démesurées du gouvernement qui menacent la vie privée et violent les principes de base applicables aux traitements des données à caractère personnel.

Pour les informaticiens, il est plus question de conscientiser la profession sur les dérives du "code". L'informatique doit être au service de l'Homme, sa finalité est d'améliorer le quotidien de celui-ci et non pas à limiter ou à porter atteinte aux droits fondamentaux. Par conséquent, la conception et la réalisation des programmes et applications informatiques doivent être encadrées par les règles de l'éthique et la morale. Le choix d'un code de bonnes pratiques serait bienvenu pour orienter l'exercice de la profession.

Une réflexion conjointe entre juriste et informaticien devrait donc permettre d'apporter des éléments de réponses sur les questions suivantes :

- En quoi ce fichier constitue-t-il une menace pour les libertés individuelles ?
- Quelles sont les faces cachées du méga-fichier TES ?
- Quelle garantie de sécurité pour un fichier de cette envergure ?
- Par quel moyen peut-on renforcer la protection de la vie privée face aux pouvoir de contrôle de l'Etat ?

Convergences du Droit et du Numérique – Contribution à l'atelier.

« Circulation transnationale et interception des données sur internet au service des activités de renseignement ».

Maxime KHELOUFI, *communauté juridique*.
Doctorant au Centre de Recherche et de Documentation Européennes et Internationales – Université de Bordeaux.

Actuellement doctorant travaillant sur *« les activités de renseignement et la protection des droits fondamentaux en Europe »*, le projet Convergences du Droit et du Numérique a naturellement retenu tout mon intérêt.

En effet, depuis plus d'un an, j'ai eu l'occasion, lors de mes recherches, d'observer qu'au sein même des activités de renseignement, le principal élément déclencheur de bouleversements ces dernières années avait trait au numérique et notamment à la collection et au traitement généralisé de données, ceci permettant ensuite leur transformation en « renseignement » utile à la prise de décision politique, notamment de la part du pouvoir exécutif.

Ce volet très automatisé des activités de renseignement renvoie aux activités de renseignement dites « techniques », par opposition aux activités de renseignement dites « humaines ». Même si cette distinction reste dans une certaine mesure de l'ordre de la théorie, la technique ne pouvant se passer d'interventions humaines, elle trouve toutefois une pertinence pour ce qui concerne les nouveaux enjeux juridiques induits.

La question la plus générale consiste à savoir quel équilibre trouver entre d'une part, l'usage de nouvelles techniques numériques au service du renseignement, ce dernier restant essentiel dans la perspective d'assurer la sécurité d'un Etat et de ses citoyens, et d'autre part, la protection des droits et libertés fondamentaux qu'il convient, dans une société démocratique, de garantir le plus largement possible.

Ces dernières années, on assiste à la construction de cadres juridiques, à la fois nationaux et européens (Union européenne et Conseil de l'Europe), venant poser certaines règles et limites aux activités de renseignement. Toutefois, la technologie numérique, alliée à certains vides juridiques semble permettre un contournement très aisé de ces cadres.

C'est ici qu'une question plus précise apparait et opère le trait d'union entre droit et numérique. **Comment les données circulent-elles sur le réseau internet et peuvent-elles techniquement faire l'objet d'interceptions à l'insu de leur expéditeur et de leur destinataire ?**

Ceci peut être illustré très simplement par l'hypothèse suivante. Un individu A envoie un courriel à son collègue de bureau B. Quel chemin sera emprunté par ce courriel ? Un élément d'extranéité, entendu ici comme un transit par l'étranger, peut-il apparaitre ? Le cas échéant, un service de renseignement étranger peut-il techniquement et aisément intercepter ce courriel entre nos deux collègues de bureaux ? Cette problématique étant par la suite renforcée par la possibilité pour le service de renseignement étranger ayant intercepté l'information de la transmettre aux services de renseignement de l'Etat dont les collègues de bureaux sont ressortissants.

Cet aspect technique est particulièrement intéressant pour mes recherches car il permettrait, si tel était le cas, de mettre en lumière un moyen de contournement du cadre juridique existant autour des activités de renseignement. Bien naturellement, cet aspect technique, m'est parfaitement obscur en tant que juriste et les connaissances d'un technicien sur la question seraient les bienvenues. Ceci démontre une nouvelle fois la nécessité pour les chercheurs de collaborer toujours plus afin d'apporter aux autres tout l'éclairage de leurs domaines respectifs. Aussi, je serais très intéressé de pouvoir apporter à un technicien certains éléments de réponse sur des points juridiques pouvant l'intéresser et l'aider dans ses recherches.

Peut-on penser le droit en algorithme ?

Schopenhauer définissait les 3 stades d'une révolution : *« Toute vérité franchit trois étapes. D'abord, elle est ridiculisée. Ensuite, elle subit une forte opposition. Puis, elle est considérée comme ayant été une évidence. »*

Les relations entre droit et numériques sont de plus en plus nombreuses et complexes. L'aspect quantitatif nous obligeant à évoquer le sujet des relations, l'aspect qualitatif nous conduisant à observer les difficultés provoquées par cette coexistence.

La coexistence du droit et du numérique est un sujet particulièrement d'actualité : protection des données, responsabilité des machines, encadrement légal des GAFA, justice prédictive, etc…

Il en ressort que ces relations peuvent être abordées sous 2 angles : soit l'adaptation du numérique au droit, soit l'inverse.

C'est ce dernier axe qui constituera le paradigme de la présente étude, au travers d'une question originale : peut-on penser le droit en algorithme ?

Le droit n'appelle pas ici de définition particulière, si ce n'est que la dataisation des données juridiques posera sans doute la question des règles à utiliser comme base de données, notamment la doctrine, qui pourrait voir son rôle affirmer (le jurisclasseur en numérique ou doctrine.fr sont des outils davantage utilisés que les bases de données brutes de la cour de Cassation ou du Conseil d'Etat).

L'algorithme est un terme qui nécessite plus d'attention, de par son caractère polysémique. En effet, celui-ci est aujourd'hui perçu uniquement sous son angle numérique. Pourtant, l'algorithme est à l'origine une simple suite d'instruction articulée selon une forme logique.

Gérard Berry (1948–), chercheur en science informatique en donne la définition suivante :

« Un algorithme, c'est tout simplement une façon de décrire dans ses moindres détails comment procéder pour faire quelque chose. Il se trouve que beaucoup d'actions mécaniques, toutes probablement, se prêtent bien à une telle décortication. Le but est d'évacuer la pensée du calcul, afin de le rendre exécutable par une machine numérique (ordinateur…). On ne travaille donc qu'avec un reflet numérique du système réel avec qui l'algorithme interagit. »

L'algorithme est un ensemble de programmes permettant d'obtenir un résultat (fonctionnalité). Par exemple, obtenir un tableau est la fonctionnalité du programme excel. Le programme est une suite d'instruction permettant, si elles sont correctement exécutées, d'obtenir le résultat souhaité.

En réalité, l'algorithme est un raisonnement logique pouvant se vérifier indépendamment du langage de programmation, l'algorithmique exprime les instructions résolvant un problème donné **indépendamment des particularités de tel ou tel langage**. Si le programme était une dissertation, l'algorithmique en serait le plan, une fois mis de côté la rédaction et l'orthographe.

L’algorithme permet d’organiser une suite d’instruction s’exécutant sans que l’humain est à intervenir à chaque fois.

Enfin, le terme penser signifie d’une part, il s’agira de plonger dans la logique algorithmique, dans la mesure du possible pour un profane, afin de tenter d’en cerner les mécanismes et les limites quant à l’intervention humaine. Et d’autre part, d’en comparer les ressorts logiques avec ceux du droit, afin d’observer dans quelle mesure il est possible (ou non) de les calquer.

L’intérêt d’une telle démarche n’est pas évident de prime abord : le droit concerne l’organisation des hommes en sociétés, l’algorithme permet le fonctionnement d’un ordinateur. Le droit est l’art de la sémantique là ou l’algorithme est mathématique.

Pourtant à y regarder de plus près, la comparaison semble possible, pour au moins deux raisons :

D’une part, l’algorithme est un raisonnement logique, qui ne repose pas nécessairement sur des données mathématiques.

Et d’autre part, le droit, en vue d’organiser la vie en société, doit lui aussi s’astreindre à un raisonnement logique : le syllogisme judiciaire. Le syllogisme judiciaire, comprend une majeure, une mineure et une conclusion : D est puni de la peine P, C a commis l'infraction D, D aura la peine P.

Le droit obéit donc à son propre algorithme.

Il semble cependant qu’un tel raisonnement ne colle qu’imparfaitement à la réalité, et n’est d’ailleurs applicable au sens strict qu’en droit pénal, en vertu du principe d’interprétation stricte de la loi. En effet, la majeure (la règle de droit applicable) dépend au préalable de la qualification des faits, et donne déjà lieu en soi à un contentieux important (en cas de concours de responsabilités civiles, ou d’invocabilité d’un traité).

Aussi l’intérêt de ce sujet est-il double : sur le plan théorique, l’utilisation d’algorithmes en vue d’exercer une fonction juridique est une réalité, a-t-elle point qu’elle fait planer une réelle menace sur les professions juridiques telles que nous les connaissons aujourd’hui (référence nécessaires).

Mais cet aspect pratique, cette crainte qu’inspire la technologie (au-delà de la science-fiction) doit être doublé d’une approche plus théorique, qui vient la compléter. En effet, il s’agira ici de penser l’algorithme et le droit dans leur complémentarité, dans leur similarité en matière de raisonnements, de buts. Il ne s’agit pas de nier les différences importantes qui les séparent, mais de chercher les dénominateurs communs à même de permettre la cohabitation du droit et du numérique.

Aussi la question centrale est celle de savoir s’il est possible d’« algorithmer » le droit ? Et si oui, dans quelle mesure.

Pour répondre à cette question, la démarche se fera en deux temps : tout d’abord, décomposer l’algorithme, et le replacer dans un paradigme sémantique, et non algébrique (I). Il sera alors possible d’observer l’imbrication des raisonnements algorithmique et juridique, en se demandant si ce dernier doit s’insérer dans le premier, ou inversement (II).

I. La logique, point de convergence entre l'algorithme et le droit

Un algorithme est une suite d'instructions, qui une fois exécutée correctement, conduit à un résultat donné

A. La logique algorithmique : démystification de l'algorithme numérique

L'algorithme peut se diviser en 3 éléments principaux :

- Une fonctionnalité, c'est-à-dire un objectif, un résultat à atteindre.
- Une variable, qui est une « boite » ou l'on stock le résultat d'un calcul (calcul choisi par le programmateur, le calcul étant une instruction donnée à la machine)
- Un raisonnement logique, le test

Les instructions pouvant être exécutées par un algorithme

Les ordinateurs, quels qu'ils soient, ne sont capables de comprendre que quatre catégories d'instructions : l'affectation de variables, la lecture / écriture, les tests et les boucles.

En effet, l'algorithme n'est pas qu'une suite d'instructions, il est également et surtout un enchainement logique entre les instructions. Une instruction A correspondra à une situation précise, et ne pourra être donné si l'on se trouve dans une autre situation.

La programmation d'un algorithme est donc sur le principe, relativement simple : il faut tout d'abord programmer des variables. Puis, créer un test logique permettant de vérifier la variable, et de la réponse (vrai ou faux) à ce test va découler l'instruction à suivre.

