Rencontres JEUNES CHERCHEURS

DROIT & NUMÉRIQUE

3ème édition

Lex Electronica
Volume 25 - 2

Vulnérabilité(s) : l'appréhension des défis du numérique par le droit

Actes de colloque dirigés par
Ledy Rivas Zannou & Eve Gaumond

Notice de remerciements

L'aventure de la troisième édition des Rencontres Jeunes Chercheurs Droit & Numérique n'aurait pu être possible sans le soutien de plusieurs intervenant(e)s que nous tenons à remercier sincèrement.

D'abord, nous souhaitons exprimer notre gratitude aux Professeurs **Olivier Delas** et **Vincent Gautrais** qui soutiennent le projet Jeunes Chercheurs Droit & Numérique depuis sa création et qui ont été à la fois d'une grande aide et d'une grande générosité dans l'organisation de cette année. Un merci spécial également au Professeur **Pierre Trudel** qui a accepté et agi à titre de parrain de l'évènement cette année.

Ensuite, nous souhaitons également remercier la Chaire Jean Monnet en intégration européenne de l'Université Laval, la Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique de l'Université de Montréal, la Chaire UNESCO sur la diversité des expressions culturelles de l'Université Laval, le Centre de recherche en droit prospectif (CRDP) et l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) pour le support institutionnel.

Nous adressons nos remerciements à toutes les personnes qui se sont impliquées dans l'organisation de cette troisième édition des Rencontres Jeunes Chercheurs Droit & Numérique. Nous pensons spécialement pour le comité d'organisation à Mrs. Guillaume Macaux, et Simon Du Perron ainsi qu'à Mme Clémence Varin. Notre gratitude va à l'endroit des Professeur(e)s **Pierre-Luc Déziel** et **Véronique Guévremont** sans oublier les Professeur(e)s **Céline Castets-Renard** et **Alexandra Bensamoun** qui, avec **Olivier Delas**, **Vincent Gautrais**, **Pierre-Luc Déziel** et **Guillaume Macaux** ont assuré la présidence des panels.

Enfin, ne pouvant pas les citer, nous adressons au comité d'évaluation scientifique des contributions notre grande reconnaissance.

Ledy Rivas Zannou et Eve Gaumond

SOMMAIRE

Présentation du collectif « Vulnérabilité(s) : L'appréhension des défis du numérique par le droit » **5**

Ledy Rivas ZANNOU et Eve GAUMOND

Co-regulation or Capitulation ? Addressing conflicts arising by AI and standardization **11**

Johannes BRAKE

Quelles Œillères imposer à l'État ? Le regard du droit québécois sur la technologie à reconnaissance faciale utilisée par les forces de l'ordre au Royaume-Uni **24**

Samy CHEKIR

La vie privée des groupes : nouveau cadre théorique pour une protection contre le profilage algorithmique **36**

Simon DU PERRON

Les vulnérabilités inhérentes à l'approche individualiste des données de santé dans l' « ère big data » **48**

Fabien LECHEVALIER

Les données personnelles à l'épreuve de l'*open data* des décisions de justice : entre principe de transparence de la justice et droit à la vie privée..... **60**

Flora DORNEL

Appréhender les inégalités d'accès à la justice par les médias sociaux : une perspective empirique sur l'information juridique **72**

Alexandra BAHARY-DIONNE

Vulnérabilités + contrat électronique : l'exemple du consentement électronique **87**

Ledy Rivas ZANNOU

La vulnérabilité des engagements pris par les États pour protéger et promouvoir la diversité des expressions culturelles dans l'environnement numérique : quelle(s) stratégie(s) pour les Parties à la Convention de 2005 ? **99**

Clémence VARIN

PRÉSENTATION DU COLLECTIF « VULNÉRABILITÉ(S) - L'APPRÉHENSION DES DÉFIS DU NUMÉRIQUE PAR LE DROIT »

Ledy Rivas ZANNOU[1] **et Eve GAUMOND**[2]

1 L'auteur est candidat au doctorat en droit des technologies nouvelles à la Faculté de droit de l'Université de Montréal. Il assume actuellement, les fonctions de Coordonnateur de la Chaire L.R. Wilson en droit des technologies de l'information et du commerce électronique.

2 L'auteure est candidate à la Maîtrise en droit à la Faculté de droit de l'Université Laval. Elle est auxiliaire de recherche à la Faculté de droit de l'Université Laval et chargée de projet au sein de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique.

[1] L'aventure continue… Les Rencontres Jeunes Chercheurs Droit & Numérique sont nées de l'initiative de Guillaume MACAUX et Christelle PAPINEAU alors respectivement candidats au doctorat en droit à l'Université Laval et à l'Université de Montréal. L'ambition était de permettre aux étudiant·e·s gradués.es œuvrant dans le domaine du droit du numérique de présenter les résultats de leurs recherches, de rencontrer leurs pairs et d'échanger entre eux. Trois ans plus tard, ces rencontres contribuent toujours au développement d'une communauté dynamique de jeunes chercheurs en droit du numérique.

[2] Une troisième édition toute spéciale. La crise de la Covid-19 est indissociable de l'histoire de cette troisième édition. D'abord, elle nous aura forcé à abandonner l'idée de tenir l'événement en « présentiel » au mois d'avril et à plutôt accepter le fait que les *Rencontres* auraient lieu en ligne, au mois de septembre. Bien que sceptiques quant aux vertus des conférences en ligne, nous avons pris le pari de détourner le regard de ce que l'on perdrait à ne se rencontrer qu'à distance. Contre mauvaise fortune bon coeur, nous avons choisi d'essayer de tirer parti des bénéfices de cette réorientation.

[3] Quelques pierres supplémentaires à l'édifice. C'est ainsi que la crise - paralysant tout - nous a donné l'impulsion pour produire ce collectif. Si nous ne pouvions pas - à proprement parler - nous rencontrer, nous donnerions à tout le moins l'opportunité aux idées de se côtoyer en les couchant sur papier. Pour cette troisième édition, les *Rencontres* investissent donc un nouveau medium : en plus de la conférence annuelle, nous publions les présents actes de colloque intitulés *Vulnérabilité(s) : L'appréhension des défis du numérique par le droit* dans un numéro spécial de la revue *Lex Electronica*. Les conférenciers qui le désiraient ont été invités à produire un texte sur les vulnérabilités en contexte numérique qu'ils devaient aborder sous le prisme de leur champ d'expertise respectif.

[4] Pourquoi traiter des vulnérabilités en droit numérique ? L'idée de nous intéresser aux vulnérabilités a été évoquée pour la première fois en mai 2019 à la clôture de la deuxième édition des *Rencontres*. À ce moment, nulle pandémie à l'horizon. À vrai dire, du concept de pandémie, nous n'avions qu'une idée vague, et en ce qui a trait au mot, nous ne l'avions probablement même jamais véritablement prononcé. Il n'y a pas à dire, c'était le temps d'avant. Aujourd'hui le terme est usé, ressassé, éculé, si

bien que nous aurions vraiment préféré ne pas en traiter dans le cadre de cet avant-propos. Or c'eût été taire la présence d'un éléphant dans la pièce. Si la crise a façonné le processus d'écriture de ces articles, on ne peut nier qu'elle teintera aussi la manière dont on en fait la lecture. En effet, la pandémie a magnifié les vulnérabilités en contexte numérique de telle manière qu'il n'est plus possible de les ignorer.

[5] Huit regards sur les vulnérabilités en droit numérique. Point n'est besoin de rappeler que les vulnérabilités qui prévalent dans l'environnement numérique sont nombreuses. Dans ce collectif, les auteurs proposent de traiter de certaines de ces vulnérabilités suivant des approches disciplinaires originales et parfois audacieuses. Ainsi, les huit textes qui composent ce collectif abordent la notion de vulnérabilité(s) en explorant à la fois les raisons internes et externes au droit du numérique. Cette analyse est suivie dans la plupart des cas de proposition de solutions singulières que nous présenterons à travers les lignes qui suivent.

[6] Co-Regulation or Capitulation – Addressing conflicts arising by AI and standardization. Dans son article Johannes BRAKE s'intéresse à la corégulation de l'intelligence artificielle (IA). Pouvant prendre différentes formes, ce type d'encadrement consiste généralement à allier des principes éthiques plus généraux, des normes légales exécutoires ainsi que des standards techniques concrets (ex : normes ISO). Cette action concertée de différents types de normativités permet de tirer parti des avantages des divers types de normes pour mitiger les risques que soulèvent les systèmes d'IA, tout en assurant une souplesse et un dynamisme suffisant pour encourager l'innovation. L'auteur, en invitant à plus d'« *innovation in the regulator's tool box* », prépare le terrain pour les autres contributions qui traitent de situations de vulnérabilités numériques plus ciblées.

[7] Quelles œillères imposer à l'État ? Le regard du droit québécois sur la technologie à reconnaissance faciale utilisée par les forces de l'ordre au Royaume-Uni. À travers cette contribution, Samy CHEKIR s'intéresse au droit applicable à l'utilisation de caméras munies d'algorithmes de reconnaissance faciale par les forces policières. L'auteur mène une analyse afin de déterminer si l'affaire britannique *R (Bridges) v Chief Constable of the South Wales Police* aurait connu une issue similaire si elle avait été entendue au Canada. L'exercice de droit comparé permet

d'identifier certaines lacunes des lois québécoises et canadiennes en matière de protection de la vie privée et de protection des renseignements personnels. Cette analyse est aussi l'occasion d'adresser une mise en garde contre le « techno-solutionnisme » qui pourrait guider la décision de recourir à ce type de technologies de reconnaissance faciale. L'auteur souligne également l'absence d'obligation en droit québécois et canadien de considérer le critère d'intérêt public pour traiter des données personnelles. Ce constat amorce la réflexion sur la vie privée en tant que droit collectif qui sera traité plus en détail dans les deux textes qui suivent.

[8] La vie privée des groupes : nouveau cadre théorique pour une protection contre le profilage algorithmique. Il est question dans cet article de l'émergence de la notion de groupe algorithmique qui découle de l'exploitation de mégadonnées. À la lumière de cette nouvelle réalité, Simon DU PERRON se prononce en faveur d'une redéfinition du droit à la vie privée qui serait élargi de manière à reconnaître l'intérêt qu'ont les groupes (en tant que groupe) de ne pas faire l'objet de discrimination basée sur des biais résultant du traitement algorithmique des données. À l'appui de son propos, l'auteur présente habilement trois pistes théoriques émergentes qui influenceront le développement d'une théorie de la vie privée groupale plus aboutie.

[9] Les vulnérabilités inhérentes à l'approche individualiste des données de santé dans l'« ère big data ». Fabien LECHEVALIER, tout comme l'auteur du texte précédent, fait le constat suivant : le paradigme de l'individualité en matière de vie privée est insuffisant dans le contexte technologique actuel. En outre, il formule une critique à l'endroit des théories traditionnelles de la vie privée spécifiques au secteur de la santé. Il analyse plus particulièrement l'approche avis et choix qui est actuellement préconisée dans le cadre du traitement de renseignements personnels sur la santé en présentant ses principales lacunes. Il avance l'hypothèse que des pistes de solutions pour pallier ces lacunes pourraient se trouver dans une approche collectiviste de la vie privée.

[10] Les données personnelles à l'épreuve du big data des décisions de justice : entre principe de transparence de la justice et droit à la vie privée. S'il est acquis que l'exploitation technologique des données de santé peut susciter des situations de vulnérabilité, le traitement technologique des données judiciaires en soulève également. Dans cet

article, Flora DORNEL s'intéresse à certains enjeux en présentant les conceptions française et canadienne de la transparence du système de justice et en expliquant comment, dans les deux systèmes juridiques, l'*open data* judiciaire influe sur ce principe primordial qu'est la transparence de la justice. Cette analyse met en lumière un bouleversement de l'équilibre préexistant entre le droit à la vie privée et le principe de transparence du système judiciaire. Pour rétablir l'équilibre - ou en trouver un nouveau - l'auteure propose d'appliquer les principes du *privacy by design* dans le cadre du développement de solutions de diffusion de l'information judiciaire en ligne.