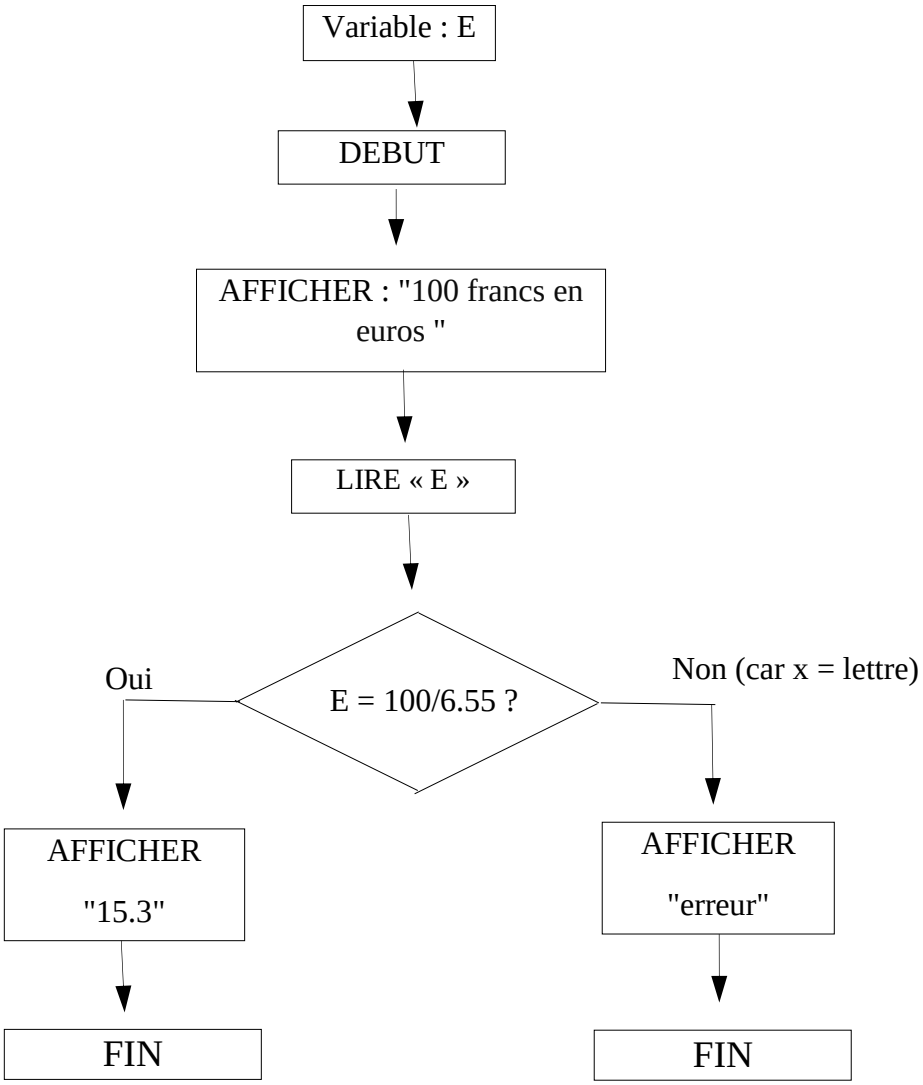
Exemple :

Concevoir un algorithme qui convertit en euros un prix en francs donné par l'utilisateur

Si 1 euro représente 6,55957 F, alors x francs est représenté par $x \times 1 \div 6{,}55957$ soit $x \div 6{,}559957$ euros.

Dans l'algorithme, on va noter x le prix en francs et e le prix en euros.

```
Variable E en Entier (E = x/6.55)
Début
Ecrire "x francs en euros :"
Lire E
Si E (vrai) Alors
  Ecrire "prix en euros = E"
Sinon
  Ecrire « erreur »
Fin
```


Variable : E
DEBUT
AFFICHER : "100 francs en euros "
LIRE « E »
E = 100/6.55 ?
Oui
Non (car x = lettre)
AFFICHER "15.3"
AFFICHER "erreur"
FIN
FIN

B. L'application au droit

Les instructions applicables dans le cadre d'un algorithme numérique peuvent se transposer en droit :

1) La variable, c'est le besoin de stocker une information au cours d'un programme, on utilise une **variable**.
   Pour employer une image, une variable est une **boîte**, que le programme (l'ordinateur) va repérer par une **étiquette.** Pour avoir accès au contenu de la boîte, il suffit de la désigner par son étiquette. Traduit en droit, c'est une notion définie. Une fois définie, la notion peut être utilisée à nouveau

2) La lecture/écriture, ce sont l'interaction entre l'utilisateur et la machine, la machine lit une instruction, puis écrit la réponse qu'elle y apporte en appliquant le programme. Traduit en droit, il s'agit davantage ici de questions de langage et de définition

3) Le test, c'est l'avancée du raisonnement pour arriver au résultat. Ce raisonnement s'écoule selon une logique, au travers de tests logique.

Un test peut s'exprimer sous 2 formes :

a) **Si** booléen **Alors**
   Instructions
   Finsi

b) **Si** booléen **Alors**
   Instructions 1
   Sinon
   Instructions 2
   Finsi

Un booléen est une expression dont la valeur est VRAI ou FAUX. Cela peut donc être

- une variable (une notion) de type booléen
- une condition

La variable ayant déjà été défini, il faut préciser ce qu'est une condition. Il s'agit d'une comparaison entre deux valeurs.

En droit cela se traduit de la manière suivante :

Si responsabilité de l'article 1240 (vrai) **Alors**
Indemnisation **(VARIABLE)**

OU

Si chiffre d'affaire < 82 200 euros **Alors**
Régime des micro BIC **(CONDITION)**

4) La boucle, c'est la sécurité du raisonnement, qui en assure la fiabilité. En effet, la boucle permet, en cas de réponse non comprise dans les possibilités, de ne pas aller au

bout du raisonnement. De cette manière, le programme arrive toujours à un résultat (attention, ce résultat peut être de signaler l'erreur à l'utilisateur. Exemple, voulez-vous un café, la réponse attendue est oui ou non. En cas de « peut-être », la boucle de l'algorithme renvoi un message « saisir à nouveau » afin d'obtenir une instruction possible.

Variable 1240 en Caractère
Début
Ecrire "l'article 1240 est-il applicable ? (O/N)"
Lire 1240
TantQue 1240 <> "O" et 1240 <> "N"
Lire 1240
FinTantQue
Fin

De même, l'algorithme est un cheminement, un raisonnement logique, en vue d'obtenir un résultat. De ce point de vue, la parallèle peut être aisément fait avec le droit, et notamment le syllogisme judiciaire

II. Application pratique de l'algorithme au raisonnement juridique

A. L'insertion du droit dans un raisonnement de type algorithme

Prenons un exemple classique en droit, le droit de la responsabilité civile.

Pour une question de responsabilité, 3 algorithmes sont nécessaires (nous le verrons plus tard, il s'agit ici d'un postulat arbitraire, résultant d'un choix humain) :

- Algorithme 1 : détermination de la règle applicable : règle générale ou règle spéciale ?
- Algorithme 2 : en supposant l'application de la règle spéciale, quelle règle spéciale appliquer ?
- Algorithme 3 : sur la base de la règle spéciale, quelle solution donner au litige ?

Si l'on applique l'algorithme 1, voici ce que l'on peut écrire :

Variable règle applicable **en Entier**
Début
Ecrire « Il y a-t-il un produit défectueux ? »
Lire règle applicable
Si produit (vrai) ET

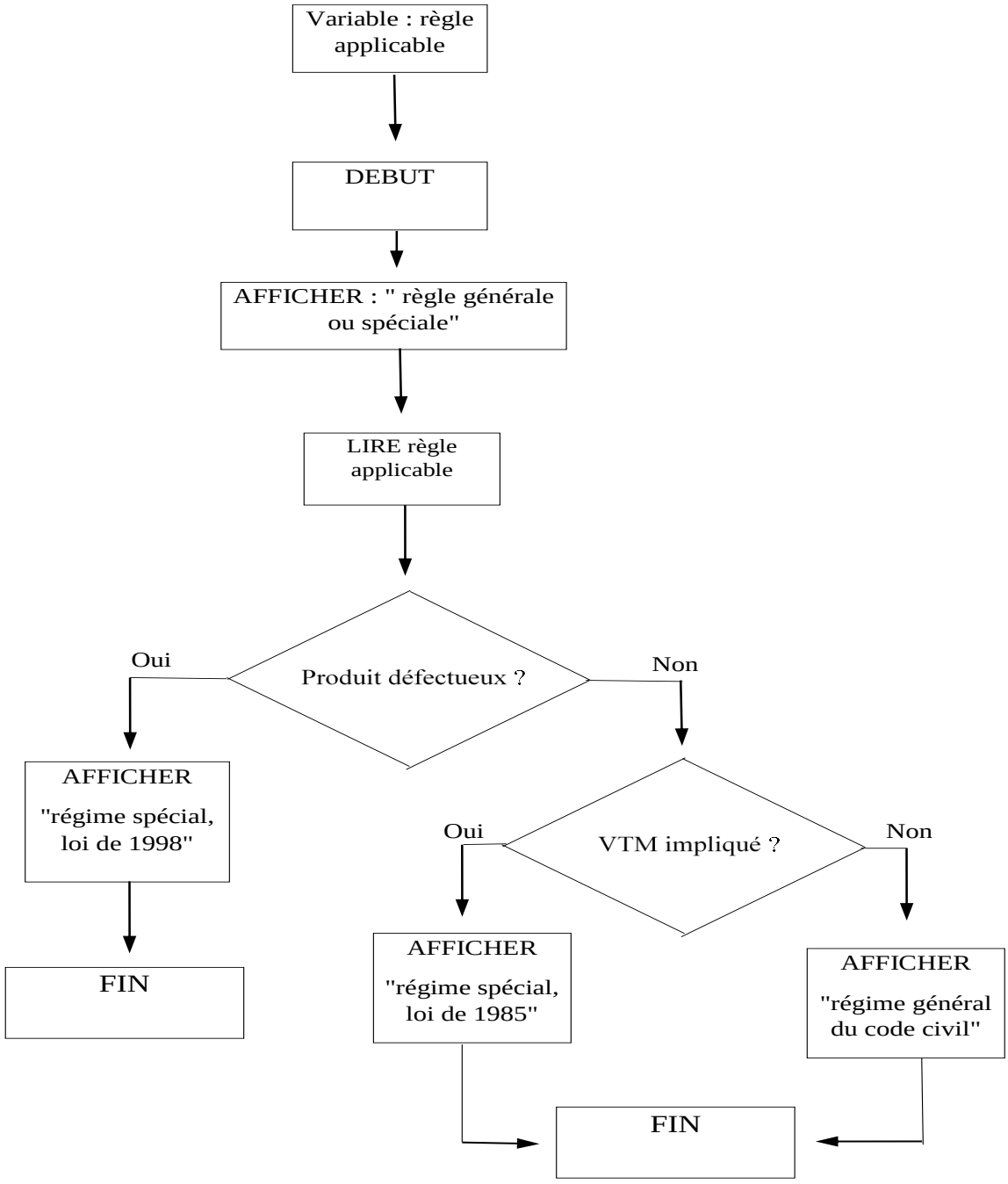
Défaut (vrai)

Alors
Ecrire "régime spécial, loi de 1998"

Sinon
Si Véhicule terrestre à moteur (vrai) ET

Impliqué (vrai)

Alors
Ecrire "régime spécial, loi de 1985"
Sinon
Ecrire "règle générale"
Finsi
Fin



Deux constations peuvent être faites à ce stade :

Tout d'abord, le raisonnement juridique est ici vérifié par le raisonnement juridique dès lors que la situation se complexifie, du fait que plusieurs règles peuvent potentiellement s'appliquer.

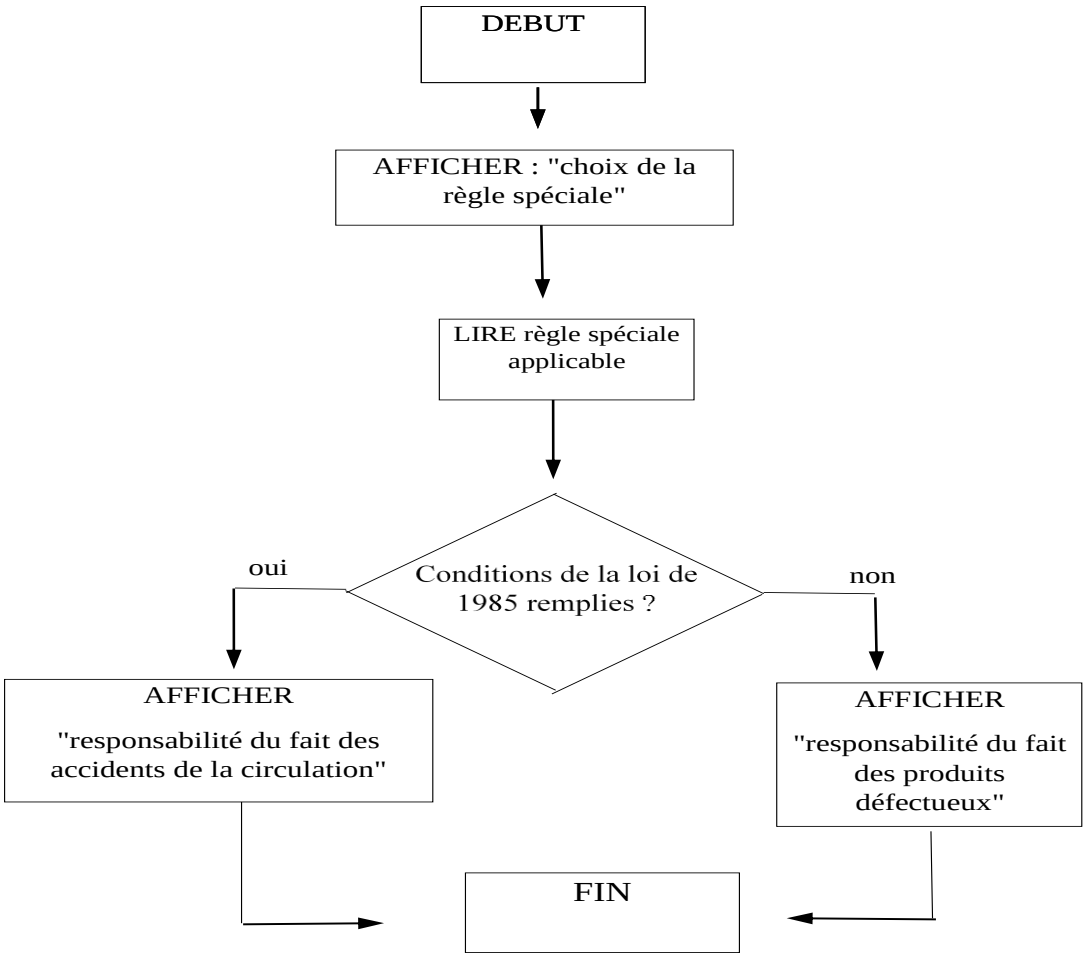
En effet, que faire lorsque la situation appelle plusieurs responsabilités ?

Il faudra alors appliquer l'adage « Lex specialis derogat legi generali »

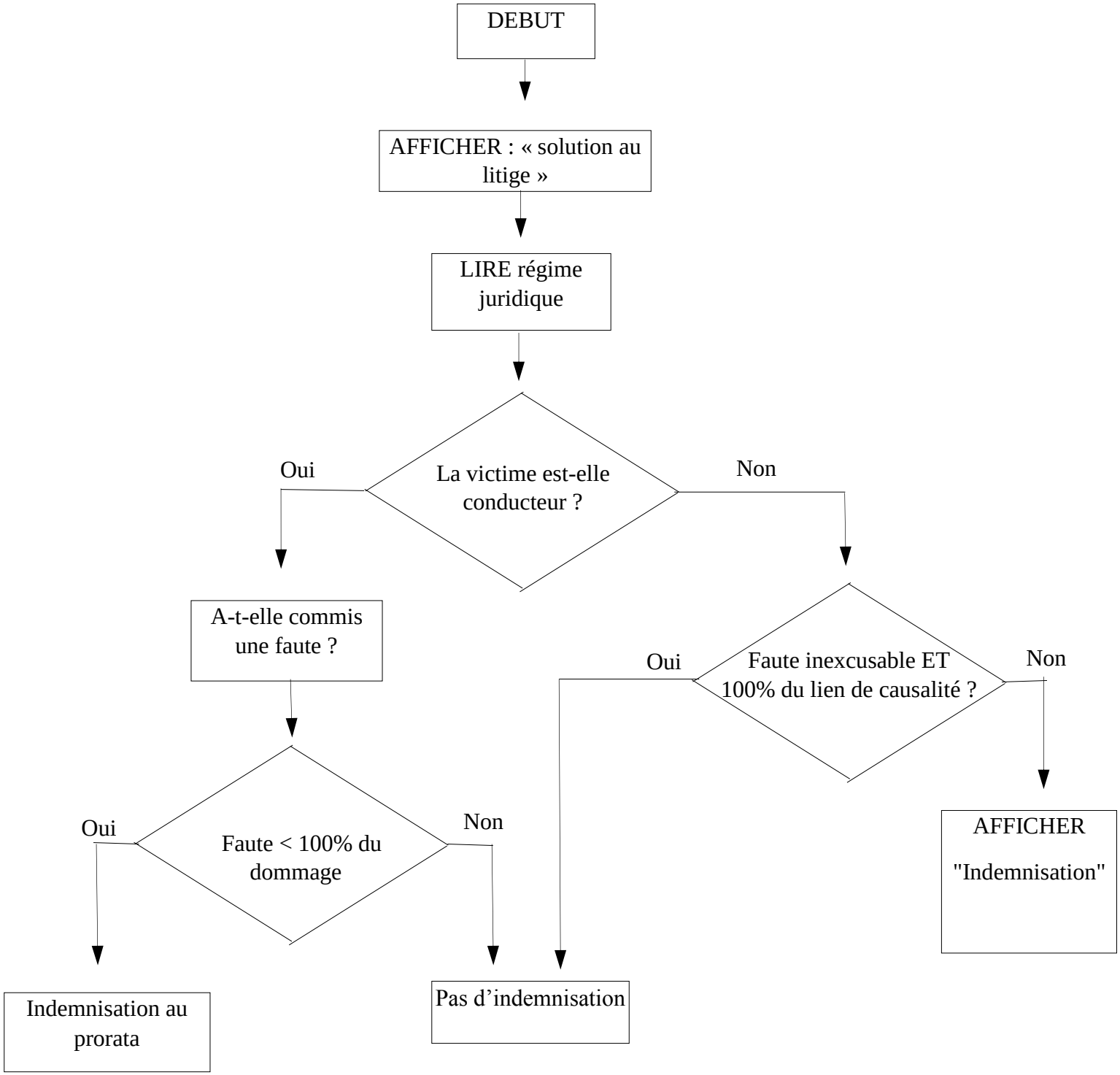
De plus, un tel algorithme nécessite une programmation humaine à triple titre

- En amont, déterminer quels sont les questionnements pertinents : ici opérer une distinction primaire entre règle générale et règle applicable, puis poser comme question la présence d'un produit défectueux, puis de l'implication d'un VTM. Ces questionnements auraient pu être tout à fait différents, il s'agit ici d'un biais humain.
- Ensuite, l'affectation des variables est également une opération humaine : il a ici été arbitrairement décidé de ce qu'était un VTM, un produit, un défaut, etc…
- Enfin, le déroulé logique des tests répond également à une programmation humaine.

Algorithme 2 :



Algorithme 3 :



Conclusions :

- Un algorithme nécessite une programmation, donc une intervention humaine
- L'algorithme implique un raisonnement qui se termine immanquablement par oui ou par non. Un tel raisonnement peut être vu par le juriste comme réducteur, dans la mesure où de nombreuses règles, qu'ils s'agissent de lois de jurisprudences, n'opèrent

pas de rupture aussi brutale, préférant les solutions conditionnées (référence nécessaire). On notera que la sémantique permet ici des nuances que ne permettent pas a priori les chiffres.

Les enjeux de l'utilisation de la visioconférence dans le procès pénal

Depuis le début des années 2000, le champ d'application de la visioconférence dans le procès a été sans cesse élargi. Historiquement introduit en droit français comme correctif de situations d'absence problématiques, l'usage de la visioconférence tend aujourd'hui à devenir une véritable alternative à la présence physique des justiciables et des autres acteurs du procès, et ce en différentes matières. Ainsi, en matière administrative, le contentieux des étrangers a accueilli cette forme d'audience virtuelle d'abord pour les audiences relatives au placement d'étrangers en rétention administrative[1] puis pour celles relatives aux décisions de non-admission de séjour au titre de l'asile[2]. L'usage de la visioconférence est également prévu devant les juridictions civiles depuis 2007[3], bien que sa pratique ne semble que peu répandue en la matière. Mais c'est surtout l'utilisation de la visioconférence dans le procès pénal qui apparaît comme étant la plus développée, et d'ailleurs la plus problématique.

En effet, cette expansion, motivée par la volonté de limiter les coûts judiciaires, ne manque pas de soulever nombre de difficultés sur le plan tant juridique que sociologique, qui tiennent aux modalités de mise en œuvre de ce procédé.

Sur le plan juridique, ce sont **les grands principes et droits fondamentaux de la procédure pénale qui entrent en confrontation avec l'utilisation de la visioconférence**.

Le recours aux audiences dématérialisées du fait de l'usage de la visioconférence vient ainsi questionner la protection des droits de la défense. La place de l'avocat pose notamment question. Si la loi lui offre une option entre se trouver à l'audience ou aux côtés de son client, le choix offert par cette alternative est source de bien des hésitations. Faut-il privilégier la présence de l'avocat dans la salle d'audience pour lui permettre de convaincre pleinement le tribunal, au risque d'affaiblir sa fonction de conseil du client loin de lui ? Et dans cette hypothèse, comment garantir la confidentialité des échanges entre l'avocat et son client ? Faut-il au contraire privilégier l'assistance aux côtés du client détenu, pour l'accompagner et le conseiller directement, au risque d'affaiblir considérablement sa force de persuasion du tribunal ? Et même dans cette hypothèse, il n'est pas certain que la question de la confidentialité des échanges entre l'avocat et son client soit résolue puisque ce qu'il se passe dans la salle de visioconférence du lieu de détention entre l'avocat et le prévenu détenu est diffusé instantanément dans la salle d'audience…

La question de la confidentialité des échanges se pose d'ailleurs à un autre niveau, et tient cette fois à la confidentialité ou plus précisément à la sécurité des télécommunications audiovisuelles. Alors que la visioconférence peut être utilisée au stade de l'instruction pour les auditions et interrogatoires, il est en effet impératif de pouvoir assurer, au plan technique, une parfaite sécurité de la liaison pour garantir le secret de l'instruction.

---

1 Art. L. 222-4 et s. CESEDA.

2 Art. L.213-9 du Code de l'entrée et du séjour des étrangers et du droit d'asile.

3 Loi n°2007-1787 du 20 décembre 2007 - art. 25

C'est encore la question de la qualité de la contradiction qui se pose. L'intermédiaire technique qu'est l'écran ne permet en effet pas la spontanéité des échanges qui est celle qui découle d'une présence physique et simultanément de tous les acteurs du procès dans la même salle d'audience.

C'est également la question de la publicité des débats qui est susceptible de se poser. L'article L. 111-12 du Code de l'organisation judiciaire prévoit que la publicité doit être organisée dans les deux salles d'audience reliées par visioconférence. Il paraît pourtant pour le moins incongru d'imaginer que les lieux de détention deviennent des lieux ouverts au public pour assurer cette publicité. Il faudrait alors considérer que l'organisation de la publicité dans la salle d'audience au Palais de justice suffit dès lors que le public voit lui aussi l'écran sur lequel l'image du prévenu est diffusée[4]. Mais c'est alors une autre question qui se pose, et qui tient cette fois à la mise en œuvre technique de la visioconférence. Quel cadrage choisir ? La publicité des audiences vise en effet à permettre aux citoyens de contrôler que la justice s'exerce de façon indépendante et impartiale, et notamment de contrôler que les parties ne sont victimes d'aucune pression. Or, un plan strict sur les parties au procès permet certes de voir avec précision leur visage, leurs expressions, leur langage corporel, mais ne permet pas de voir leur environnement. Cette question peut d'ailleurs s'avérer cruciale lorsque la visioconférence est utilisée aux fins de prolonger la garde à vue ou lors des défèrement en vue d'une comparution immédiate. A l'inverse, un plan trop large ne permettrait pas d'apprécier à leur juste valeur les comportements des parties, alors qu'il s'agit là d'un élément important de la manifestation de la vérité, le contentieux pénal étant un contentieux éminemment personnel.