[11] Appréhender les inégalités d'accès à la justice par les médias sociaux : une perspective empirique sur l'information juridique. Alexandra BAHARY-DIONNE présente quant à elle, les résultats d'une étude ethnographique qui traite de l'accès à l'information juridique en ligne. Son analyse du contenu des échanges entre les membres de deux groupes Facebook destinés au partage d'information juridique démontre que le numérique tend à renforcer les vulnérabilités préexistantes quant à l'accès au droit et à la justice. Ce constat amène l'auteure à proposer une vision étendue de la cyberjustice : une vision qui prendrait en compte les disparités entre les divers groupes sociaux dans le cadre de la conception et la mise en œuvre des technologies judiciaires. Enfin, elle met de l'avant une vision qui ne postulerait pas que les initiatives qui aident certains groupes sont nécessairement bénéfiques pour tous.

[12] Vulnérabilités + contrat électronique : l'exemple du consentement électronique. Bien qu'a priori, les points de recoupement entre les questions de contrats numériques et l'accès à l'information juridique par la « cyberjustice informelle » ne semblent pas si évidents, l'article de Ledy Rivas ZANNOU s'inscrit sans contredit dans la continuité logique de celui d'Alexandra BAHARY-DIONNE puisqu'il traite des difficultés d'accessibilité et de compréhensibilité des contenus contractuels. L'auteur met en perspective les principaux obstacles – inflation informationnelle et déficience communicationnelle – qui nuisent à l'intégrité du consentement dans les contrats numériques. Suivant ce constat, il explore certaines avenues innovantes qui pourraient permettre de pallier ces lacunes. Parmi celles-ci, on peut citer en exemple la simplification « algorithmisée » des contrats pour les rendre plus intelligibles. Il s'agit là uniquement de l'une des nombreuses solutions proposées dans l'article.

[13] La vulnérabilité des engagements pris par les États pour protéger et promouvoir la diversité des expressions culturelles dans l'environnement numérique : quelle(s) stratégie(s) pour les Parties à la Convention de 2005 ? Enfin, Clémence VARIN boucle la boucle avec sa contribution. Elle rejoint dans une certaine mesure l'idée de co-régulation avancée par Johannes BRAKE au tout début en la faisant atterrir cette fois dans le contexte précis de la culture. Dans un contexte où les plateformes numériques comme Netflix ou Spotify font émerger un certain nombre de défis en matière de protection et de promotion de la diversité des expressions culturelles par les États, l'auteure s'attarde sur la mise en œuvre d'un article spécifique de la Convention sur la diversité des expressions culturelles de l'UNESCO. Elle expose différentes enceintes dans lesquelles les Parties auraient intérêt à faire la promotion des objectifs et principes de ce traité afin de continuer à garantir la protection et la promotion de la diversité des expressions culturelles dans l'environnement numérique et ainsi respecter leurs engagements vis-à-vis de ce dernier. Elle explore notamment l'idée de co-régulation et de l'inclusion de considérations culturelles dans les déclarations et les codes d'éthiques qui se multiplient dans le domaine de l'IA comme un moyen d'atteindre les objectifs de cette convention dans l'environnement numérique. Ainsi, l'article de Clémence Varin constitue un exemple appliqué d'une situation où la co-régulation pourrait permettre concrètement de mitiger des vulnérabilités émergentes.

[14] Passer le témoin ! Cette concertation des divers acteurs constitue également une piste à explorer dans les domaines de la santé ou de la justice par exemple. Peut-être ces questions seront-elles abordées lors de la 4e édition des Rencontres Jeunes Chercheurs Droit & Numérique ? La publication de ce numéro fut une expérience formatrice pour bon nombres d'entre nous. Nous remercions tous ceux qui y ont travaillé et espérons sincèrement que l'avenir en fera une tradition pérenne.

CO-REGULATION OR CAPITULATION ? ADDRESSING CONFLICTS ARISING BY AI AND STANDARDIZATION

Johannes BRAKE[1]

1 Doctoral Candidate, Chair for Constitutional and Administrative Law, Faculty of Law, Saarland University ; E-mail : johannes.brake@uni-saarland.de

Summary

While an enormous number of business models and opportunities based on artificial intelligence (AI) turn it into an essential technology for competitiveness in the digital age, risks arise as well, recognized globally in a vast amount of policy statements. An adequate regulation that reconciles high-level ethics, dynamic technological progress and enforceable rules calls for cooperation, which can be found in legally referenceable technical standards. Such co-regulation reduces frictions between static rules and dynamic technology and allows for a flexible and dynamic legal framework for AI. But standard-setting is subject to strong competition and not without conflict. The implications of competition for AI-standards and differing ethics and values on AI-standardization are not yet clear. Competition due to diverging ethical approaches and ambitions means that standardization is more than a merely technical issue. While this aspect is reflected in part by AI-standards presented in this paper, important specifications and guidance for foreseeable collisions and conflicts are missing. This has to be accounted for in emerging regulation of AI. Further concretization with regard to the structure, competencies and boundaries of co-regulation is necessary. This paper pursues these issues with a focus on conflict and convergence in the regulatory framework of AI applications across jurisdictional boundaries. It provides insight in emerging AI-standards and obstacles for cooperation in national approaches to AI, thereby offering a starting point for further research regarding regulatory frameworks that incorporate AI-standards as an instrument of co-regulation. This paper shows that standards form already an important instrument in AI-regulation and outlines three approaches how to advance this development, indicating that the challenges for co-regulation of AI can most likely be mastered.

A. INTRODUCTION

[1] Measurable advantages in business operations turn AI into an essential technology for competitiveness in the digital age[2]. Growing industry adoption raised the question of rules for AI and sparked the publication of countless policy papers and research regarding ethical development and deployment of AI-systems[3], moving the discussion far beyond *Asimov's* "robot laws". The need for regulation that reconciles high-level ethics, dynamic technological progress and enforceable rules calls for multi-stakeholder cooperation in the process of developing and enforcing rules, which can be found in co-regulation. This encompasses in the broadest sense all variations of regulation between state-exclusive and industry self-regulation[4]. Combining abstract legislation with concrete technical standards constitutes one form of such co-regulation, reducing frictions between static rules and dynamic technology. In general, technical standards can allow for a flexible and dynamic legal framework in three ways: They are embedded or referenced in legislation and regulation, or they can serve as guidelines in the application and interpretation of general legal terms and concepts[5]. For AI, standards that address terminology, processes and products could determine how AI has to be developed, implemented and evaluated by industry and supervisors. This could create a level playing field globally while being voluntary and innovation-friendly[6].

[2] However, due to its far-reaching effects, standard-setting is subject to strong competition and not without conflict. The implications of competition for AI-standards and how the ethical dimension of AI affects

2 For common examples in finance see Cavanillas/Curry/Wahlster, «The Big Data Value Opportunity» in Cavanillas/Curry/Wahlster, *New Horizons for a Data Driven Economy*, Springer, 2016, pp. 3, 4; Frost/Gambarcorta/Huang/Shin/Zbinden, *BigTech and the changing structure of financial intermediation*, BIS Working Paper, 2019.

3 Jobin/Ienca/Vayena, *Artificial Intelligence: the global landscape of ethics guidelines*, arxiv 2019; Russell, «Provably beneficial artificial intelligence» in De Grey/Rossiter, *The Next Step: Exponential Life*, BBVA OpenMind, 2017; Bostrom/Yudkowsky, «The Ethics of Artificial Intelligence», in Ramsey/Frankish, *Cambridge Handbook of Artificial Intelligence,* Cambridge 2014; Wallach/Allen, *Moral Machines,* Oxford 2009.

4 See Hoffmann-Riem, «Artificial Intelligence as a Challenge for law and Regulation» in Wischmeyer/Rademacher, *Regulating Artificial Intelligence*, Cham 2020, p. 18-22, 24; Barraud, «La corégulation d'Internet (ou comment répondre á la plurinormativité par l'internormativité) - une contribution francaise», (2018) *Les Cahiers de Droit* Vol. 59, pp. 91-97.

5 For example terms like "state of the art", "best available", "best practicable". See Büthe/Mattli, *The New Global Rulers*, Princeton 2011, pp. 6, 17, 205; Büthe/Mattli, «Setting International Standards», (2003) *World Politics* Vol 56, p.7; See for other jurisdictions and areas; Kablan/Oulai, «L'essence des approches du droit cyberspatial et l'opportunité de la co-régulation», (2009) *Revue générale du droit* Vol 39, pp. 37-39; Busch, «Towards a "New Approach" in European Consumer Law: Standardisation and Co-Regulation in the Digital Single Market», (2016) *EuCML*, pp. 197, 198; Peng, «Private Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime», (2018) *Cornell International Law Journal* Vol. 51, pp. 450-453, 455.

6 Scherer, «Regulating Artificial Intelligence», (2016) *Harvard Journal of Law & Technology* Vol. 29, pp. 373, 387-388, 395; Hoffmann-Riem, «Artificial Intelligence as a Challenge for law and Regulation» in Wischmeyer/Rademacher, *Regulating Artificial Intelligence*, Cham 2020, pp. 21-23; Büthe/Mattli, *The New Global Rulers*, Princeton 2011, p. 4.

the relationship between cooperation and competition are not yet clear. While research about AI-regulation is emerging, it is largely abstract, focusing on regulatory experience[7], national frameworks[8] or cooperation[9]. This paper seeks to sharpen the view on AI-regulation by providing insight in where emerging co-regulation might find AI-standards (B) and how competition and obstacles for cooperation are rooted in national AI-strategies (C), thereby offering a starting point for conception of future regulatory frameworks and re-evaluation of instruments for co-regulation (D).

B. REGULATING AI WITH THE HELP OF STANDARDS

[3] Standards for AI are being suggested in various kinds of documents, ranging from ethical guidelines to technical specifications. For the aim of this paper and in the context of co-regulation in need for specific rules, standards will be understood only as more or less technical specifications, which from a process-oriented view can roughly be categorized into informal standards produced by companies and consortia in marked-driven processes, and formal standards developed in a network of state or state-accredited organizations following a set procedure[10].

I. INFORMAL STANDARDS FOR AI

[4] In the IT-sector, self-regulation by company-produced informal standards is common, making market dominance of companies a decisive factor for regulatory outcome[11]. Therefore, leading technology companies could direct the way their industry approaches AI. If this will be the case is uncertain as AI is still a field of dynamic development, but we can already observe the formation of standardization consortia[12]. For example, MLPerf is an approach to measure specific AI performance as fairly as possible, taking ethics into consideration[13]. On the other hand, as

7 Cihon/Maas/Kemp, *Should Artificial Intelligence be Centralised? Design Lessons from History*, 7.2.2020, retrieved from < https://www.cser.ac.uk/resources/should-AI-governance-centralised>.

8 Scherer, «Regulating Artificial Intelligence», (2016) *Harvard Journal of Law & Technology* Vol. 29.

9 Cihon, *Standards for AI Governance*, Oxford 2019, retrieved from <https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf>.

10 For a different terminology see for example Belleflamme, «Coordination on formal vs. de facto standards: a dynamic approach», (2002) *European Journal of Political Economy* Vol. 18, p. 153.

11 See Büthe/Mattli, *The New Global Rulers*, Princeton 2011, pp. 27, 37.

12 For example World Wide Web Consortium (W3C), Industrial Internet Consortium (IIC), MLPerf, Alliance for Internet of Things Innovation (AIOTI), FIWARE.

13 MLPerf Training Rules, 2.1, see <https://github.com/mlperf/training_policies/blob/master/training_rules.adoc> and <https://mlperf.org/about/#philosophy>.

informal standards are criticized for a deficit of political accountability and regulatory structure[14], formal standardization is gaining momentum and could play an integral part in AI-regulation.