Sur un plan sociologique, **la visioconférence vient également perturber le rituel judiciaire**, en isolant les personnes entendues par visioconférence de l'ambiance solennelle de l'audience, ce qui peut par la suite avoir des répercussions sur la réception de l'audience et plus avant de la décision de justice. Les effets « impressionnants » de l'apparat judiciaire ne sauraient en effet être véhiculés de la même façon pour les justiciables lorsqu'ils se trouvent placés eux-mêmes sur la scène du théâtre de la justice et lorsqu'ils paraissent assister à ce rituel à distance devant un écran de quasi-télévision. C'est donc toute la dimension pédagogique et cathartique de la justice pénale qui est susceptible d'être perturbée par l'utilisation de la visioconférence dans le procès pénal.

Pour toutes ces raisons, si la visioconférence ne mérite sans doute pas d'être totalement condamnée, il importe de réfléchir aux conditions de sa mise en œuvre, sur le plan technique comme juridique. Telles sont les quelques questions qui seront abordées lors de notre étude.

4 Cass. crim., 16 mars 2016, n° 15-87.644

Thème D

« Droit des données à caractère personnel »

Les discussions de ce thème ont porté sur les points suivants :

1. Évolution du droit relatif aux données à caractère personnel ;
2. Diversité des pratiques constatées ;
3. Nature des données à caractère personnel.

Évolution du droit relatif aux données à caractère personnel

Le droit des données à caractère personnel, issu en France de la loi « Informatique et Libertés » de 1978, va connaître une profonde transformation avec l'entrée en vigueur en 2018 du Règlement général sur la protection des données (RGPD). Le RGPD propose une harmonisation des règles et des procédures, tout en laissant une marge d'appréciation aux États pour la mise en œuvre de certaines dispositions. Ainsi, des différences entre les pratiques des États pourront perdurer, sans qu'il soit possible actuellement de les énumérer précisément, puisque les États membres ont jusqu'au 25 mai 2018 pour concrétiser le RGPD.

Si les principes généraux ne changent pas, la mise en œuvre opérationnelle des droits subit des modifications substantielles. En France, cela conduira au basculement du régime d'autorisation actuellement mis en œuvre par la CNIL à un régime répressif de « redevabilité » (« *accountability* ») des responsables de traitement. De nouvelles obligations sont créées à la charge des responsables de traitement, exprimées en termes d'objectifs (tels que les obligations de « portabilité des données », de « sécurité », de « recours à des procédés d'anonymisation », etc.) sans que leur mise en œuvre soit précisément décrite. Cela suscite une certaine nervosité chez les responsables de traitement et sous-traitants.

À ce titre, la sécurité des données doit-elle être considérée comme un objet juridique ou seulement technique ? Une section du RGPD est intégralement consacrée à ce sujet. Est-on face à une obligation de moyens ou de résultat ? Il semble qu'il s'agisse d'une « obligation de moyens renforcée », les moyens mis en œuvre étant comparés à l'état de l'art. La mise en place de référentiels (comme ceux devant être rédigés par un GIP dans le cas du partage, de la transmission et de l'hébergement des données de santé, par exemple) doit permettre de définir un niveau de sécurité minimal, et évolutif afin de rester conforme à l'évolution des techniques.

L'obligation de notification à l'autorité de contrôle pose également question. S'il ne s'agit que d'une information factuelle, elle peut conduire au lancement d'une enquête conduisant à l'incrimination du notificateur pour ses manquements. Peut-elle être considérée comme une auto-incrimination ? Comment concilier le droit au respect de la vie privée et le droit au procès équitable ? Ces éléments ont déjà pu être testés en pratique lors de l'affaire « Orange », en 2015.

Le RGPD pose une définition très large des données de santé et de leur origine (indifférence de la source), qui conduit à faire disparaître le flou relatif à la notion de « donnée de bien-être », qui n'a en fait aucune réalité juridique. Étant donné que l'acceptation large de la notion de données de santé se trouve dans le préambule du RGPD, il reviendra à la CJUE d'interpréter la définition des données de santé à la lumière de ces dispositions du préambule du règlement. La distinction entre données de bien être et données de santé devra donc se faire au prétoire, ou éventuellement par les autorités de protection des données. Cette question a déjà été abordée par le G29 dans un document intitulé « *Health data in apps and devices* ».

Sur le plan des droits fondamentaux, la fondamentalisation de la protection des données nécessite d'organiser sa coexistence avec d'autres droits fondamentaux, en s'appuyant sur le principe de proportionnalité. L'un des sujets de friction récemment mis en exergue est celui des activités de renseignement, qui viennent porter atteinte à la protection des données à caractère personnel et à d'autres droits fondamentaux. Ces activités nécessitent un encadrement prenant en compte les questions des finalités, de la proportionnalité et de la création de garde-fous. La technique joue ici un rôle important, les réglementations (nationale et/ou européenne) pouvant être aisément contournées par la mise en œuvre de procédures techniques, comme le routage des données sur l'Internet permettant l'interception « hors sol » dans le cadre d'échanges croisés de données entre services de différents États.

Diversité des pratiques constatées

En parallèle du droit et de son évolution, on constate une très grande diversité de pratiques.

La publicité ciblée est un très grand moteur d'innovations techniques et de pratiques, du fait des montants en jeu au niveau mondial. Elle conduit de nombreux fournisseurs de solutions techniques à mettre en œuvre des mécanismes de collecte, parfois sans laisser le choix à leurs usagers.

Tel est le cas de la géolocalisation, que la plupart des usagers ne savent pas désactiver. Tel est aussi le cas de la collecte des conversations d'ambiance, effectuée de façon passive par certains équipements de salon sans que l'usager en ait conscience (du fait de Conditions générales d'utilisation peu claires, de façon délibérée ou non) et sans que ces fonctionnalités puissent être facilement désactivées, si tant est qu'elles puissent l'être. Le fait de ne plus pouvoir retirer la batterie de son ordiphone est une modalité technique qui a une influence sur le niveau de confidentialité que l'on peut atteindre. De nombreux équipements peuvent être détournés de leur usage pour collecter des données à caractère personnel : courbe de consommation électrique instantanée renseignant sur le film que l'on visionne, accéléromètre des ordiphones pour identifier la démarche des personnes ou les vibrations de l'air dues aux conversations ambiantes, etc. Afin de limiter ces risques, il est essentiel d'appliquer les principes du « *privacy by design* » lors de la conception des dispositifs.

Les notions de loyauté et de finalités de la collecte sont essentielles sur le plan juridique pour éviter les abus. Elles conditionnent également la mise en œuvre effective du consentement de l'usager à la collecte de ses données. Or, les formes de consentement sont profondément renouvelées par le numérique. Dans l'environnement en ligne, qu'est-ce qu'un consentement explicite, ou encore spécifique ? Les usagers sont face à un « *privacy paradox* », à savoir l'écart entre l'affirmation de la préoccupation personnelle et les usages constatés.

Ceci conduit à une privatisation du droit, par la recherche de la responsabilisation d'acteurs privés ayant des objectifs qui ne paraissent pas toujours conciliables avec ceux de la protection des données. Cette asymétrie conduit à une surestimation du caractère protecteur du RGPD, dont il faudrait pouvoir mesurer pratiquement l'effectivité. Selon quels critères cette mesure de l'effectivité peut-elle être étudiée ? Quels outils pourraient-ils permettre aux individus d'assurer la protection de leurs données personnelles, de pouvoir choisir le niveau de protection qu'ils souhaitent, ou de prendre conscience des enjeux autour de la protection des données personnelles ? Cela pourrait être l'objet d'études empiriques portant sur l''effectivité de la protection des données du RGPD, sur la base d'un échantillon de personnes et d'entreprises.

Nature des données à caractère personnel

On constate une prolifération de données et d'informations, constituées tant de données brutes que de données induites, résultant d'un traitement appliqué à un unique ensemble de données brutes ou bien par croisement de plusieurs ensembles.

La question de la définition même des catégories de données semble parfois faire débat. Qu'est ce qu'une donnée ? À partir de quel moment sommes nous face à une donnée à caractère personnel ? Par capillarité, il semble que toute donnée dont la variation est conditionnée par l'action d'une personne puisse en théorie être considérée comme une donnée à caractère personnel.

Une distinction supplémentaire est effectuée avec le statut de donnée sensible. Tout comme le rythme des pas d'une personne, sa voix renseigne sur l'état émotionnel et de santé de cette personne. La voix doit-elle donc toujours être considérée comme une donnée sensible ? Il semble plus pertinent que cette catégorisation soit conditionnée par l'usage qui est fait de la donnée, et donc de la nature des traitements qui lui sont appliqués.

Le RGPD définit de manière exhaustive ce qui peut être une donnée sensible mais il semble qu'en pratique les utilisateurs, de manière subjective, considèrent bien plus de leurs données comme étant sensibles. Or, elles ne bénéficient pas du régime juridique de protection renforcée imposant le principe d'interdiction de traitement des données. En la matière, la marge de manœuvre des États-membres est importante, le consentement de la personne et les exceptions possibles sont nombreuses. Malgré tout, l'existence du principe d'interdiction oblige les États à se justifier de la licéité des traitements réalisés contrairement aux traitements opérés sur des données à caractère personnel non sensibles. Ici encore, il semble que responsables de traitement et utilisateurs ont une approche subjective des notions parfois en décalage avec les catégories créées par le droit.

Synthèse réalisée par François Pellegrini à partir des éléments débattus collectivement lors de la table ronde

Convergences du droit et du numérique

Contribution de Sarah Cadiot – Avocate en droit de la protection des données personnelles

Communauté d'appartenance : communauté juridique

Sujet : Moins de Dix-Huit Moins pour se Préparer au Règlement Européen sur la Protection des Données Personnelles

L'adoption du règlement européen sur la protection des données personnelles (le « Règlement ») par le Parlement européen le 14 avril 2016 constitue l'aboutissement de longues années de négociations et marque un tournant majeur dans la régulation des données personnelles, tant pour les individus que pour les entreprises.

Le Règlement conserve les principes clefs du droit de la protection des données personnelles prévus par la Directive 95/46/EC. Plus de 25 ans après l'adoption de la Directive, le Règlement modifie ces principes afin qu'ils n'appliquent plus logiquement aux technologies actuelles et, on peut l'espérer, aux technologies de demain. Le Règlement renforce les droits des individus concernant le traitement de données qui leur sont personnelles et, en cela, vient répondre à une demande croissante du public de plus de confiance et de maitrise de ces données dans l'environnement numérique.

Le nouveau régime demande des efforts de mise en conformité significatifs aux entreprises traitant les données personnelles, quel que soit leur secteur d'activité. Le Règlement apporte un certain nombre de mesures visant à faciliter des obligations jusque-là fastidieuses, très formalistes, et souvent trop peu harmonisées au niveau européen. Néanmoins, ces obligations sont généralement plus importantes et seront soumises à un régime de sanctions financières que les législateurs européens ont volontairement voulu prohibitif, pouvant s'élever jusqu'à quatre pour cent du chiffre d'affaires mondial annuel d'une entreprise.

Les entreprises ont jusqu'au 25 mai 2018 pour se préparer, date à laquelle toutes les dispositions du Règlement entrent en vigueur. Moins d'un an et demi, c'est donc le temps qu'ont les entreprises pour se poser les bonnes questions et mettre en œuvre la bonne de stratégie de mise en conformité. C'est un délai qui peut paraitre long mais qui, pour les entreprises, doit être utilisé afin de préparer une stratégie qui correspond à leurs besoins, leur capacité organisationnelle et leur public.

Eléments de contribution

Cette contribution vise à proposer des pistes d'analyse de questions clés soulevées par le futur cadre européen de la protection des données personnelles. Il s'agit de s'interroger sur les questions que les entreprises doivent garder à l'esprit pour la préparation à ces nouvelles obligations et restrictions.

Les éléments ci-dessous se sont pas une liste exhaustive des problématiques importantes soulevées par le Règlement et doivent être compris par chaque entreprise selon ses moyens, ses effectifs, et ses activités de traitement différemment.

- Droits des individus

Le Règlement ne crée qu'un seul nouveau droit – le droit à la portabilité des données – mais renforce de manière générale les droits des individus face aux entreprises traitant leurs données personnelles, ne serait-ce que par le montant des potentielles amendes et la mauvaise publicité que celles-ci peuvent apporter à une entreprise.

Ces droits, nombreux et tous connectés entre eux, demandent aux entreprises de s'organiser notamment au niveau humain, par exemple en mettant un place un protocole de prise en charge des questions et plaintes liées aux données personnelles, mais également au niveau technologique, pour s'assurer que les décisions liées à l'exercice de ces droits se traduisent par les actions nécessaires dans les bases de données.

- Principe d'*accountability*

C'est un des principes clés du Règlement, que la Commission Nationale de l'Informatique et des Libertés (CNIL) définie comme « l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données ».

Le Règlement vise à assouplir le système actuel de déclaration et autorisation préalables très contraignants qui s'effectue auprès de la CNIL. Il renverse la logique en demandant aux entreprises d'être les maîtres de leur propre conformité, mettant en place en système de contrôle *ex post* pour la plupart des cas de traitements de données personnelles. Apparemment plus simple et moins coûteux, ce nouveau régime demande un certain travail en interne aux entreprises, notamment de repenser leurs pratiques de gestion des données personnelles et de documenter ces pratiques.

- Obligations relatives à la transparence

Les législateurs européens ont compris que l'individu doit être tenu informé des traitements auxquelles sont soumises leurs données personnelles, et ont par conséquent décidé de renforcer les obligations de transparence. Ces obligations demandent des mises à jour aux entreprises, et permettent par la même occasion de repenser le rapport de l'entreprise à son public concernant le traitement des données.

- Responsabilités accrues du sous-traitant

La spécificité du droit européen de la protection des données personnelles a longtemps été la dichotomie entre responsable de traitement et sous-traitant dont le résultat est un régime d'obligations allégé pour ces derniers. Le Règlement conserve ces deux rôles mais accroit

considérablement les obligations imposées aux sous-traitants. Jusque-là relativement épargnés, ceux-ci vont devoir trouver les moyens de se mettre en conformité avec leurs nouvelles obligations.

- Sécurité des données

La sécurité des données et des opérations de traitement qui utilisent ces données est déjà inscrite dans les obligations de la Directive. Le Règlement voit plus loin et tape plus fort, demandent notamment aux entreprises d'informer la CNIL, et les individus concernés dans certaines situations des violations de données personnelles dans un délai de soixante-douze heures après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

COMMENT MESURER L'EFFECTIVITE DU REGLEMENT GENERAL DE LA PROTECTION DES DONNEES PERSONNELLES ?

Proposition d'Olivia Tambou, Maître de Conférences en droit public à l'Université Paris-Dauphine

Atelier Convergences du droit et numérique

Problématique proposée :

Quels outils, quelles méthodes peuvent être créées notamment entre juristes et informaticiens pour mener une recherche empirique et expérimentale afin de mesurer l'effectivité d'une norme telle que le Règlement Général de la Protection des Données (ci-après RGPD) ?

Les éléments de contexte

1. **La notion d'effectivité en droit : une notion complexe à cerner[1]**

La notion d'effectivité est un concept utilisé pour envisager la réalité des effets produits par une règle de droit. Elle est utilisée par les juristes, les sociologues, qui s'intéressent au rapport que le droit entretient avec les faits. Elle tend à interroger la capacité du droit à assumer sa fonction de direction des comportements des humains. Elle permet d'envisager comment une norme est exécutée, respectée dans les faits par les acteurs. Ainsi **François Ost et Michel van de Kerchove** considèrent qu' « est effective la règle utilisée par ses destinataires comme modèle pour orienter leur pratique» [2].

Une partie de la doctrine juridique semble envisager l'effectivité d'une norme de façon binaire : une norme serait effective parce qu'elle est respectée ou ne serait pas effective. D'autres proposent en revanche de considérer qu'une norme est plus ou moins effective. La valeur ajoutée de la notion d'effectivité est alors de permettre d'introduire cette idée de degré[3] en prenant notamment en compte les effets négatifs, pervers et positifs d'une norme. **Julien Betaille** définit d'ailleurs l'effectivité d'une norme comme « *le degré d'influence qu'exerce la norme juridique sur les faits au regard de sa propre finalité* ».[4] Il se rapproche ainsi de l'approche sociologique de la notion d'effectivité qui est conçue comme « *l'instrument conceptuel d'évaluation (du) degré de réception (de la norme), le moyen de mesurer des écarts entre pratique et droit.* » Il admet néanmoins que « *la mesure concrète de cet écart relève en grandes partie des techniques propres à la sociologie et qu'elle ne peut difficilement être appréhendée par l'analyse juridique*. »[5]

Pour illustrer cette richesse de la notion d'effectivité, **Boris Barraud** [6] distingue deux sortes d'effectivité :

- **L'effectivité matérielle** qui « *repose sur le fait empiriquement constatable du conformisme ou de l'infraction à la règle par ses destinataires…* »
- **L'effectivité symbolique** qu'il définit comme **«** *l'appréhension psychologique de la règle* »

[1] Cette notion est très proche de la notion d'efficacité qui désigne ce qui produit l'effet qu'on attend. L'efficience quant à elle permet de vérifier qu'une norme a atteint l'objectif fixé au moindre coût. Cf. Anne Lise Sibony : Du bon usage des notions d'efficacité et d'efficience en droit, in *L'efficacité de la norme juridique. Nouveau vecteur de légitimité ?* Sous la direction de Marthe Fatin-Rouge Stefanini, Laurence Gay, Ariane Vidal-Naque, Bruylant 2012

[2] François OST et Michel VAN DE KERCHOVE, De la pyramide au réseau, p. 330.

[3] En ce sens Julien Betaille, Les conditions juridiques de l'effectivité de la norme en droit public interne : illustrations en droit de l'urbanisme et en droit de l'environnement, thèse 2012 p. 25

4 Ibid p. 32.

[5] Ibid. p. 25

[6] Boris Barraud. L'échelle de juridicité : un outil pour mesurer le droit et fonder une théorie syncrétique (première partie : présentation). Archives de philosophie du droit, Dalloz, 2013, pp.365-423

Il fait de l'effectivité un des critères pour mesurer la juridicité d'une norme. La méthode de calcul qu'il propose pourrait peut-être servir de base de réflexion pour mesurer l'effectivité du RGPD :

- identifier des critères d'effectivité,
- affecter à chaque critère un indice (nullement, faiblement, moyennement, fortement, pleinement rempli par exemple)
- déterminer une méthode de calcul

2. Le RGPD

Le RGPD poursuit une double finalité :

- assurer un niveau élevé et cohérent de protection des données personnelles équivalent dans tous les Etats membres notamment par le biais de l'harmonisation
- lever les obstacles aux flux de données à caractère personnel au sein de l'Union européenne et vers des Etats tiers

La réalisation de ces objectifs passe notamment par :

- **La responsabilisation des acteurs**
    - Attribution de nouveaux droits aux individus afin qu'ils puissent contrôler l'usage de leurs données personnelles (Ex : droit à la portabilité) La concrétisation de cette approche se retrouve notamment à l'article Art.1 Loi République numérique : « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi*. »
    - Démarche préventive de régulation par les acteurs privés : Privacy by design, privacy by default, Certification, Etude d'impact, Obligation de notification etc.)
- **Le développement de mécanismes de régulation et d'interrégulation des autorités de la protection des données (DPAs)**
- **Le renforcement des outils de répressions** en cas de violation des règles consacrées par le règlement (recours devant les juges ou les DPAs, sanctions plus élevées, possibilité ouverte de forme d'action de groupe en matière de protection des données personnelles)

3. L'effectivité du RGPD mise en doute par l'analyse juridique doctrinale

- Norme peu adaptée à la technologie, aux nouveaux usages numériques (Iot, smart cities etc.)
- Norme peu adaptée aux comportements des internautes, des consommateurs qui ne sont pas vraiment des conso-acteurs.
- Importance des mesures d'application devant être prises soit par des institutions et des organes de l'UE, soit par les Etats membres, soit par les acteurs dans un délai de deux ans (règlement incomplet, pas applicable avant 2 ans)
- Des clauses ouvertes permettent aux Etats membres de faire des choix nationaux. Cela viendrait complexifier l'application transnationale de la norme pour les acteurs.
- Beaucoup d'incertitudes juridiques augurant du maintien d'une vision des acteurs de la protection des données personnelles fondée sur la gestion du risque.
- Incapacité à imposer des effets extraterritoriaux alors même que la libre circulation des données a une dimension nécessairement internationale
- Importance des obligations ne pouvant être prises en compte et acceptées par les acteurs (en raison des coûts, de l'absence de connaissance ou d'intelligibilité de la norme surtout pour des PME, les start-ups)

Pour aller au-delà de cette analyse juridique doctrinale, il conviendrait d'identifier un certain nombre d'indicateurs/critères permettant de mesurer avec plus de finesse le degré d'effectivité du RGPD.

L'objet de cette recherche interdisciplinaire sera de proposer :

- Une méthode recherche pour mesurer l'effectivité du RGPD en prenant en compte l'existence de quatre types possibles de destinataires :
    - Les Etats membres
    - Les autorités de régulation
    - Les entreprises
    - Les individus
- Elaboration d'un outil permettant de:
    - visualiser une norme de droit européen avec ses mesures européennes ou nationales d'application.
    - quantifier la variation, du contenu, de la forme des règles d'application du RGPD dans les Etats membres
    - d'évaluer l'effectivité du RGPD par l'étude de l'évolution des comportements des acteurs privés (association, ONG, entreprises) sorte de baromètre sondant de façon régulière l'effectivité matérielle et symbolique du RGPD

Le périmètre de la recherche établi devra être préalablement établi :

- Idéalement le RGPD dans son ensemble mais possibilité de se concentrer sur certaines dispositions phares
- Ampleur géographique France uniquement ou d'autres Etats membres, si oui lesquels (Allemagne, Espagne ?...)

Sources à exploiter :

- GDPR.expert, l'outil d'analyse du nouveau règlement européen, développé par le cabinet d'avocats Ulys
- Le travail de Datavizualisation du RGPD réalisée par la CNIL
- La normologie juridique autour de ELI et ECLI
- Le RGPD
- Les travaux de Boris Barraud disponibles sur Academia https://univ-amu.academia.edu/BorisBarraud

La sécurité des données à caractère personnel : de l'utopie à la réalité.
Approche juridique[1]

Sécurité – données à caractère personnel – risque

Le point de départ de cette réflexion réside ainsi dans le double constat du renouvellement profond des enjeux relatifs à la protection des données à caractère personnel dans le contexte du développement rapide des nouvelles technologies de l'information et de la communication (TIC) d'une part, et de la nécessité de renforcer en conséquence la sécurité des données pour assurer la protection du droit à la vie privée et familiale d'autre part.