II. FORMAL STANDARDS FOR AI

[5] For AI as a global technology utilized by global actors, substantial standardization occurs on the international level, where standards are developed in centrally coordinated global organisations, in which countries can't be direct members. As early as 2017, the International Standards Organisation (ISO) and International Electrotechnical Commission (IEC) established a joint subcommittee working on AI-specific challenges, which already issued documents addressing the data aspect of AI[15], while other committees work on adherent issues[16].

[6] In parallel, there are initiatives on the national level as well. In 2019 the German standardization organisation DIN published **DIN SPEC 92001-1** regarding quality assessment and risk evaluation of (ethically) critical AI-systems[17]. For the USA, the American National Standards Institute (ANSI) publishes standards developed by accredited private organizations[18] such as the Institute of Electrical and Electronics Engineers (IEEE), whose **IEEE P7000-series** is expected to have significant impact. Its first document on AI establishes an impact assessment[19] with further projects addressing transparency, privacy, bias and value-based AI[20]. Similarly, the Standards Council of Canada published the privately developed AI-standard **CAN/CIOSC 101:2019** for design and usage of AI-Systems, introducing minimum requirements for the organizational structure of AI-companies

14 Cath/Wachter/Mittelstadt/Taddeo/Floridi, «Artificial Intelligence and the 'Good Society'», (2018) *Sci. Eng. Ethics* 24, pp. 505, 507, 513, Saurwein/Just/Latzer, «Governance of Algorithms: options and limitations», (2015) *info* Vol 17 No. 6, pp. 35, 41.

15 Publications of ISO/IEC JTC 1/SC42 address big data terminology, reference architecture, Use cases and derived requirements, trustworthiness of AI and a Standards roadmap, while work in development addresses issues from Governance implications, over terminology and an Assessment of robustness to Bias in AI systems, Risk Management and computational approaches, see <https://www.iso.org/committee/6794475/x/catalogue/p/1/u/0/w/0/d/0>.

16 Software and processes, programming languages, graphics and data representation, cybersecurity and privacy protection, see ISO/IEC JTC 1 SC 7, 22, 24 and 27.

17 While it doesn't contain specific requirements concerning ethical conduct, it introduces a differentiation with regard to risk and criticality, referring to the relevance of AI-systems to safety, security, privacy or ethics, see DIN SPEC 92001-1:2019-04 - Artificial Intelligence - Life Cycle Processes and Quality Requirements Part 1: Quality Metamodel, pp. 6, 15, 16.

18 For example the AI-standard ANSI/CTA-2089 for terminology in health care.

19 IEEE 7010-2020 - IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being.

20 See Koene/Smith/Egawa/Mandalh/Hatada, IEEE P70xx, Establishing Standards for Ethical Technology, Proceedings of KDD, KDD'18, 2018.

and for processes to implement ethical considerations, without specifying ethical requirements itself[21].

III. STANDARDS BETWEEN COOPERATION AND COMPETITION

[7] Despite the early stage of AI-standardization, this selection of AI-documents indicates that standardization is being taken seriously on the global and national level and that ethical issues are considered essential for AI. Regulatory frameworks could soon utilize AI-standards as a form of co-regulation.

[8] But as the race for AI-standards has started, competition is emerging, illustrated by the different approaches between formal and informal standardization. Another form of competition, between states, seems at first sight contradictory to the harmonizing function of international standards that reduce barriers to trade in global markets across jurisdictions[22]. In this spirit, the Agreement on Technical Barriers to Trade obliges members of the World Trade Organization to use international standards as the technical basis of domestic laws and regulations[23]. Indeed, this indicates how standards spread globally : They provide a first-mover advantage to the initiator, which results in a strong incentive to push national standards globally in support of domestic champions[24]. Complaints against voting blocs illustrate the competition inherent to international standardization[25]. For AI, another aspect could prove to be an obstacle for international cooperation: The underlying conflicts could be reinforced by diverging values. Standards influence technological design, which impacts social interactions and is influenced by values of the designer, even though the technical language of standards might

21 For example AI-risk officers, CAN/CIOSC 101:2019, pp. 9, 12; The Conference Board of Canada, *Getting Aligned. How Adopting Standards Affects Canada's Productivity and Growth*, Standards Council Canada, 2015, p. 5.

22 Büthe/Mattli, *The New Global Rulers*, Princeton 2011, p. 6.

23 WTO, Agreement on Technical Barriers to Trade, Art. 2.4 TBT and Annex 3 F TBT.

24 Büthe/Mattli, *The New Global Rulers*, Princeton 2011, p. 4, 9; Egan, «Setting Standards: Strategic Advantages in International Trade», (2002) *Business Strategy Review* Vol. 13 (1), pp. 51, 59; Cihon, *Standards for AI Governance*, Oxford 2019, p. 22, retrieved from <https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf>.

25 Egan, «Setting Standards: Strategic Advantages in International Trade», (2002) *Business Strategy Review* Vol. 13 (1), p. 61.

make this aspect less visible[26]. As standards are not purely technical, differences in ethics and values might lead to further conflicts.

C. CONFLICTING APPROACHES TO AI AND ETHICS

[9] A review of 84 documents on AI and ethics identifies eleven shared principles, out of which transparency, fairness, beneficence, accountability and privacy are dominant[27]. Another analysis identified twelve ethical principles in 100 documents[28]. While both reviews find fairness and transparency to be central[29], the findings differ substantially. Furthermore, a differentiation between the issuers of the documents changes the results; transparency and accountability being predominantly shared principles among public actor policies[30]. Apart from transparency, no consensus on ethics for AI is found - and even shared principles require interpretation and concretization[31]. The strategic positions to ethics and standardization of major global players illustrate political competition for regulatory approaches to AI more clearly.

26 See Reidenberg, «Governing Networks and Rule-Making in Cyberspace», (1996) *Emory Law Journal* Vol. 45, pp. 918, 927-928 ; Reidenberg, «The Rule of Intellectual Property Law in the Internet Economy», (2007) *Houston Law Review* Vol. 44, pp. 1075-1076 ; Orwat/Bless, «Values and Networks», (2016) *ACM SIGCOMM Computer Communication Review* 46 no. 2, p. 25; Koops, «Criteria for Normative Technology» in Brownsowrd/Yeung, *Regulating Technologies*, Oxford and Portland 2008, p. 157 ; regarding growing challenges Reidenberg, «Lex Informatica: The Formulation of Information Policy Rules through Technology», (1997) *Texas Law Review* Vol. 76, p. 592; Selbst/Boyd/Friedler/Venkatasubramanian/Vertesi, *Fairness and Abstraction in Sociotechnical Systems*, 2018, pp. 2-3, 8 retrieved from <https://dl.acm.org/doi/pdf/10.1145/3287560.3287598> ; Kroes/van de Poel, «Design for Values and the Definition, Specification, and Operationalization of Values», in van den Hoven/Vermaas/van de Poel, *Handbook of Ethics, Values, and Technological Design*, Dordrecht 2014, pp. 168-170 ; Büthe/Mattli, *The New Global Rulers*, Princeton 2011, pp. 12, 33, 41, 45.

27 Tansparency, fairness, beneficience, accountability, privacy, harmlessness and safety, freedom with autonomy and self-determination, trust, dignity, sustainability, solidarity. Dominance meaning being mentioned in more than half of the documents, Jobin/Ienca/Vayena, *Artificial Intelligence: the global landscape of ethics guidelines*, arxiv 2019, pp. 3, 7.

28 Accountability, safety, human control, reliability, stability, fairness, diversity and non-discrimination, sustainability, transparency, multi stakeholder engagement, lawfulness and compliance, privacy and data protection, Perrault/Shoham/Brynjolfsson/Clark/Etchemendy/Grosz/Lyons/Manyika/Mishra/Niebles, «The AI Index 2019 Annual Report», Stanford University, 2019, p. 148.

29 Jobin/Ienca/Vayena, *Artificial Intelligence: the global landscape of ethics guidelines*, arxiv 2019, p. 6; Perrault/Shoham/Brynjolfsson/Clark/Etchemendy/Grosz/Lyons/Manyika/Mishra/Niebles, «The AI Index 2019 Annual Report», Stanford University, 2019, p. 148.

30 Cath/Wachter/Mittelstadt/Taddeo/Floridi, «Artificial Intelligence and the 'Good Society'», (2018) *Sci. Eng. Ethics* 24, pp. 505, 523. See also Greene/Hoffmann/Stark, «Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning», *Proceedings of the 52nd Hawaii International Conference on System Sciences 2019*, retrieved from <https://scholarspace.manoa.hawaii.edu/bitstream/10125/59651/0211.pdf>; Zeng/Lu/Huangfu, *Linking Artificial Intelligence Principles*, arxiv 2018, retrieved from <https://arxiv.org/pdf/1812.04814.pdf>.

31 Yeung/Weller, «How is Transparency understood by legal scholars and the machine learning community?» in Bayamligolu/Baraliuc/Janssens/Hildebrandt, *Being Profiled: Cogitas Ergo Sum*, Amerstam 2018, pp. 37, 39; Zeng/Lu/Huangfu, *Linking Artificial Intelligence Principles*, arxiv 2018; Jobin/Ienca/Vayena, *Artificial Intelligence: the global landscape of ethics guidelines*, arxiv 2019, pp. 7, 13, 14; Perrault/Shoham/Brynjolfsson/Clark/Etchemendy/Grosz/Lyons/Manyika/Mishra/Niebles, «The AI Index 2019 Annual Report», Stanford University, 2019, p. 149; Haas/Gießler/Thiel, «In the realm of paper tigers», AlgorithmWatch, 28.4.2020, retrieved from <https://algorithmwatch.org/en/ai-ethics-guidelines-inventory-upgrade-2020/>.

I. THE EUROPEAN APPROACH

[10] According to the EU-Commission, AI-regulation should follow a "European Approach" aligned to European values[32]. A risk-based approach to AI-regulation will focus on criticality and individual impact. Additionally, product liability law, an area especially relevant for standards, might be substantially extended[33]. Regarding foreseeable competition in AI, standardization is regarded as a central regulatory instrument for supporting technical leadership of Europe[34]. The European Parliament aims at guarding industry from non-EU standards as well[35]. This follows a general trend, as the EU seeks stronger influence in global IT-standardization[36].

II. THE US-APPROACH

[11] AI is considered central for global US-leadership as well and American values are to be promoted in a competitive AI-strategy that favours innovation over regulation[37]. This aims at avoiding enforceable technical specifications[38] and restraining regulatory action[39]. Similar to the EU, risk-based regulation is suggested, however with an emphasis on mitigating competitive disadvantages for US-companies by allowing flexible implementation and enforcement of principles[40]. Therefore, standardization that leaves the leading role to the private sector is preferable to other regulatory instruments[41]. While the USA seems to avoid formal standardization that could be referenced in enforceable regulation and prefers private standardization that protects established

32 EU-Commission, COM(2018) 320 final, 15.5.2018, pp. 5, 9, 11.

33 EU-Commission Expert Group on Liability and New Technologies – New Technologies Formation, *Liability for Artificial Intelligence*, 2019.

34 EU-Commission, COM(2018) 320 final, 15.5.2018, pp. 5, 9, 11; EU-Commission, Joint Initiative on Standardisation, p. 2.

35 European Parliament, Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 2017.

36 EU-Commission, White Paper Modernising ICT Standardisation in the EU - The Way Forward, COM(2009) 324 final, 2009; EU-Commission, Communication - European Standards for the 21st Century, (2016) 358 final, 2016; EU-Commission, Communication - ICT Standardisation Priorities for the Digital Single Market, COM(2016) 176 final, 2016.

37 White House, Executive Order 13859 Maintaining American Leadership in Artificial Intelligence, 2019; White House, Memorandum for the Heads of Executive Departments and Agencies, 2020, pp. 4, 7.