L'adoption du nouveau règlement général européen sur la protection des données à caractère personnel en avril 2016[2], qui devra être mis en œuvre par les Etats en mai 2018, peut constituer un point de départ pour la réflexion sur la sécurité des données. Cette question de la sécurité est particulièrement épineuse car les données à caractère personnel doivent faire l'objet d'une protection pour assurer le droit des personnes concernée au respect de leur vie privée – d'autant plus que certaines données telles que les donnée de santé sont considérées comme des données sensibles devant faire l'objet d'une sécurité renforcée – alors même que le développement prolifique du numérique dans tous les secteurs tend à affaiblir la sécurité de ces mêmes données, à augmenter le risque d'atteinte à la vie privée. Dès lors, notre réflexion principale consiste à s'interroger sur la manière d'appréhender en droit ce risque dans un environnement numérique qui implique à la fois un échange massif de données mais aussi des échanges de données en dehors des strictes relations soumises au secret professionnel comme par exemple la relation médecin-patient.

Le nouveau règlement général européen sur la protection des données à caractère personnel consacre la section 2 de son chapitre IV intitulé « Responsable du traitement et sous-traitant » à la sécurité des données. La section se compose de trois articles dont un portant sur les mesures de sécurité et deux sur les situations de violation de données à caractère personnel entendue comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ». A partir de ces trois articles, la réflexion juridique peut être engagée selon deux axes.

1) Mesurer le risque

Le premier axe s'articule autour de la lecture du premier article de la section, l'article 32, qui préconise la mise en place par le responsable du traitement et le sous-traitant d'une

[1] Sophie Gambardella, Docteur en droit, Post-doctorante, Université Jean-Moulin, Lyon 3.
[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE L119 du 4 mai 2016.

approche par le risque. Une telle approche devrait, en théorie, les conduire à prendre des mesures techniques et opérationnelles pour assurer la sécurité des données, en l'état des connaissances.

Ces mesures peuvent notamment consister en la pseudonymisation, le chiffrement des données ou encore l'adoption de moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité des données. Or, la pseudonymisation n'est pas, selon le groupe de l'article 29, « (…) une méthode d'anonymisation. Elle réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée et constitue par conséquent une mesure de sécurité utile », ce qui signifie que les données ayant fait l'objet d'une pseudonymisation peuvent être ré-identifiées par le responsable du traitement mais parfois aussi par des tiers qui peuvent les combiner avec des informations émanant d'autres sources.

La loi de modernisation du système de santé de 2016 a, par exemple, mis en place un SNDS. Le SNDS contiendra notamment « les informations relatives aux bénéficiaires de soins et de prestations médico-sociales ». Cette catégorie de données est la plus sensible dans une perspective de protection de la vie privée des personnes concernées en contexte d'*open data*. Les données rendues accessibles ne doivent, en effet, pas être nominatives pour répondre à l'exigence de protection de la vie privée. Dès lors, le décret précise que, si cette catégorie de données inclut le sexe, le mois, l'année de naissance, le rang de naissance, le lieu de résidence, les informations médico-administratives et le cas échéant, les informations relatives au décès, elle ne doit, en revanche, pas faire mention ni du nom, ni du prénom ou encore de l'adresse du bénéficiaires de soins et de prestations médico-sociales[3]. Le caractère non nominatif de ces données est alors assuré par un pseudonyme[4]. L'article R 1461-7 1°) du code de la santé publique précise que la procédure de pseudonymisation des données de santé doit être organisée « de sorte que nul ne puisse disposer à la fois de l'identité des personnes, notamment de leur numéro d'inscription au Répertoire national des personnes physiques, d'une part, et du pseudonyme […] d'autre part ». En théorie, la sécurité des données devrait être ainsi assurée par le fait qu'elles demeurent des données non nominatives. Toutefois, comme la ré-identification des données est possible, puisque coexistent d'un côté, le code et de l'autre, le numéro d'inscription au Répertoire national d'identification des personnes physiques, ces données demeurent des données à caractère personnel. Les risques d'atteinte à la vie privée en cas notamment de piratage du SNDS sont donc réels.

De plus, même l'anonymisation des données ne certifie pas que l'identification des personnes concernées soit impossible dans la mesure où certaines données semblent intrinsèquement identifiantes. A titre d'exemple, face à une maladie très rare, le nombre de patients à l'échelle mondiale est réduit et le risque d'identification d'un d'entre eux existe malgré la mise en œuvre d'une méthode d'anonymisation des données. Les risques d'atteinte

[3] Article R. 1461-4 du code de la santé publique.
[4] Selon l'article R. 1461-4 du code de la santé publique, le pseudonyme est « constitué d'un code non signifiant obtenu par un procédé cryptographique irréversible du numéro d'inscription au Répertoire national d'identification des personnes physiques ».

à la vie privée sont donc réels dès lors qu'est mis en place l'*open data* d'autant plus qu'en matière de santé les données générées sont pour certaines des données dites sensibles notamment celles qui portent sur l'état pathologique de la personne concernée.

L'article 32 doit, par ailleurs, nécessairement être lu à la lumière de l'article 25 du Règlement qui consacre la méthodologie du *privacy by design* qui « consiste à intégrer la protection des données personnelles dès la conception des outils de collecte, de traitement et d'exploitation des données en préconisant une approche proactive du responsable de traitement afin de prévenir *ex ante* le risque d'atteinte à la vie privée, qui doit se prolonger tout au long de la vie du projet »[5]. Reste à savoir quels risques peuvent être anticipés ?

Les interrogations sont alors multiples : Le risque pour la protection des données est-il maîtrisable ? Dans quelle mesure, le responsable du traitement doit-il le réduire ? Quelles sont finalement la nature et la portée de l'obligation qui pèse sur le responsable du traitement dans ce contexte ? Obligation de résultat, de moyens ?

Ce premier axe de la recherche consiste ainsi à se demander si le risque zéro existe et si non dans quelle mesure ce risque peut-il être diminué ? Cette question est avant tout une question technique dont la réponse permettra de s'interroger alors en droit sur l'opportunité de la mise en œuvre d'un principe de précaution numérique.

2) <u>Réagir face à la réalisation du risque</u>

Le second axe de réflexion est résolument plus juridique et porte sur les deux autres articles de la section 2 qui, en cas de violation des données à caractère personnel, exige du responsable du traitement et du sous-traitant une notification à l'autorité de contrôle et une communication à la personne concernée de la violation.

Une mesure similaire a été introduite, en France, en 2011, par l'article 34 bis de la loi n° 78-17 du 6 janvier 1978. Or, la mise en œuvre de cette disposition a fait l'objet d'un arrêt du Conseil d'Etat en 2015 (Conseil d'État, 18 décembre 2015, n° 385019, ***Société Orange***) qui interroge par bien des aspects. En effet, la notification de violation des données faite à l'autorité de contrôle peut conduire le responsable du traitement et le sous-traitant à être sanctionnés pour non-respect des exigences de sécurité. Or, « [il] ressort de l'interprétation de la Cour européenne des droits de l'Homme que le droit de garder le silence et de ne pas s'auto-incriminer est une exigence du procès équitable »[6]. Toutefois, **le Conseil d'Etat considère que, dès lors que le responsable du traitement n'a pas à notifier ses éventuels**

[5] Célia ZOLYNSKI, « La Privacy by Design appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », Dalloz IP/IT, 2016, p. 404. Sur cette question du Privacy by design voir aussi : Matthieu DARRY et Leila BENAISSA, « Privacy by Design : un principe de protection séduisant mais complexe à mettre en œuvre », Dalloz IP/IT, 2016, p. 476.

[6] Nathalie METALLINOS, « Notification des violations de données à la CNIL : tendre le bâton pour se faire battre ? Observations sous Conseil d'État, 18 décembre 2015, n° 385019, Société Orange », Dalloz IP/IT, 2016, p. 144.

manquements à la sécurité, son droit de ne pas s'auto-incriminer est préservé. Il reste que le responsable du traitement et le sous-traitant doivent notifier la violation et donc déclenchent par ce biais une enquête sur un éventuel manquement à leur obligation de sécurité. L'article 33 du règlement européen met ainsi en tension deux droits : d'un côté, le droit au procès équitable du responsable du traitement et d'un autre côté, le droit au respect de la vie privée de la personne concernée.

Au delà de cette question très juridique, d'autres réflexions sont impulsées par ces dispositions. En premier lieu, techniquement un responsable de traitement a-t-il nécessairement connaissance de l'ensemble des atteintes au droit à la vie privée lorsqu'il est, par exemple, l'objet d'un piratage. En somme, est-il toujours en mesure de remplir son obligation d'information ? En second lieu, à partir de quel moment un manquement à son obligation de sécurisation des données est-il constitué ? Cette question est étroitement liée à la question de la nature de l'obligation qui incombe au responsable du traitement et à la notion de « mesures appropriées », qu'est finalement une mesure appropriée en contexte d'incertitude technique ? Toute la nébuleuse qui entoure la question de la sécurité des données ne porterait-elle pas finalement atteinte à la sécurité juridique même ?

Ma réflexion sur la sécurité des données est aujourd'hui à l'état embryonnaire et soulève plus de questions que ce qu'elle apporte de réponses. Toutefois, il me semble nécessaire sur cette question de travailler de manière pluridisciplinaire pour que la réflexion juridique soit en adéquation avec des situations de faits non pas hypothétiques mais bien réelles.

Anonymization et droit à la “privacy“ dans le context de l’ Internet des Objets (IdO)

L’Internet des Objets (IdO) represents un nouveau paradigm de réseau de réseaux d’objets, où il y la communication sans interaction humaine. Les objets sont devenus de plus en plus intelligents et sont desormais capables de collecter beaucoup de données et notamment il peuvent prendre des décisions soit en local soit collectivement.

Avec l’advent aussi des technologies qui se basent sur les nuages (cloud computing), il y a la possibilité d’externaliser les données. Dans un cloud et de tojours nouveaux services sont mis à disposition qui prevoient la possibilité dde prendre des decisions dans un cloud.

Evidemment, dans ce type de context il y a une difficulté de traiter la “protection des données personnelles“ qui a origine aussi de la diversité des technologies et des composants qui caracterisent l’IdO.
Il ya pas mal d’applications qui peuvent être envisagés : montres intelligents pour mesurer les activités pendant la journée, applications domotiques où les objets de la maisons sont connectés et [euvent communiquer entre eux, les voitures connectés qui peuvent faire communiquer les objets à l’interieur de la voiture ou les voitures entre eux, applications dns le domain de la santé, etc.
Déjà en terms de composants on peut trouver des RFID, puces, smartphones, robots, capteurs, etc. Notamment, ces composants sont caracterisées par des differences en termes de portée de communications. Les capacities associées sontaussi très hétérogenes, avec une chute directe sur le montant de donnés produits.

Dans les systems de communications traditionnelles normalement le perimeter est défini avec precision, les elements à proteger aussi. Dans le context de l’IdO le montant de donnés produit, les approaches cross-layer, les different domaines d’applications, les elements très heterogene rendent tout completement plus compliqué alors que une precise comprehension des perimetres pour assures le droit à la privacy et à l’anonymization doit être bien concerté.

Géolocalisation et IA

Les données personnelles sont protégées par la Loi du 6 janvier 1978 Informatique et libertés ainsi que par le Règlement n° 2016/679 eu 27 avril 2016 applicable à partir du 25 mai 2018. Parmi les données de caractère personnel, certaines données peuvent apparaître aujourd'hui plus importantes que d'autres. Tel est le cas des données de géolocalisation – aujourd'hui fondamentales sur Mobile – qui améliorent la précision du ciblage publicitaire et qui sont un facteur d'irrigation du commerce de proximité, du tourisme ou des transports[1]. Les spécialistes de marketing relationnel et connaissance client peuvent cibler les porteurs de leur application de bons de réduction C-Wallet, qui sont ensuite invités à activer sur leur mobile les fonctionnalités nécessaires à la réception des promotions ciblées pendant leur parcours d'achat. Cela suppose que les consommateurs potentiels aient accepté d'être géolocalisés de façon à être captés à proximité des magasins où ils peuvent profiter des promotions.

L'amalgame de données peut être source de services. C'est encore l'exemple de Facebook dont les notifications peuvent être adaptées à la localisation géographique de l'internaute de façon à lui présenter des évènements locaux, des informations populaires de la ville où il se trouve, un point météo ou des informations sur les films qui passent à proximité ou des restaurants… ceci en fonction des pages likées et de sa géolocalisation.