38 White House, Memorandum for the Heads of Executive Departments and Agencies, 2020, p. 5.

39 See Regulatory Impact Analysis, White House, OMB Circular A-4, Regulatory Analysis, 17.9.2003; White House, Memorandum for the Heads of Executive Departments and Agencies, 2020, pp. 11-13.

40 White House, Memorandum for the Heads of Executive Departments and Agencies, 2020, pp. 4, 5.

41 White House, Memorandum for the Heads of Executive Departments and Agencies, 2020, p. 7; White House, OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, 27.1.2016.

US-champions, global leadership in AI-standards is a strategic goal[42]. In this light, the US standardization organisation ANSI seeks to fight the long-standing trend of a weak US-position in formal standardization and position government experts in leading positions on the international level[43]. Similarly, the US seeks influence by joining the G7 Partnership on AI following initial efforts of resistance[44].

III. THE CHINESE APPROACH

[12] China developed AI-strategies as early as 2016, underlining its ambition to lead in international rules and technology for AI[45]. The Chinese strategy for standardization reflects this position, being considered both a cornerstone of Chinese AI-regulation and a competition policy[46]. Furthermore, China too aims at implementing its ethics in AI-standards[47]. In this context, AI should allow societal advancement and control[48]. Given the existing Chinese Social Credit System[49], the scope of this view becomes clear. This also reflects the Chinese top-down and state-lead approach as well as the growing Chinese initiative in standard-setting[50].

42 White House, *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, 2019; White House, *Executive Order 13859 Maintaining American Leadership in Artificial Intelligence*, 2019. See also Cath/Wachter/Mittelstadt/Taddeo/Floridi, «Artificial Intelligence and the 'Good Society'», (2018) *Sci. Eng. Ethics* 24, pp. 505, 513.

43 ANSI, Comments from the American National Standards Institute on National Institute of Standards and Technology Request for Information on Artificial Intelligence Standards, pp. 3, 6, 7; Mattli/Büthe, «Setting International Standards», (2003) World Politics Vol. 56, p. 24.

44 US Department of State, *Joint Statement From Founding Members of the Global Partnership on Artificial Intelligence*, 15.6.2020, retrieved from <https://www.state.gov/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence>.

45 Ministry of Industry and Information Technology, *Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018–2020),* translated by Triolo/Kania/Webster, retrieved from <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020>; State Council, *A Next Generation Artificial Intelligence Development Plan*, 2017, translated by Sapio/Chen/Lo, retrieved from <https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf>.

46 Zhang/Yang/Qian/Tang/Luo/Leng/Li/Han, «Artificial Intelligence and People's Consensus» in Jin, *Reconstructing Our Orders*, 2018, p. 24; Cihon, *Standards for AI Governance*, Oxford 2019, pp. 21, 23; Ding, *Deciphering China's AI Dream*, Oxford 2018.

47 SAC, «National Guidelines on AI Standards System Released», 17.8.2020, retrieved from <www.sac.gov.cn/sacen/events/202008/t20200817_346835.htm>. SECSEC, Guidelines for the Establishment of the New Generation of Artificial Intelligence Standards System, 25.8.2020, retrieved from <https://www.secsec.eu/guidelines-for-the-establishment-of-the-new-generation-of-artificial-intelligence-stamdards-system-released-by-sac-cac-ndrc-most-and-miit-in-china/framework-of-china-ai-standards>.

48 AI as "Moral Tools", Sun, «Artificial Intelligence and Ethical Principles» in Jin, *Reconstructing Our Orders*, 2018, pp. 31-38, 50, 69; see also, National Information Security Standardization Technical Committee, *Artificial Intelligence Security Standardization White Paper*, translated by CSET, 2019, retrieved from <https://cset.georgetown.edu/wp-content/uploads/t0121_AI_security_standardization_white_paper_EN.pdf>.

49 State Council, Guiding Opinions of the State Council on Establishing and Improving the System of Joint Incentive for Keeping Faith and Joint Punishment for Losing Faith and Accelerating the Advancement of the Development of Social Honesty, 2016, retrieved from < http://en.pkulaw.cn/Display.aspx?LookType=3&Lib=law&Cgid=272126&Id=22433&SearchKeyword=&SearchCKeyword=&paycode=>.

50 Murphree/Breznitz, «Innovation in China: Fragmentation, Structured Uncertainty, and Technology Standards», (2013) *Cardozo Law Review*, p. 203; Peng, «Private Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime», (2018) *Cornell International Law Journal* Vol. 51, pp. 448-450; Peng, «Standards as a Means to Technological Leadership? China's ICT Standards in the Context of the International Economic Order» in Toohey/Picker/Greenacre, *China in the International Economic Order*, Cambridge 2015, pp. 128-129.

D. ADDRESSING CHALLENGES TO AI REGULATION

[13] Emerging conflicts due to political competition and differences in values are acknowledged in China[51] and in other countries, reinforcing the incentive to install government experts in relevant organizations as well as an alignment with strategic partners[52]. How the increased motivation for states to engage in standard-setting will affect cooperative regulation of AI has to be observed and evaluated. But experience in other areas shows that due to political competition different regulatory approaches persist[53]. Competition and conflicting values could prove as an obstacle for cooperation in setting international standards or result in competing national standards for AI. This raises concerns that a global landscape of AI-regulation fragmented by national strategies and industry initiatives could lead to a "race to the bottom", allowing companies to choose favourable regulation and leading to risks not being addressed[54]. Therefore, especially regarding fundamental value-based decisions, national legislation is called for[55]. While this could reinforce fragmentation, stricter local rules could also set a global benchmark, similar to EU-data protection law. In both cases, cooperation loses to competition.

[14] However, the amount of cooperation possible will ultimately depend on the specific regulatory framework on both national and international levels. Three ways to mitigate emerging conflicts could be explored: First an openness of technology and standards for a pluralism of ethics, second a more detailed framework for AI-standardization on the

51 Chinese Ministry of Science and Technology, «Next Generation Artificial Intelligence Development Plan issued by State Council», *China Science & Technology Newsletter No. 17*, 15.9.2017, retrieved from <http://fi.china-embassy.org/eng/kxjs/P020171025789108009001.pdf>; Zhang/Yang/Qian/Tang/Luo/Leng/Li/Han, «Artificial Intelligence and People's Consensus» in Jin, *Reconstructing Our Orders*, 2018, pp. 39, 63, 75; Wang/Yu/Li/Jin, «Artificial Intelligence and International Norms» in Jin, *Reconstructing Our Orders*, 2018, pp. 203, 205, 207, 217, 222, 225.

52 See for example Australia, Department of Industry, Innovation and Science «Australia's Tech Future», Canberra 2018, p. 45; Cave/Hoffman/Joske/Ryan/Thomas, «Mapping China's Technology Giants», Australian Strategic Policy Institute, Canberra 2019, p. 17; Standards Australia, *An Artificial Intelligence Standards Roadmap*, 2020, pp. 4, 19-26.

53 Büthe/Mattli, *The New Global Rulers*, Princeton 2011, p. 11; Cihon, *Standards for AI Governance*, Oxford 2019, p. 7, 15; Baum/deNeufville/Barrett/Ackerman, «Lessons for Artificial Intelligence from Other Global Risks» in Tinnirello, *The Global Politics of Artificial Intelligence*, Boca Raton, forthcoming; Kim/Lee/Kwak, «The changing patterns of China's international standardization in ICT under techno-nationalism: A reflection through 5G standardization», (2020) *International Journal of Information Management* Vol. 54, 102145.

54 Wagner, «Ethics as an escape from regulation» in Bayamlioglu/Baraliuc/Janssens/Hildebrandt, *Being profiled: cogitas ergo sum*, Amsterdam 2018, p. 86; Cihon, *Standards for AI Governance*, Oxford 2019, pp. 7, 17; Radaelli, «The puzzle of regulatory competition», (2004) *Journal of Public Policy* 24 no. 1, p. 1; Egan, «Setting Standards: Strategic Advantages in International Trade», (2002) *Business Strategy Review* Vol. 13 (1), p. 61.

55 Scherer, «Regulating Artificial Intelligence», (2016) *Harvard Journal of Law & Technology* Vol. 29, pp. 379-380; Wagner, «Ethics as an escape from regulation» in Bayamlioglu/Baraliuc/Janssens/Hildebrandt, *Being profiled: cogitas ergo sum*, Amsterdam 2018, p. 86; Hoffmann-Riem, «Artificial Intelligence as a Challenge for law and Regulation» in Wischmeyer/Rademacher, *Regulating Artificial Intelligence*, Cham 2020, p.7. See also Slaughter, «The real new world order», (1997) *Foreign Affairs* Vol. 76, p. 197.

international level, and third increased guidance on the adoption and reception of standards on the national level.

[15] However, the amount of cooperation possible will ultimately depend on the specific regulatory framework on both national and international levels. Three ways to mitigate emerging conflicts could be explored: First an openness of technology and standards for a pluralism of ethics, second a more detailed framework for AI-standardization on the international level, and third increased guidance on the adoption and reception of standards on the national level.

[16] Limiting cooperation and standardization to strictly technical questions might limit emerging conflicts. However, since it is unlikely that completely undisputed areas of standard-setting can be identified, the scope of this approach seems limited. More promising is a strict approach to ethical pluralism implemented in AI-standards[56], as aimed for in CAN/CIOSC 101:2019[57]. Standardized impact assessments and risk evaluations leave room for diverse ethical specifications. Yet, to answer how neutral such frameworks really are, how to implement value-neutral standardization and how to reconcile this with regulating "by design"[58], further research would be required.

[17] Alternatively, the procedure of standard-setting could be adjusted[59] : International law could be leveraged for imposing stricter rules[60] for example regarding national delegations according to Annex 3 TBT-Agreement[61], restraining the influence of governments and favoring pluralistic national structures as a prerequisite for contributions to

56 Jobin/Ienca/Vayena, *Artificial Intelligence: the global landscape of ethics guidelines*, arxiv 2019, pp. 16, 17; retrieved from <https://arxiv.org/pdf/1906.11668.pdf>.

57 Another way could be listing all ethical considerations, see the project ISO/IEC AWI TR 24368 - Information Technology - Artificial Intelligence - Overview of ethical and societal concerns.

58 Stuart Russell proposes a "value function" for AI-systems, see Wolchover, «The Artificial Intelligence Pioneer has a few concerns», *Wired*, 23.5.2015, retrieved from: <https://www.wired.com/2015/05/artificial-intelligence-pioneer-concerns>; Russell, «Provably beneficial artificial intelligence» in BBVA OpenMind, *The Next Step: Exponential Life*, 2017while others are skeptical, Koops, «Criteria for Normative Technology» in Brownsowrd/Yeung, *Regulating Technologies*, Oxford and Portland 2008, p. 170; see also Reidenberg, «The Rule of Intellectual Property Law in the Internet Economy», (2007) *Houston Law Review* Vol. 44, p. 1095.

59 See for internet regulation Brown/Marsden, Regulating Code. Good Governance and Better Regulation in the Information Age, Cambridge, 2013, p. 198.

60 Compared for example to the ISO code of ethics and code of conduct, see <https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/codeethics_2004-en.pdf> and <https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100397.pdf> and ISO Directive 1, Procedures for the technical work, 1.7.1., which refers simply to National Bodies.

61 WTO, Agreement on Technical Barriers to Trade, Annex 3 B, G. See also Mattli/Büthe, «Setting International Standards», (2003) *World Politics* Vol. 54, p. 42.

standardization[62]. This could limit political conflicts and foster cooperation. By contrast, new general international treaties for AI might not help cooperation but just add another layer of complexity[63] and are in any case not very promising in light of the power shift from institutions like the WTO to less formalized structures like the Organisation for Economic Cooperation and Development (OECD)[64], illustrated also by the initiatives of the G7 Partnership for AI[65].

[18] A completely contrasting approach could be applied at the national level that emphasizes stronger involvement of the state by creating competent national agencies for AI-regulation[66]. This could result in stronger regulatory guidance of co-regulation regarding the reception of AI-standards by evaluating, approving or extending them and requires the legislator to structure the process and to provide necessary incentives[67]. While national rules for fundamental value-based decisions become possible, standard-setting could remain unaffected and co-regulation supported.

E. CONCLUSION

[19] This paper showed that standards form an important instrument in regulatory approaches to AI globally by exploring AI-standards and corresponding strategies. While AI-standards could allow for co-regulation of AI, conflicts are emerging as it can be assumed that relevant actors will not give up their expressed ambition to influence standardization of AI. Differences in ethics and values could pose challenges to the cooperation

62 In Western Europe and South America, private, non-profit organizations dominate while North America has a mixed landscape of standardization organizations and in Asia state-lead organizations dominate. However, the level of autonomy is difficult to ascertain. See <https://www.iso.org/members.html#:~:text=ISO%20members%20%20%20-Country%2FTerritory%20%20,%20%202%20%2052%20more%20rows%20>.

63 Cihon/Maas/Kemp, *Should Artificial Intelligence be Centralised? Design Lessons from History*, 7.2.2020, retrieved from < https://www.cser.ac.uk/resources/should-AI-governance-cen-tralised>.

64 See early Slaughter, «The real new world order», (1997) *Foreign Affairs* Vol. 76.

65 Installing the Secretariat of the G7 GPAI at the OECD, US Department of State, *Joint Statement From Founding Members of the Global Partnership on Artificial Intelligence*, 15.6.2020, retrieved from <https://www.state.gov/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence>.

66 For initiatives regarding central digital agencies in Europe, see European Parliament, Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL), 16.2.2017; German Parliament, *Answer of the Government - Specific Goals and Measures of the Government in the area of Artificial Intelligence*, BT-Drs. 19/1982, 27.4.2018, p. 8; see also Hoffmann-Riem, «Artificial Intelligence as a Challenge for law and Regulation» in Wischmeyer/Rademacher, *Regulating Artificial Intelligence*, Cham 2020, p. 13; stronger involvement suggested early by Reidenberg, «Lex Informatica: The Formulation of Information Policy Rules through Technology», (1997) *Texas Law Review* Vol. 76, p. 592.

67 This has proven effective in German Cybersecurity Regulation, where the Federal Office for Information Security publishes standards on basis of ISO-standards in a sophistica-ted legal framework.

necessary for setting standards and their suitability for national reception. As AI pushes for innovation in the regulator's toolbox, further research is necessary, for which this paper provided a starting point by outlining different levels of regulatory action, thereby indicating that challenges for co-regulation of AI can most likely be mastered.

QUELLES ŒILLÈRES IMPOSER À L'ÉTAT ? LE REGARD DU DROIT QUÉBÉCOIS SUR LA TECHNOLOGIE À RECONNAISSANCE FACIALE UTILISÉE PAR LES FORCES DE L'ORDRE AU ROYAUME-UNI

Samy CHEKIR[1]

1 L 'auteur est avocat et candidat au microprogramme de 2e cycle en droit des technologies de l'information à l'Université de Montréal.

Résumé

Dans cette contribution, nous portons un regard critique sur le recours aux caméras de surveillance munies d'une technologie de reconnaissance faciale par les autorités policières dans les lieux publics. Plus précisément, nous procédons à l'analyse d'une décision rendue par la High Court of Justice au Royaume-Uni ayant rejeté le recours d'un individu qui contestait la légalité de cette nouvelle technique d'enquête. Les arguments étudiés s'inscrivent essentiellement sous deux volets, soit d'une part le droit à la vie privée comme droit fondamental et d'autre part, l'encadrement législatif de ces technologies.

Nous procédons ensuite à l'analyse de la situation sous l'angle du droit canadien et québécois. Au terme de cette brève étude, nous constatons un certain nombre de similitudes entre le droit anglais et le droit canadien et québécois, et ce, tant sur le plan du droit de la vie privé que sur l'encadrement des technologies pouvant lui porter atteinte. Ceci étant, certaines différences nous laissent croire qu'un tribunal canadien n'en serait pas arrivé aux mêmes conclusions que la High Court of Justice dans l'état actuel du droit. Évidemment, la porte demeure ouverte pour le législateur qui peut en tout temps intervenir afin de permettre ou interdire le recours à une telle technologie par les autorités policières.

INTRODUCTION

[1] Les avancés technologiques des dernières années ont permis à certains États d'augmenter la surveillance sur leur territoire[2]. C'est ainsi que les gouvernements se sont de plus en plus dotés de caméras de surveillance leur permettant d'observer les faits et gestes de leurs citoyens. Plus récemment, s'est ajoutée une intelligence capable d'identifier automatiquement les personnes repérées par le biais de la reconnaissance faciale.

[2] Nous entreprendrons ici l'ambitieuse tâche de porter un regard sur les applications possibles de cette technologie et les limites de son utilisation en procédant à l'analyse d'une décision rendue par la High Court of Justice au Royaume-Uni[3]. L'exposé de ce cas d'étude nous permettra d'identifier certaines des nombreuses[4] règles applicables à l'utilisation de cette technologie par les autorités anglaises. Pour ce faire, nous porterons, dans un premier temps, un regard sur les protections offertes aux droits fondamentaux affectés avant de passer, dans un second temps, au cadre normatif structurant le recours à cette technologie. Nous nous attarderons par la suite à une étude analogue de certaines règles applicables au Québec dans un contexte similaire.

I. ROYAUME-UNI

I.1. CONTEXTE

[3] En septembre 2019, la High Court of Justice d'Angleterre et du Pays de Galles rendait une décision[5] portant sur la légalité de l'utilisation de caméras de surveillance à reconnaissance faciale en direct par les forces policières de South Wales (ci-après « SWP »)[6]. Le demandeur, Edward

2 Elly Cosgrove, *One billion surveillance cameras will be watching around the world in 2021, a new study says*, CNBC, 6 décembre 2019, en ligne : https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html; Matthew Keegan, *Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled*, The Guardian, 2 décembre 2019, en ligne : https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled; et Hannah Devlin, *'We are hurtling towards a surveillance state': the rise of facial recognition technology*, The Guardian, 5 octobre 2019, en ligne : https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state.

3 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin) (Demande d'autorisation d'appel accueillie).

4 Surveillance Camera Commissioner, *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*, 2019, p. 3, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf.

5 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3.

6 Pour une étude complète de l'utilisation de cette technologie par la SWP voir : Bethan Davies, Martin Innes et Andrew Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff Universities' Police Science Institute, 2018, en ligne : https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bdafb4403ce64828d6fbc04/1541077838619/AFR+Report+%5BDigital%5D.pdf.

Bridges, soutient être victime, comme bien d'autres, de violations à son droit à la vie privée des suites de l'utilisation par la SWP de l'outil AFR Locate[7]. Plus précisément, le demandeur soulève trois moyens identifiés par la Cour comme étant (1) la violation de son droit à la vie privée garanti par la *Convention européenne des droits de l'homme*[8], (2) la violation de ses droits prévus par les lois sur la protection des renseignements personnels et (3) l'obligation du secteur public de traitement égal des citoyens[9]. La présente étude ne fera état que des deux premiers moyens.

I.2. ANALYSE DE LA DÉCISION

A. *CONVENTION EUROPÉENNE DES DROITS DE L'HOMME*

[4] Se fondant sur l'article 8 de la *Convention* qui consacre le droit à la vie privée et ses limites, le demandeur estime que les nouvelles techniques d'enquête policières portent atteinte à ses droits fondamentaux. Au terme de l'analyse de ce premier moyen, la Cour conclut qu'il est vrai que le traitement de données biométriques des citoyens par les forces de l'ordre constitue une entrave importante à leur droit à la vie privée[10]. Le fait que ce traitement se produise dans un lieu public n'affecte en rien cette conclusion, puisque les citoyens conservent une expectative raisonnable de vie privée à l'égard de leur données biométriques même dans ces lieux[11]. En l'espèce, la Cour se dit toutefois satisfaite que le cadre normatif en place comprenant le *Data Protection Act 2018*[12], dont nous ferons état plus loin, le *Surveillance Camera Code of Practice*[13] ainsi que les politiques mises en place par la SWP suffisent à répondre au critère du second alinéa de l'article 8 de la *Convention*, soit la nécessité que l'ingérence soit

7 Pour une explication, voir Bethan Davies, Martin Innes et Andrew Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff Universities' Police Science Institute, 2018, en ligne : https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bdafb4403ce64828d6fbc04/1541077838619/AFR+Report+%5BDigital%5D.pdf, p. 4. Voir également : *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin) (Demande d'autorisation d'appel accueillie), par. 7, 23 et suiv.

8 *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, S.T.E. no 5 (entrée en vigueur le 3 septembre 1953) (ci-après « *Convention européenne des droits de l'Homme* » ou « *Convention* »).

9 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3., par. 18.

10 *Ibid*., par. 59 à 62 ; Voir aussi Surveillance Camera Commissioner, *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*, 2019, p. 3, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file.

11 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3., par. 54 et 57.

12 *Data Protection Act 2018*, 2018 c. 12. Notons, à titre informatif, que cette loi intègre au droit national les principes édictés par le *Règlement général sur la protection des données*, règlement no 2016/679. À cet effet, voir : Department for Digital, Culture, Media & Sport, *Data Protection Act 2018. Factsheet – Overview*, p. 2, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711162/2018-05-23_Factsheet_1_-_Act_overview.pdf.

13 Surveillance Camera Commissionner, *Surveillance Camera Code of Practice*, 2014, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

prévue par la loi[14]. Soulignons de plus que l'ingérence doit également constituer « une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui »[15]. Ce dernier volet est satisfait dès lors que l'ingérence passe le test établi par la jurisprudence[16], comme en l'espèce[17].

B. LOIS PARTICULIÈRES

[5] En ce qui concerne les revendications sous ce chapitre, nous concentrons notre analyse sur les articles 34 et 35 de la *Data Protection Act 2018* (ci-après « DPA 2018 ») d'une part et sur l'article 64 de cette même loi d'autre part.

[6] Suite à une analyse détaillée de ces dispositions, le Tribunal conclut dans un premier temps que le recours à la technologie AFR Locate est strictement nécessaire à l'accomplissement des fonctions de la SWP[18] et que l'objectif poursuivi est par ailleurs d'intérêt public[19]. La Cour déplore cependant le caractère trop général de la politique mise en place par la SWP pour l'utilisation de AFR Locate, mais elle retient qu'il revient au Commissaire à l'information d'établir les éléments que doivent prévoir de telles politiques. En l'espèce, la politique de la SWP, bien que peu précise en règle générale, suffit au contexte propre de l'affaire. Le Juge n'ira que d'un commentaire suggérant à la SWP de bonifier ses politiques suivant les recommandations du Commissaire à l'information lorsque celles-ci seront disponibles[20]. Avec égard, nous sommes d'avis que la Cour est passée à côté de l'opportunité de statuer sur l'obligation d'adopter une politique détaillée prévoyant certains éléments et abordant certains sujets

14 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3., par. 85 à 91 et 96. Ce constat ne fait pas l'unanimité : Jamie Grace, Machine Learning Technologies and Their Inherent Human Rights Issues in Criminal Justice Contexts, 2019, en ligne : https://ssrn.com/abstract=3487454 ou http://dx.doi.org/10.2139/ssrn.3487454.

15 *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, S.T.E. no 5 (entrée en vigueur le 3 septembre 1953), art. 8.

16 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3., par. 98 ; Voir aussi : Bank Mellat v Her Majesty's Treasury (No 2) [2014] AC 700, par. 20.

17 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, préc., note 3, par. 99 et s.

18 *Ibid*., par. 137. À ce sujet, voir Information Commissioner, *The use of live facial recognition technology by law enforcement in public places, Information Commissioner's Office*, 2019/01, p. 14 à 16, en ligne : https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

19 *Ibid*.