Sur ce terrain, Google est une fois encore en très nette position de force grâce à Google Maps et au rachat de l'application de trafic Waze, ce qui lui permet d'augmenter ses recettes Adwords au niveau local.

[1] CNN, Groupe Neutralité des plateformes, compte rendu des réunions des 4 et 22 octobre, 15 novembre 2013, p. 7.

La géolocalisation peut avoir un intérêt en dehors du marketing. Ainsi peut-elle être utile dans la vie quotidienne pour vérifier la position des enfants, rassurer les amis et la famille[2], ou bien encore dans la prévention, la recherche ou le contrôle de délinquants.

Une réflexion conjointe entre informaticiens et juristes pourrait être menée sur les potentialités de la géolocalisation : quels sont les outils permettant la géolocalisation et comment l'individu peut-il les contrôler ? Par ailleurs, le traitement de ces données par des procédés d'Intelligence artificielle, à des fins commerciales, de ciblage, de statistiques touristiques par exemple, commande de s'interroger sur la liberté de choix des individus, des consommateurs et les nouvelles formes de consentement. **Le guider finalement vers tel produit ou commerçant en raison de son habitude de trafic (ou encore en raison de données collectées par un objet connecté[3]) ne peut-il pas, d'une part, être éthiquement contestable, et d'autre part, poser des problématiques juridiques en droit de la consommation et droit de la concurrence ?**

[2] La géolocalisation sociale ou communautaire se développe aussi avec Safety Check de Facebook ou Google contacts dont les applis permettent à l'internaute de se géolocaliser pour ses contacts préalablement autorisés lorsqu'ils le demandent.

[3] Un pèse personne connecté qui l'alerterait sur son poids et lui recommanderait, voir achèterait via un assistant personnel, des produits light…

Thématique :
Télémédecine et sécurité des données de santé

Communauté d'appartenance :
Droit

Définition
L'utilisation des technologies de l'information et de la communication (TIC) dans le domaine de la santé a permis l'émergence d'une forme innovante de pratique médicale : la télémédecine. Juridiquement définie à l'article L. 6316-1 du Code de la santé publique (CSP), la télémédecine s'entend non seulement comme une pratique médicale à distance mais aussi comme un procédé technique qui permet l'échange d'informations médicales. Ces dernières, autrement qualifiées de données de santé, sont soumises à un régime juridique très protecteur. En effet, les dispositions de la loi du 6 janvier 1978 modifiée dite loi « Informatique et Libertés » autorisent, par exception, les traitements de données de santé.

Contexte
La loi du 26 janvier 2016 de modernisation de notre système de santé et la loi du 7 octobre 2016 pour une République numérique se sont attachées à simplifier la circulation, le partage et l'accès aux données de santé. De nombreuses mesures peuvent être citées :

- Le nouvel article L. 1110-4-III du CSP qui règlemente le partage d'informations médicales entre professionnels de santé appartenant à la même équipe de soins. Cette notion fait à présent l'objet d'une définition légale au sein du nouvel article L. 1110-12 du CSP ;
- La création du dossier médical partagé par le décret n° 2016-914 du 4 juillet 2016 ;
- L'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) à des fins de statistique publique et de recherche scientifique ou historique.

Problématique
L'échange d'informations médicales n'est plus unique et statique. En effet, les données de santé peuvent être partagées, à distance, entre des professionnels de santé appartenant ou non à la même équipe de soins. Au surplus, certains dispositifs, notamment ceux de télésurveillance médicale, permettent au patient d'enregistrer et de transmettre lui-même ses données de santé à son médecin. En réalité, la télémédecine met en jeu une nouvelle circulation des données de santé qui soulève une interrogation : comment faciliter le partage et l'échange des données de santé, promus par le législateur, tout en assurant la sécurité de ces données ?

Objectifs de la contribution
L'expertise d'un ingénieur informatique serait nécessaire sous plusieurs angles :

- Expliciter les procédés de cryptage et de chiffrement de ce type de données ;
- Apporter un éclairage pratique sur les référentiels d'interopérabilité et de sécurité prévus par le nouvel article L. 1110-4-1 du CSP ;
- Avoir une expertise sur les risques liés aux objets connectés collectant des données dont la qualification juridique est indéterminée (donnée de santé ou donnée bien être).

Internet des objets et captation de la voix : Quelle protection pour une donnée pas comme les autres ?

Charly LACOUR, Doctorant contractuel
Université de La Rochelle

Selon Charlie Kindel, le directeur Smart Home d'Amazon, « Chez Amazon, nous pensons que nous sommes à l'orée du prochain bouleversement majeur de l'informatique. Nous pensons que ce bouleversement se fera autour de la voix ».[1] Charlie Kindel, lors de cette Keynote de 2016, faisait référence à Alexa, le nouvel « assistant virtuel » d'Amazon devant être implémenté dans leur enceinte connectée Amazon Echo Dot et commandé par la voix, dont la première version s'est d'ores et déjà écoulée à plus de trois millions d'exemplaires dans le monde.

Cette annonce fait suite aux nombreux développements qu'a connu l'Internet des Objets depuis le début des années 2010, et n'est pas sans soulever de nombreuses questions tant techniques que juridiques. Ainsi, en 2013, DoctorBeet[2], concepteur de logiciels, remarque que sa télévision connectée LG collecte un grand nombre de données personnelles le concernant, depuis les émissions qu'il regarde au contenu de ses périphériques usb connectés au téléviseur. Contrairement au principe de prévention posé par le nouveau règlement européen 2016/679 du 27 avril 2016 (RGPD), qui ne sera applicable qu'a partir du 25 mai 2018 , la collecte de données est activée par défaut. Ce système de l'opt-in / opt-out, sensé protéger l'utilisateur de la collecte abusive de ses données personnelles et prouver son consentement (ou l'absence de consentement) a ce traitement , n'est cependant ici qu'un « leurre », le choix de l'opt-out par l'utilisateur n'empêchant en rien la collecte des mêmes données par LG. Si la marque a fait amende honorable par la suite, le problème se pose toujours avec acuité avec les nouvelles générations de télévisions connectées, qui incluent un système de commandes vocales. Une étude menée par des journalistes indépendants fin 2016[3],a pu démontrer que le coréen Samsung collectait les données vocales des utilisateurs de ses « smart-tv », que ceux-ci aient activé ou non le système de reconnaissance vocale[4], afin de les faire parvenir à un tiers pour les exploiter, et qu'une bonne partie de ces données transitaient de manière non sécurisée sur Internet.

Les intérêts de ces évolutions technologiques sont multiples : commandes à distance, centralisation

1 « At Amazon, we think we're on the cusp of the next major disruption in computing. We think that disruption is around voice ».
2 *To be or not to be connected* : ces objets connectés qui nous espionnent – Laure Marino – D. 2014. 2

3 CanardPc Hardware, juillet-août 2016, p.56

4 « Si vos propos contiennent des informations sensibles, personnelles ou autres, ces informations seront parmit les données saisies et transmises à un tiers par l'utilisation de la reconnaissance vocale », Samsung, politique de confidentialité

des décisions (pilotage de tous les objets connectés à partir d'un unique appareil), maîtrise de la consommation énergétique des appareils au domicile et à distance, mesures de santé...(appareils de quantified self). D'un point de vue juridique, jusqu'à l'apparition des commandes vocales, le consentement ou non à la collecte de données personnelles par le biais de ces produits ou services pouvait s'effectuer de manière active, par le biais notamment, et déjà évoqué, du système d'opt-in/opt-out. Avec les commandes vocales, en revanche, il est beaucoup plus difficile de caractériser le consentement de l'utilisateur, la captation pouvant se faire de manière continue. Que ce soit Google home, Jarvis de facebook ou Alexa d' Amazon, **le développement des assistant de vie intelligents basés sur la voix peut engendrer une captation ininterrompue de données , émises de manière passive par l'utilisateur, sans qu'il soit possible de déterminer s'il consent totalement, partiellement, ou non, à leur collecte et à leur traitement.** Or, le principe du consentement et de la prévention des atteintes à la vie privée est au cœur de la nouvelle réglementation européenne et de la législation française sur la collecte et le traitement des données personnelles.

L'essor de ces nouveaux moyens de communication entre individus et objets, la rapidité à laquelle il s'effectue, nécessite une approche pluridisciplinaire du phénomène. D'un point de vue technique, il s'agit d'assurer la sécurité dans la transmission et le stockage des données collectées, afin d'éviter toute interception des flux, ou détournement des objets comme cela a été le cas en 2016 pour la société OVH[5], ou, comme l'ont révélé les documents Wikileaks mis en ligne le 07 mars 2017, pour éviter un espionnage de masse par des Etats. Il s'agit aussi d'encadrer techniquement les informations pouvant être collectées lors de l'utilisation de commandes vocales, en accord avec les réglementations nationales, régionales et internationales. Pour ce faire, le statut de la voix dans ce contexte juridique doit être au préalable repensé : doit -elle être soumise au statut des données sensibles, en ce que de la collecte passive de données audio peut découler la collecte de données relatives aux convictions politiques, religieuses,... ? Doit-elle plutôt bénéficier du statut des données de santé , telles que définis par le RGPD ? Comment caractériser l'étendue du consentement de l'utilisateur quant au recueil, au stockage et au traitement des données audio ?

Les chiffres parlent d'eux mêmes : à l'horizon 2018, chaque foyer pourrait disposer en moyenne de 30 appareils connectés[6]. Le Droit comme la technologie doivent permettre d'instaurer la confiance en des objets qui pourraient bien devenir indispensables à la société de demain.

5 http://www.lemonde.fr/pixels/article/2016/09/26/derriere-une-serie-d-attaques-informatiques-tres-puissantes-un-reseau-d-objets-connectes-pirates_5003470_4408996.html

6 http://www.lemonde.fr/festival/video/2015/10/06/le-monde-festival-2015-objets-connecte-s-enfer-ou-paradis_4783629_4415198.html

Traitement automatique de la parole :
Quelle écoute pour nos systèmes ?

La parole est communément définie comme la faculté de communiquer oralement propre aux hommes. Intrinsèquement liée au langage, elle est une réalisation manifeste de ce dernier. Notre voix, quant à elle, assure mécaniquement la production de la parole par la vibration des cordes vocales, grâce à la pression de l'air expiré des poumons et aux résonateurs constitués par les cavités buccales et nasales. D'un point de vue conceptuel, parole et voix peuvent être appréhendées comme les deux constituants d'un signe linguistique selon la définition donnée par Ferdinand de Saussure[1], la parole composant le signifié et la voix, le signifiant. En pratique, nous sommes quotidiennement confrontés à l'analyse multiniveaux des signaux de parole. En plus de comprendre le « sens » du message qui nous est transmis, cette analyse nous révèle de nombreuses autres informations sur notre interlocuteur : âge, sexe, origines géographiques et socioculturelles, physionomie, état de santé, émotions, *etc.* Notre voix, véhicule privilégié de nos interactions sociales, révèle donc énormément sur nous.

Ayant connu une très forte expansion dans les années 1960 suite à la publication de la théorie de l'information de Claude Shannon, le traitement de la parole (*speech processing*) est aujourd'hui une composante fondamentale des sciences de l'ingénieur. Situé au croisement de la physique (acoustique, propagation des ondes), des mathématiques appliquées (modélisation, statistique), de l'informatique (algorithmique, techniques d'apprentissage) et des sciences de l'homme (perception, raisonnement), le traitement de la parole a rapidement été décliné en de nombreux domaines d'étude : reconnaissance et vérification du locuteur, transcription automatique de la parole, synthèse vocale, détection des émotions, *etc.* Depuis une quinzaine d'années, la discipline dans son ensemble a progressé de manière remarquable et de grandes avancées ont été enregistrées. Les grands acteurs du numérique ne s'y trompent d'ailleurs pas. Pour eux, l'avenir de nos interactions avec les systèmes passe par l'analyse des signaux de parole. Nous avons coutume de dire que « les paroles s'envolent, les écrits restent ». Toutefois, les changements profonds induits par le numérique pourraient rendre caduc le proverbe. Avec l'explosion annoncée de l'Internet des Objets, nous serons de plus en plus encouragés à interagir de façon « naturelle » avec nos systèmes. Téléviseurs, agents conversationnels ou encore systèmes d'authentification seront littéralement « à notre écoute ». Toutefois quelle sera la qualité de celle-ci ? Nos nouveaux compagnons de vie auront-ils la décence de parfois entendre sans écouter ? Sauront-ils conserver les secrets que nous leur confierons ?