20 *Ibid*., par. 139 à 141.

nécessaires à la satisfaction de l'objet du DPA 2018. À défaut, nous devons, nous aussi, nous en remettre aux futurs directives et communiqués du Commissaire à l'information afin de mieux saisir la portée de ces politiques.

[7] Dans un second temps, la Cour rappelle qu'en plus de l'adoption de politiques, une autorité policière souhaitant traiter des données du public doit également produire une évaluation de l'impact qu'aura le traitement qu'elle envisage faire sur les données personnelles en question et leur protection, le tout en vertu de l'article 64 DPA 2018[21]. Elle estime que la SWP satisfait ici à cette exigence[22].

[8] À la lumière de ce qui précède, nous retenons que le législateur anglais souhaite responsabiliser les contrôleurs de données face aux enjeux liés à la protection des renseignements personnels. Pour ce faire, il leur impose des obligations en amont du traitement de ces renseignements par l'adoption de politiques internes et en procédant à l'évaluation des risques potentiels. De plus, le traitement des données par un contrôleur est encadré par des principes généraux prévus dans la loi[23] en plus de règles strictes applicables à certaines situations particulières[24].

II. CANADA - QUÉBEC

[9] Dans un esprit comparatif, nous étudierons le recours éventuel à une technologie comparable par les autorités policières canadiennes sous les mêmes angles que ceux précédemment abordés. Nous verrons donc d'abord (II.1.) le droit à la vie privée garanti par la *Charte canadienne des droits et libertés*[25] (ci-après « *Charte canadienne* ») avant de nous intéresser plus particulièrement au (II.2.) régime mis en place par le législateur et applicable au traitement de données biométriques.

---

21 *Data Protection Act 2018*, 2018 c. 12, art. 64. L'évaluation imposée par cet article fait également l'objet d'une suggestion du Commissaire aux caméras de surveillance : Surveillance Camera Commissioner, *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*, 2019, p. 3 et 4, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf. Voir aussi Information Commissioner, *The use of live facial recognition technology by law enforcement in public places, Information Commissioner's Office*, 2019/01, p. 13 et 14, en ligne : https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

22 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, préc., note 3, par. 148.

23 *Data Protection Act 2018*, 2018 c. 12, art. 35 à 40.

24 *Ibid*., art. 35(3) et (5).

25 *Charte canadienne des droits et libertés*, partie I de la Loi constitutionnelle de 1982 [annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R-U)].

II.1. *CHARTE CANADIENNE DES DROITS ET LIBERTÉS*

[10] Le droit à la vie privée est consacré par l'article 8 de la *Charte canadienne* qui garantit la protection contre les fouilles, les perquisitions et les saisies abusives[26]. Le recours à la technologie de reconnaissance faciale par les forces policières étant une technique relativement nouvelle, peu de décisions se sont penchées sur la question[27]. Il faut donc selon nous s'en remettre à la jurisprudence concernant le traitement des données biométriques[28] ou, plus largement, la protection de la vie privée informationnelle[29].

[11] Avant toute chose, il faut nous demander si la donnée biométrique constitue un renseignement personnel susceptible de bénéficier de la protection de l'article 8 de la *Charte canadienne*. À ce sujet, que l'on se fie à la définition de la Cour suprême[30], qui fait référence aux caractère intime des détails que révèle un renseignement personnel, ou à celle du législateur[31], qui se fonde plutôt sur le fait qu'un renseignement est personnel dès lors qu'il permet l'identification de l'individu concerné, force est de constater qu'une donnée biométrique doit être considérée comme étant un renseignement personnel. Elle est ainsi susceptible de bénéficier de la protection de l'article 8 de la *Charte canadienne*.

[12] Il importe de préciser que ces données ne sont que susceptibles de bénéficier de cette protection étant donné le champ d'application de l'article 8 qui se limite aux cas où il existe une attente raisonnable de la

---

26 *R.* c. *Mills*, 2019 CSC 22, par. 12; *R.* c. *Reeves*, 2018 CSC 56, par. 2 et 11; *R.* c. *Jones*, 2017 CSC 60, par. 38 ; *R.* c. *Spencer*, 2014 CSC 43, par. 15; *R.* c. *Dyment*, [1988] 2 R.C.S. 417 ; *Hunter* c. *Southam*, [1984] 2 R.C.S. 145. Voir également en doctrine : Karim Benyekhlef et Pierre-Luc Déziel, *Le droit à la vie privée en droit québécois et canadien*, Montréal, Éditions Yvon Blais, 2018, p. 80 et suiv.; Gerald Chan et Nader R. Hasan, *Digital Privacy Criminal, Civil and Regulatory Litigation*, Toronto, LexisNexis Canada, 2018, p. 3 et Julie M. Gauthier, *Le droit de la biométrie au Québec : sécurité et vie privée*, Montréal, Éditions Yvon Blais, 2015, p. 35.

27 *R.* v. *Voong*, 2018 ONCJ 352, par. 8 et suiv. L'argument du caractère personnel des données biométriques extraites par la technologie à reconnaissance faciale ne fait pas l'objet d'une analyse par la Cour.

28 Dans son mémoire, Julie M. Gauthier suggère que la technologie de reconnaissance faciale traite des données biométriques. Elle discute également des données biométriques de façon plus large comme étant des renseignements personnels. Suivant ce raisonnement ces données tomberaient sous l'égide du droit à la vie privée : Julie M. Gauthier, *Le droit de la biométrie au Québec : sécurité et vie privée*, préc., note 26, aux pages 22, 23 et 27 à 33.

29 La Cour suprême identifie trois sphères dans lesquelles un individu peut bénéficier d'un droit à la vie privée, soit les sphères territoriale, personnelle et informationnelle : *R.* c. *Dyment*, [1988] 2 RCS 417, par. 19. Voir également : Karim Benyekhlef et Pierre-Luc Déziel, *Le droit à la vie privée en droit québécois et canadien*, préc., note 26, aux pages 85 et 86 et Julie M. Gauthier, préc., note 26, 2015, p. 35.

30 *R.* c. *Plant*, [1993] 3 R.C.S. 281, p. 293. L'application de cette notion a par la suite été élargie par la Cour suprême dans *R.* c. *Spencer*, [2014] 2 R.C.S. 212. Voir également : Karim Benyekhlef et Pierre-Luc Déziel, préc., note 26, aux pages 89 et 91.

31 Loi sur la protection des renseignements personnels (L.R.C. (1985), ch. P-21), art. 3 et Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c. A-2.1, art. 54.

part d'un individu à la protection de ces renseignements[32]. Cette attente raisonnable s'évalue, selon la jurisprudence, sous le couvert de nombreux critères que l'on peut regrouper en quatre catégories, soit « (1) l'objet de la fouille ou de la perquisition contestée; (2) le droit du demandeur à l'égard de l'objet; (3) l'attente subjective du demandeur en matière de respect de sa vie privée relativement à l'objet; et (4) la question de savoir si cette attente subjective en matière de respect de la vie privée était objectivement raisonnable, eu égard à l'ensemble des circonstances »[33].

[13] En l'espèce, comme mentionné précédemment, le traitement des données biométriques affecte la sphère informationnelle de la vie privée. De plus, ces données étant des renseignements personnels, l'individu visé bénéficie d'un droit à l'égard de celles-ci. De même, considérant la nature de ces données, il est raisonnable de croire qu'un individu visé aurait une attente subjective à l'égard de sa vie privée. Finalement, nous sommes d'avis que les données biométriques du visage permettant l'identification en temps réel d'une personne relèvent de son cœur biographique et, pour cette raison, justifient une attente objectivement raisonnable en matière de respect à la vie privée[34]. Il faut donc conclure que le traitement de ce type de données constitue une fouille et une saisie au sens de l'article 8 de la *Charte canadienne*. Reste à savoir si cette fouille et saisie est abusive.

[14] Le caractère abusif d'une fouille ou d'une saisie se présumera si celles-ci ne sont pas expressément autorisées[35]. Il faudra, pour renverser cette présomption, établir que la fouille, la saisie ou la perquisition est permise par une règle de droit, que celle-ci est raisonnable et que la fouille, la perquisition ou la saisie s'est réalisée raisonnablement[36]. En l'espèce, c'est la common law qui, selon nous, constituerait la règle de droit permettant la fouille ou la saisie, puisqu'elle confère, aux policiers canadiens, des pouvoirs similaires à ceux des policiers anglais[37]. Par ailleurs, le caractère raisonnable de la règle de droit est établi dans la

32 Karim Benyekhlef et Pierre-Luc Déziel, préc., note 26, aux pages 87 et 89. Voir également : *R.* c. *Spencer*, [2014] 2 R.C.S. 212, par. 16 et Gerald Chan et Nader R. Hasan, *Digital Privacy Criminal, Civil and Regulatory Litigation*, Toronto, LexisNexis Canada, 2018, p. 3.

33 *R.* c. *Spencer*, [2014] 2 R.C.S. 212, par. 18. Voir également : *R.* c. *Mills*, 2019 CSC 22, par. 13; *R.* c. *Reeves*, 2018 CSC 56, par. 28; *R.* c. *Jones*, 2017 CSC 60, par. 13; Karim Benyekhlef et Pierre-Luc Déziel, préc., note 26, aux pages 93 et 94 ; Gerald Chan et Nader R. Hasan, *Digital Privacy Criminal, Civil and Regulatory Litigation*, Toronto, LexisNexis Canada, 2018, p. 5.

34 *R.* c. *Cole*, [2012] 3 R.C.S. 34. Cité par Karim Benyekhlef et Pierre-Luc Déziel, préc., note 26, 94. Voir également les facteurs énumérés par la Cour suprême dans l'évaluation de la quatrième catégorie de facteurs dans *R.* c. *Tessling*, [2004] 3 R.C.S. 432, par. 32. Cité par I*bid*., p. 97.

35 *Hunter* c. *Southam*, [1984] 2 R.C.S. 145, p. 160 et 161. Cité par *Ibid*., p. 102. L'autorisation pourra notamment prendre la forme d'un mandat.

36 *Ibid*., p. 103. Voir aussi *R.* c. *Collins*, [1987] 1 R.C.S. 265.

37 Martin Vauclair et Tristan Desjardins, *Traité général de preuve et de procédure pénales*, 26e éd., Montréal, Éditions Yvon Blais, 2019, par. 212 et suiv., p. 95 et s.

mesure où il existe « un juste équilibre entre l'atteinte à la vie privée qu'elle suppose et l'importance ou la valeur de l'objectif sociétal qu'elle poursuit »[38]. Finalement, l'analyse du caractère raisonnable de l'exécution de la fouille, la perquisition ou la saisie se fera au cas par cas considérant la nature hautement factuelle de ce dernier critère.

[15] En ce qui concerne le recours aux technologies de reconnaissance faciale par les corps policiers, nous avons de la difficulté à croire qu'une règle de droit permettant une telle mesure soit considérée comme raisonnable. En effet, le traitement aléatoire des données biométriques du visage de tous les passants d'un lieu public sans motif particulier relatif à chacun d'entre eux semble faire fi de l'importance de la balance entre l'objectif poursuivi et le droit à la vie privée des individus concernés[39]. Malgré notre doute, et suivant les similitudes entre les cadres d'analyse anglais et canadiens, il est tout à fait possible qu'un tribunal canadien, aux prises avec la même question, en arrive à une conclusion similaire[40].

[16] Ceci étant, la jurisprudence et la doctrine insistent, tout comme l'a fait la jurisprudence anglaise[41], sur la nécessité d'un encadrement des mesures de surveillance technologiques auxquelles ont recours les forces policières[42]. Ainsi, l'utilisation de la technologie de reconnaissance faciale se doit d'être balisée si elle doit passer le test de la jurisprudence.

II.2. LOIS PARTICULIÈRES

[17] Il est désormais acquis que les données biométriques traitées par les technologies de reconnaissance faciale sont des renseignements personnels au sens des lois québécoise et canadienne[43]. Ainsi, notre étude de ces lois se fera sous l'angle des dispositions prévoyant des obligations similaires à celles prévues au DPA 2018 vues précédemment.

38 K. Benyekhlef et P.-L. Déziel, préc., note 26, p. 109.

39 Ce n'est d'ailleurs pas pour rien que des dispositions spécifiques visant l'octroi d'un mandat général permettant d'avoir recours à des dispositifs de surveillance électronique existent au *Code criminel* tels que l'art. 487.01(4) et (5). Même dans le cadre de l'émission de ce type de mandat, l'article 487.01(1) C.cr. prévoit notamment que les forces policières doivent détenir des motifs suffisants justifiant l'émission du mandat.

40 Bien que, par le passé, la Cour suprême ait mis en garde les autorités contre l'utilisation de technologies de surveillance vidéo des citoyens : *R.* c. *Wong*, [1990] 3 R.C.S. 36. Voir l'analyse qu'en fait la doctrine dans K. Benyekhlef et P.-L. Déziel, préc., note 26, p. 239.

41 *Supra*, note 13. Voir également *S v. United Kingdom*, (2009) 48 EHRR 50, par. 99 et 103.

42 K. Benyekhlef et P.-L. Déziel, préc., note 26, aux pages 239 à 243. Voir également : *R.* c. *Wong*, [1990] 3 R.C.S. 36 et *R.* c. *Duarte*, [1990] 1 R.C.S. 30.

43 Soit respectivement la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1 et la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21.

[18] La loi québécoise prévoit que la collecte des données par un organisme public doit être « nécessaire à l'exercice des attributions de cet organisme ou à la mise en oeuvre d'un programme dont il a la gestion »[44]. N'étant pas sans rappeler les dispositions anglaises vues précédemment[45], cet article a été interprété comme établissant une obligation de stricte nécessité[46]. Ce critère ne semble pas trouver son pendant du côté fédéral, bien que le législateur ait tout de même choisi de limiter la collecte des renseignements personnels à « ceux qui ont un lien direct avec ses programmes ou ses activités »[47]. En dépit de cette différence et à défaut d'une définition de l'expression « lien direct »[48], nous sommes d'avis que les renseignements personnels collectés par une institution fédérale doivent également respecter un critère de nécessité[49]. Toutefois, bien qu'exigé par la loi anglaise, le critère d'intérêt public que doit revêtir le traitement des données semble absent des lois québécoise et canadienne les rendant plus souples à cet égard, distinction qu'il importe de souligner.

[19] De plus, notons l'absence non seulement de l'obligation d'adopter des politiques relatives à la protection des renseignements personnels[50], mais également de l'obligation de procéder à une évaluation du risque inhérent à la collecte et au traitement de ces renseignements. L'absence de ces obligations nous paraît regrettable, puisqu'elles permettraient de mieux conscientiser les organismes visés et d'assurer une réflexion de leur part en amont de la collecte et de l'utilisation des données recueillies. Cette

---

44 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, art. 64 al. 2. La loi québécoise est plus stricte, à cet égard, que le DPA 2018 en ce qu'elle ne fait pas de distinction entre données sensibles ou non, tout renseignement personnel devant satisfaire au critère de nécessité.

45 Les dispositions québécoises et canadiennes semblent regrouper, en une seule disposition pour chaque loi, les obligations imposées par les paragraphes 35(1)a) et 35(1)b) DPA 2018.

46 *Syndicat des employées et employés professionnels et de bureau, section locale 57* et *Caisse populaire St-Stanislas de Montréal*, 1998 QCSAT 2765 et *M.L.* c. *Gatineau (Ville de)*, 2010 QCCAI 68. Cité par K. Benyekhlef et P.-L. Déziel, préc., note 26, p. 318. Voir également : Julie M. Gauthier, préc., note 26, p. 70 et suiv.

47 *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21, art. 4.

48 K. Benyekhlef et P.-L. Déziel, préc., note 26, p. 273.

49 *Ibid*., p. 319 ; Voir également : Commissariat à la protection de la vie privée du Canada, Reconnaissance faciale automatisée dans les secteurs public et privé, Gatineau, 2013, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303/, p. 8 et 9. Une telle interprétation est, selon nous, conforme à l'esprit de la loi qui vise la protection des renseignements personnels de la population.

50 Quoique le Commissariat à la protection de la vie privée du Canada recommande l'adoption de politiques : Commissariat à la protection de la vie privée du Canada, Reconnaissance faciale automatisée dans les secteurs public et privé, Gatineau, 2013, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303/, p. 9.

absence milite selon nous en faveur d'un moratoire[51] sur le recours à la technologie de reconnaissance faciale par les autorités policières dans l'attente d'un encadrement législatif mieux adapté à cette nouvelle réalité. À tout événement, ceci ne signifie pas que les lois québécoise et canadienne fournissent aux citoyens une protection plus faible, puisqu'à titre d'exemple, la loi québécoise édicte tout de même une obligation de « prendre les mesures de sécurité propres à assurer la protection des renseignements personnels [...] »[52].

[20] Notons en dernier lieu que le législateur québécois a prévu des dispositions au sujet de l'utilisation de données biométriques[53]. L'article 44 LCCJTI prévoit à cet effet que « [n]ul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques »[54]. Nous n'avons retracé aucune décision ayant interprété cette disposition[55]. Cependant, il semblerait qu'à sa lecture même, l'article 44 LCCJTI constitue un obstacle imposant au recours à la technologie qui nous occupe[56].

CONCLUSION

[21] À la lumière de la présente étude, nous constatons que le droit à la vie privée en tant que droit fondamental est protégé de manière similaire au Royaume-Uni et au Canada. Toutefois, ceci ne signifie pas pour autant que les cadres d'analyse développés par les tribunaux anglais et canadiens seront appliqués de la même manière. Leur application peut être influencée par bien des facteurs, que ce soit les valeurs de ces sociétés qui, à certains égards, peuvent diverger, ou encore le corpus législatif concernant la protection des renseignements personnels qui peut orienter l'analyse des décideurs dans un sens comme dans l'autre. À

51 Cette approche est adoptée ailleurs dans le monde, notamment en Australie ainsi que dans certaines villes américaines telles que San Francisco et Seattle : Kate Crawford, Roel Dobbe, Theodora Dryer, Genevieve Fried, Ben Green, Elizabeth Kaziunas, Amba Kak, Varoon Mathur, Erin McElroy, Andrea Nill Sánchez, Deborah Raji, Joy Lisi Rankin, Rashida Richardson, Jason Schultz, Sarah Myers West, and Meredith Whittaker. *AI Now 2019 Report*, New York, AI Now Institute, 2019, p. 32, en ligne : https://ainowinstitute.org/AI_Now_2019_Report.html.

52 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, art. 63.1.

53 *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1, art. 44 et 45 (ci-après « LCCJTI »).

54 *Ibid*., art. 44.

55 À l'exception d'une décision rendue par la Commission d'accès à l'information par laquelle elle rejette l'argument suivant lequel une empreinte vocale constitue une donnée biométrique : *C.R.* c. *Loto-Québec*, 2012 QCCAI 300.

56 Sous réserve d'une intervention législative similaire à celle se trouvant à la *Loi sur le système correctionnel du Québec*, RLRQ c S-40.1, qui à son article 18.0.1 écarte expressément l'application de l'article 44 LCCJTI.

cet effet, bien que certaines des obligations imposées au contrôleur de données par la loi anglaise le sont également aux organismes publics par les lois fédérale et québécoise, ces règles présentent certaines distinctions.

[22] Pour finir, ce texte ne se veut pas un plaidoyer à l'encontre de l'instauration, au Canada, d'une technologie comme celle utilisée par le service de police de South Wales. Les autorités policières devraient bénéficier des innovations technologiques afin de demeurer à jour dans la poursuite de leur mission. Cela dit, il faut selon nous éviter de verser systématiquement dans le « technosolutionnsime ». En ce sens, on ne peut tolérer qu'il ne soit porté atteinte de façon déraisonnable et arbitraire aux droits fondamentaux des citoyens au nom du combat contre la criminalité.

LA VIE PRIVÉE DES GROUPES : NOUVEAU CADRE THÉORIQUE POUR UNE PROTECTION CONTRE LE PROFILAGE ALGORITHMIQUE

Simon DU PERRON[1]

1 L'auteur est candidat à la Maîtrise en droit des technologies de l'information à la Faculté de droit de l'Université de Montréal et assistant de recherche au Laboratoire de cyberjus-tice.

Résumé

On observe un fossé de plus en plus grand entre d'une part, les modèles d'affaires qui misent sur l'exploitation des mégadonnées afin de catégoriser les individus en fonction de leur correspondance à différents profils algorithmiques, et de l'autre, un paradigme juridique axé sur l'individu. La vie privée des groupes est un nouveau cadre théorique multidisciplinaire qui s'inscrit en réponse à ce décalage. Le « groupe algorithmique » constitue un nouveau phénomène épistémologique généré par les nombreuses opérations de classification et d'agrégation à l'œuvre au sein des mégadonnées. Ces regroupements s'effectuent principalement à partir de données anonymisées ou dépersonnalisées de sorte que les individus sont rarement conscients de leur appartenance à un groupe algorithmique. Considérant les préjudices que le traitement algorithmique des données peut causer aux membres du groupe, mais également pour le groupe *en tant que groupe*, il importe d'élargir la portée du droit à la vie privée et de reconnaître l'intérêt collectif d'être protégé contre le profilage algorithmique. Les travaux d'auteurs qui abordent le droit à la vie privée dans une perspective antidiscriminatoire, ainsi qu'une interprétation novatrice de l'article 8 de la *Convention européenne des droits de l'Homme,* constituent un bon point de départ pour articuler une théorie permettant de reconnaitre un droit collectif à la vie privée des groupes.

INTRODUCTION

> *Sometimes the only way to protect the individual is to protect the group to which the individual belongs. Preferably before any disaster happens.*
>
> - Luciano Floridi, "Open Data, Data Protection, and Group Privacy"[2]

[1] Tout autour de nous, les technologies numériques scrutent et enregistrent des facettes de nos vies : les endroits que nous visitons, les sites web que nous consultons, les téléséries que nous regardons, etc. L'exploitation de ces mégadonnées (*big data*) caractérise le modèle d'affaires des géants du numérique[3], décrit par Shoshana Zuboff comme un capitalisme de surveillance qui cherche à traduire toute expérience humaine en information pouvant servir de valeur marchande pour les entreprises qui la détiennent et savent l'exploiter[4]. Dans ce contexte marqué par des techniques d'analyse des données conçues pour opérer à la plus large échelle possible[5], force est d'admettre que les données *personnelles* n'occupent en réalité qu'une place anecdotique[6].

[2] Or, le droit à la vie privée demeure strictement axé sur l'individu et l'ensemble des outils élaborés pour protéger la vie privée lui sont destinés[7]. On observe un fossé de plus en plus grand entre d'une part, l'exploitation des mégadonnées afin de catégoriser les individus en fonction de leur correspondance à différents profils algorithmiques[8], et de l'autre, un paradigme juridique axé sur l'individualité. C'est en réponse à ce décalage que s'inscrit la vie privée des groupes (*group privacy*) : un nouveau cadre théorique multidisciplinaire développé dans l'ouvrage *Group Privacy New Challenges of Data Technologies*[9].

2 Luciano Floridi, « Open Data, Data Protection, and Group Privacy » (2014) 27-1 *Philosophy & Technology*

3 Groupe d'examen du cadre législatif en matière de radiodiffusion et de télécommunications, *L'avenir des communications au Canada : le temps d'agir*, Ottawa, 2020, p. 210.