L'actualité met quotidiennement en exergue ces questionnements. Très récemment, la police de l'Arkansas a ainsi émis un mandat demandant à Amazon de lui fournir les données enregistrées par son dispositif Echo

[1] [Saussure] "Cours de linguistique générale", Paris, 1916.

afin de l'aider dans la résolution d'un meurtre ayant eu lieu en novembre 2015[2]. En effet, les enquêteurs ont découvert que le produit d'Amazon était allumé et diffusait de la musique non loin de la scène du crime. Convaincue du fait que le dispositif enregistre les sons de son environnement en permanence, la police de l'Arkansas a donc demandé d'accéder aux précieuses données. Ce fonctionnement est fermement démenti par la multinationale qui précise que des enregistrements ne sont réalisés, transférés et analysés que si un mot déclencheur est prononcé (par défaut « Alexa », nom de l'assistant virtuel). Quelle que soit l'issue de cette opposition, elle illustre parfaitement la sensibilité des signaux de parole. En effet, quelle confiance accorder à des systèmes qui pourraient, si mal implémentés, écouter en permanence nos conversations ou identifier les personnes présentes dans notre foyer ?

L'exemple précédent soulève une autre question : celle de l'utilisation des signaux de parole dans le cadre juridique. Dans une récente publication scientifique[3], des chercheurs d'INTERPOL ont présenté les résultats d'une enquête réalisée sur l'utilisation de la reconnaissance du locuteur par les forces de l'ordre à travers le monde. L'article met clairement en avant l'extrême prudence qui doit entourer le recours à ces méthodes. En France, depuis 1997, la Société française d'acoustique (SFA) appelle publiquement à ne pas recourir à l'expertise en matière de reconnaissance du locuteur dans le domaine judiciaire. Il s'agit là de se prémunir des promesses de ce que le philosophe Evgeny Morozov appelle le solutionnisme technologique[4] et d'indiquer clairement que si le domaine du traitement de la parole connait d'indéniables avancées, en l'état actuel des connaissances en matière d'identification vocale, il n'existe aucune méthode scientifique qui permette d'identifier une personne avec certitude.

La voix est considérée par le Droit comme une image sonore de la personne et doit à ce titre être protégée comme les autres attributs de la personne humaine. Cette vision est consacrée par l'article 9 du Code Civil. De plus, au regard de la loi Informatique et Libertés, notre voix peut tour à tour être considérée comme une donnée biométrique, une donnée de santé (car révélatrice de pathologies), une donnée sensible (car faisant apparaître des opinions politiques, philosophiques ou religieuses), *etc.* A la lueur des précédentes réflexions et des transformations induites par le numérique, il semble donc indispensable de repenser le statut juridique de la voix et des données de parole. De plus, d'un point de vue technique, les questions de loyauté des systèmes et d'appréciation de leurs capacités doivent également être posées au risque de constater une crise de confiance des utilisateurs de ces technologies.

Félicien Vallet, Ingénieur au Service de l'expertise technologique de la CNIL

---

[2] [Journal Le Monde] "Dans l'Arkansas, la police veut entendre « Alexa », l'assistant à commande vocale d'Amazon", 30 décembre 2016.
[3] [Morrisson *et al.*] "INTERPOL survey of the use of speaker identification by law enforcement agencies", Forensic Science International, Volume 263, Juin 2016.
[4] [Morozov] "Pour tout résoudre, cliquez ici ! L'aberration du solutionnisme technologique", FYP Editions, 2014.

« Convergences du Droit et du numérique »

Christine Lassalas, Maître de conférences de droit privé, Centre Michel de l'Hospital (EA4232), Université Clermont Auvergne

« Big data » et biens communs…

Les particuliers doivent effectuer des choix qui concernent des biens, des choses ; il s'agit alors le plus souvent pour la personne, de savoir si elle veut les conserver, les donner ou les vendre. Mais encore faut-il avoir le droit de décider de garder, de donner ou de céder, ce qui conduit généralement à envisager la question de l'appropriation. Il est en effet relativement facile de concevoir une prise de décision concernant un bien qui nous appartient, mais beaucoup plus délicat de l'envisager si l'appropriation est remise en question. Or la question de l'appropriation est particulièrement complexe pour les biens immatériels. Par ailleurs, tout peut-il être objet de propriété, les données personnelles par exemple. La question de l'existence d'un droit de propriété sur ses propres données personnelles peut être débattue, mais je souhaiterais m'interroger sur la masse de données collectées à grande échelle, sur leur caractère accessible (accès ouvert, libre, gratuit..).

Dans le cadre de l'atelier de travail, je souhaiterais étudier les données personnelles non pas d'un individu, mais dans leur ensemble. Je voudrais m'intéresser au croisement de ces données, voir si elles peuvent être analysées comme un bien commun et envisager quelles conséquences aurait cette qualification sur le plan juridique, mais aussi pratique. Il convient en effet de se demander si le « réseau des données » ne peut pas constituer un objet de droit, si le volume des données personnelles (ou les données appréhendées sous leur dimension collective) ne peut pas constituer un bien commun tel que l'air ou l'Antarctique.

Si l'on s'en tient au secteur de la santé, de nombreuses données sont générées chaque jour par chacun d'entre nous : à chaque fois que nous allons chez le médecin, à la pharmacie, que nous faisons des analyses de sang, que nous utilisons des capteurs, bracelets ou montres connectés, des tensiomètres, podomètres… On peut également ajouter à cela les données fournies sur les réseaux sociaux. Cette énorme quantité d'informations disponibles une fois exploitée, peuvent servir à de multiples fins : déterminer des profils de consommation, constituer des bases de données comportementales, faire des prévisions.

L'un des enjeux principaux hormis la protection de la vie privée, tient du fait que les données personnelles collectées ont une valeur marchande. Elles ont une importance économique considérable. Mais, on peut se demander dans quelle mesure la masse des données personnelles ne peut pas être regardée comme un bien commun. Cette idée est facilement concevable dans le domaine de la santé. Le traitement croisé des données permet en effet d'envisager « des machines » qui établiront rapidement des diagnostics très précis, de créer des applications permettant de déterminer la survenue de rechutes en cancérologie ou de prévoir une maladie « à venir » en raison d'un comportement « à risque »… Il convient donc de garantir une utilisation optimale de ces données pour la société, car cette masse de données est utile à la communauté des êtres humains. Dès lors, pourquoi ne pas envisager de la traiter comme un bien commun ?

Consciente de l'importance des données et de l'attrait pour ces données, il faut s'interroger sur « le droit des entreprises ou de l'Etat » sur ces données, dans la mesure notamment où ils peuvent être tentés d'en disposer et de les vendre… On peut également se demander quel est le souhait des particuliers, les « producteurs » de données, qui peuvent vouloir un partage de leurs données mais à certaines conditions…

Une fois la qualification effectuée, si l'on considère qu'il s'agit d'un bien commun, il conviendra alors d'envisager son régime. On peut imaginer une forme « d'indivision » entre toutes les personnes dont les données sont liées. S'agissant d'un bien commun, actuellement en France, le statut est défini par l'article 714 du code civil ; il s'agit d'un bien qui appartient à tous. Mais chacun pourrait toutefois disposer de droits spécifiques (retrait, oubli…). Il faudrait également déterminer quelle instance serait compétente pour assurer la gestion de ce bien commun. Une Agence, l'Etat ?

Ma contribution à l'atelier est encore assez imprécise. J'ai quelques certitudes. Concernant la problématique, je souhaiterais déterminer dans quelle mesure la masse des données personnelles peut constituer un bien commun et envisager quelles seraient alors les conséquences.

Etant juriste, je souhaiterais pouvoir participer aux ateliers afin d'échanger et d'avoir d'autres regards sur le traitement de masse des données personnels et savoir ce que les informaticiens et les autres acteurs (les médecins et tous les soignants notamment) espèrent et attendent du Droit concernant le Big data et l'open data principalement.

Mes travaux de recherche ont un point commun : ils concernent l'étude des concepts et mécanismes fondamentaux du droit privé que sont la propriété, les personnes, les choses et les biens. J'ai ainsi consacré ma thèse à la notion de propriété scripturale, mais actuellement, j'étudie ces concepts en me situant principalement dans les secteurs de la santé et dans la sphère de la vie privée. Ainsi, certaines de mes recherches portent sur l'appropriation des éléments du corps humains ou des cellules souches. L'immatériel et les biens ne me sont donc pas inconnus, même si le domaine du numérique m'est moins familier.

Comité de pilotage

- Anne CADIOT-FEIDT, Avocate au barreau de Bordeaux, ancienne Bâtonnière de Bordeaux
- Clothilde CAZAMAJOUR, Avocate à la Cour, barreau de Bordeaux
- Jean-François DESRAMÉ, Président du Tribunal administratif de Bordeaux
- Olivier DUBOS, Professeur de droit public, chaire Jean Monnet, Coordonnateur du Forum Montesquieu, université de Bordeaux
- Anne GUÉRIN, Présidente de la Cour administrative d'appel de Bordeaux
- Vivianne LE HAY, Enseignante-chercheur en sociologie au Centre Emile Durkheim, IEP Bordeaux
- Fabrice HOURQUEBIE, Professeur de droit public, directeur de l'Ecole Doctorale de droit, université de Bordeaux
- Valérie MALABAT, Professeur de droit privé et de sciences criminelles, Directrice de l'Institut de sciences criminelles et de la justice, université de Bordeaux
- Isabelle MONTEILS, Sous-directrice, chef du département recherche et documentation, Ecole nationale de la magistrature
- François PELLEGRINI, Professeur d'informatique, Vice-président en charge du numérique, université de Bordeaux
- Benjamin PELLETIER, Directeur exécutif du Forum Montesquieu
- Olivier PUJOLAR, Maitre de conférences en droit privé, Vice-président en charge des partenariats, université de Bordeaux
- Jean-Christophe SAINT PAU, Professeur de droit privé et de sciences criminelles, Doyen de la faculté de droit et de science politique, université de Bordeaux
- Laura SAUTONIE-LAGUIONIE, Professeur de droit privé, Vice-doyen de la Faculté de droit et science politique en charge de la professionnalisation, université de Bordeaux
- Manuel TUNON de LARA, Président de l'université de Bordeaux

Comité scientifique

- Linda ARCELIN, Professeur de droit privé, université de La Rochelle
- Thierry DAUPS, Maître de conférences de droit public, Université Rennes 2
- Gilles GUGLIELMI, Professeur de droit public, université Paris 2 Panthéon–Assas
- Benjamin JEAN, Fondateur du cabinet Inno³
- Bernard LAMON, Avocat au barreau de Rennes
- Daniel LE METAYER, Directeur de recherche, Inria
- Valérie MALABAT, Professeur de droit privé et de sciences criminelles, directrice de l'Institut de sciences criminelles et de la justice, université de Bordeaux
- Nathalie MITTON, Chercheur, Inria
- Nathalie NEVEJANS, Maître de conférences en droit privé, HDR, Université d'Artois
- François PELLEGRINI, Professeur d'informatique, Vice-président en charge du numérique, université de Bordeaux
- Bertrand RIOU, Vice-président au Tribunal administratif de Bordeaux
- Thierry WICKERS, Avocat au barreau de Bordeaux, ancien bâtonnier de Bordeaux