4 Shoshana Zuboff, *The Age of Surveillance Capitalism,* 1re éd., New York, PublicAffairs, 2019.

5 "In many areas, however, a shift is taking place from collecting some data to gathering as much as possible, and, if feasible, getting everything : *N =all*." (Viktor Mayer-Schönberger et Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Boston, Houghton Mifflin Harcourt Publishing Company, 2013, p. 26.)

6 Antoinette Rouvroy, « Des données sans personne: le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », (2014) *Étude annuelle 2014 - Le numérique et les droits fondamentaux*, p. 8.

7 Karim Benyekhlef et Pierre-Luc Déziel, Le droit à la vie privée en droit québécois et canadien, Montréal, Éditions Yvon Blais, 2018, p. 51.

8 Moritz Büchi et al., « The chilling effects of algorithmic profiling: Mapping the issues », (2020) 36 *Computer Law & Security Review* 1.

9 Linnet Taylor, Luciano Floridi et Bart van der Sloot (dir.), *Group Privacy: New Challenges of Data Technologies,* Dordrecht, Springer, 2017 (ci-après « *Group Privacy* »).

I – LA VIE PRIVÉE DES GROUPES : QUAND PROTÉGER L'INDIVIDU NE SUFFIT PLUS

I.1. QU'EST-CE QU'UN « GROUPE » ?

[3] Le mot « groupe » réfère généralement à un ensemble de personnes formant un tout et défini par une caractéristique commune[10]. Cependant, pour bien saisir la notion de vie privée des groupes, il importe de distinguer le groupe « actif » du groupe « passif »[11].

[4] Le groupe actif est composé d'individus qui sont conscients de leur appartenance au groupe et qui s'y identifient. Ces membres partagent certaines caractéristiques, ainsi qu'un certain historique d'interactions et/ou d'objectifs en commun. Le groupe actif requiert un certain niveau de conscience *collective*, ce qui ne signifie pas pour autant que tous ses membres se connaissent. Les étudiants d'une même Faculté, les membres d'un club de l'âge d'or, la communauté chinoise de l'île de Montréal, sont autant d'exemples de groupes actifs. Inversement, les membres d'un groupe passif ne sont pas nécessairement conscients de leur appartenance au groupe, car l'existence du groupe dépend de l'externe ; c'est le regard des autres qui lui donne naissance. Bien qu'ils puissent partager certaines caractéristiques en commun (ex. le fait de posséder une voiture rouge), les membres d'un groupe passif n'ont aucune intention d'exister en tant que collectivité. Les « personnes âgées » ou les « personnes vulnérables » par exemple, comptent des individus pouvant ne pas s'identifier au groupe, mais néanmoins en faire partie aux yeux du public.

[5] Parmi les groupes passifs, le groupe qui retiendra davantage notre attention en lien avec la théorie de la vie privée des groupes est le « groupe algorithmique » que Linnet Taylor décrit comme « un nouveau phénomène épistémologique généré par l'analyse des mégadonnées »[12]. Le groupe algorithmique est le fruit des nombreuses classifications opérées par les différents algorithmes à l'œuvre au sein des mégadonnées[13]. Le groupe désigne ici l'ensemble des individus qui

10 Larousse, « Définitions : groupe - Dictionnaire de français Larousse », en ligne : <https://www.larousse.fr/dictionnaires/francais/groupe/38423>.

11 Cette typologie nous est inspirée par les textes suivants : Lanah Kammourieh et al., « Group Privacy in the Age of Big Data », dans *Group Privacy*, préc. note 9, p. 38 à 40 et Michele Loi et Markus Christen, « Two Concepts of Group Privacy », (2019) *Philosophy & Technology* 18, p. 2.

12 Linnet Taylor, « Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World » dans *Group Privacy*, préc. note 8, p. 14.

13 À ce sujet, voir l'article de Nancy J. King et Jay Forder, « Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data », (2016) 32-5 *Computer Law & Security Review* 696–714.

correspondent à certains profils déterminés par l'analyse des données (ex. les consommateurs ayant un intérêt pour le jardinage, les mères monoparentales vivant en secteur urbain, les parents en attente de leur premier enfant, etc.[14]). Notons que les regroupements algorithmiques s'effectuent principalement à partir de données anonymisées ou dépersonnalisées de sorte que les individus sont rarement conscients de leur appartenance à un groupe algorithmique ni de ses conséquences.

[6] Précisons que la classification entre groupe actif et groupe passif n'est pas immuable. Ainsi, l'algorithme de Netflix crée un groupe passif (et algorithmique) lorsqu'il regroupe certains utilisateurs sous la catégorie « Amateurs de films d'horreur ». Si Netflix mettait en place un forum destiné aux fans, le groupe deviendrait de plus en plus « actif » au fur et à mesure que les utilisateurs interagissent, s'organisent et partagent un sens du « nous ».

I.2 – EST-CE QUE LES « GROUPES » PEUVENT ÊTRE TITULAIRES DE DROITS?

[7] Reconnaitre des droits aux groupes implique de leur conférer la personnalité juridique. À ce sujet, Ugo Pagallo rappelle que le droit permet l'octroi de droits à des entités non humaines dont la configuration interne est appelée à changer[15]. On pense immédiatement aux personnes morales[16], mais l'histoire enseigne que des temples ont été considérés comme des sujets de droit dans la Rome antique[17]. Récemment, la personnalité juridique a été reconnue à l'égard d'un fleuve[18], de la forêt amazonienne[19] et l'on s'interroge à savoir si l'on devrait faire de même avec les agents autonomes[20].

---

14 Il s'agit de trois catégories utilisées par les courtiers en données américains pour définir des segments spécifiques de la population sur la base de l'analyse des mégadonnées (Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, 2014, en ligne : <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>).

15 Ugo Pagallo, « The Group, the Private, and the Individual: A New Level of Data Protection? » dans *Group privacy,* préc. note 9, p. 161.

16 *Code civil du Québec,* RLRQ, c. C-12, art. 298.

17 John Chipman Gray, *The Nature and Sources of the Law*, New Orleans, Quid Pro, 2012, p. 45.

18 En 2016, la Cour constitutionnelle de Colombie a reconnu la personnalité juridique au fleuve Atrato (Cour constitutionnelle colombienne, [2016] T-622) .

19 En 2018, la Cour suprême de Colombie a reconnu le statut de sujet de droit à la forêt amazonienne (El Tiempo Editorial, « Declaran la Amazonia sujeto de derechos para atacar la deforestación », *El Tiempo*, 5 avril 2018, en ligne : <https://www.eltiempo.com/justicia/cortes/amazonia-fue-declarada-sujeto-de-derechos-por-la-corte-suprema-201682>).

20 Les députés du Parlement européen ont adopté le 16 février 2017 un rapport sur l'évolution des règles de droit civil concernant la robotique qui suggère d'attribuer une « personnalité juridique spécifique aux robots » (*Proposition de résolution du Parlement européen contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique*, 2015/2103 (INL), en ligne : <http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_FR.html>, par. 59).

[8] Le droit canadien reconnait déjà des droits qui protègent les individus contre la discrimination en raison de leur appartenance à certains groupes (sexuels, religieux, ethniques, etc.)[21]. Enchâssés dans les Chartes des droits, ces « droits des minorités » sont considérés par la Cour suprême comme un des piliers de notre ordre constitutionnel[22]. Ces droits sont toutefois à distinguer des « droits collectifs » soit les droits qui appartiennent à un groupe *en tant que groupe*, et non à un groupe dans la mesure où celui-ci est constitué d'individus qui jouissent de ces droits. L'un des exemples de droit collectif au Canada est celui des droits ancestraux autochtones. Ces droits constitutionnels[23] sont détenus par les communautés autochtones elles-mêmes et ne peuvent, en principe, être exercés par les individus[24]. Le droit à l'autodétermination, qui appartient et est exercé par les peuples, est un autre exemple de droit collectif dévolu aux groupes *en tant que groupe*[25] .

I.3. QUEL TYPE DE DROIT À LA VIE PRIVÉE PEUT ÊTRE ATTRIBUÉ AUX « GROUPES » ?

[9] Afin d'éviter toute confusion, il importe de distinguer la vie privée des groupes *au sens faible* et la vie privée des groupes *au sens fort*[26]. La vie privée des groupes *au sens faible* réfère à la théorie de la vie privée relationnelle développée par Edward Bloustein dans les années 1970[27]. Cette forme de vie privée protège le désir et le besoin des individus de se rassembler, d'échanger de l'information, des émotions, de planifier et d'agir en commun dans l'atteinte de leurs objectifs[28]. Cette théorie conçoit la vie privée des groupes comme une extension de la vie privée individuelle[29]. Bloustein illustre sa théorie à l'aide de l'image du caucus dans le football américain[30]. Techniquement, seuls les joueurs à l'intérieur du caucus sont au courant de la stratégie. Bien que la stratégie discutée

---

21 *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982* [annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R.-U), art. 15 (1) ; *Charte des droits et libertés de la personne,* RLRQ, c. C-12, art. 10.

22 Renvoi relatif à la sécession du Québec, [1998] 2 RCS 217, par. 32.

23 Loi constitutionnelle de 1982, préc. note 20, art. 35.

24 Behn c. Moulton Contracting Ltd., 2013 CSC 26, par. 30.

25 François Roch, « Réflexions sur l'évolution de la positivité du droit des peuples à disposer d'eux-mêmes en dehors des situations de décolonisation, » (2002) 15-1 *Revue québécoise de droit international* 33, p. 58.

26 Cette distinction imprègne les travaux de L. Floridi, préc. note 2, p. 90-91 et M. Loi et M. Christen, préc. note 11, p. 2.

27 Edward J. Bloustein, *Individual and Group Privacy*, New York, Transaction Publishers, 1978

28 *Id.*, p. 125.

29 *Id.*

30 *Id.*, p. 126.

en caucus puisse être partagée aux téléspectateurs par les analystes du match, cela ne vient pas amoindrir la vie privée relationnelle dans la mesure où la partie adverse n'a pas accès à cette information et ne peut anticiper le prochain jeu. Le « droit au caucus »[31] protège donc l'échange d'information au sein d'un groupe du regard extérieur d'un autre groupe antagoniste. Michele Loi et Markus Christen ont surnommé ce type de vie privée la "*What happens in Vegas stays in Vegas privacy*"[32] en référence aux agissements de certains touristes à Las Vegas qui ne souhaitent pas que leurs péripéties soient révélées à leurs conjointes.

[10] La vie privée des groupes *au sens fort* est une différente théorie qui postule qu'un groupe possède un droit collectif à la vie privée qui n'est pas réductible à la vie privée de chaque individu qui le compose. Luciano Floridi donne l'exemple de proches rassemblés pour les funérailles du défunt[33]. Les endeuillés forment un groupe actif qui partage une expectative de vie privée liée au besoin d'intimité, au respect du deuil et aux coutumes culturelles ou religieuses. Dans un tel contexte, il serait erroné de prétendre que chaque membre du groupe, c'est-à-dire chaque proche du défunt, bénéficie d'un droit *individuel* à des funérailles *privées*, il semble plus approprié d'admettre que nous sommes en présence d'un droit à la vie privée revendiqué par le groupe *en tant que groupe.*

[11] Certains auteurs sont d'avis que seuls les groupes actifs peuvent réalistement bénéficier d'un droit à la vie privée *au sens fort*[34]. À notre avis, si la vie privée des groupes se limite à protéger les groupes actifs — qui bénéficient déjà de protections juridiques[35] — alors cette théorie est de peu d'utilité puisqu'elle n'offre aucune protection aux groupes algorithmiques[36]. Il importe donc de développer l'argument voulant que ces groupes puissent également bénéficier d'un droit à la vie privée *au sens fort.*

31 *Id.*, p. 123 .

32 M. Loi et M. Christen, préc. note 11, p. 2.

33 L. Floridi, préc. note 12, p. 91.

34 L. Kammourieh et al., préc. note 10, p. 55 ; M. Loi et M. Christen, préc. note 11, p. 15.

35 Supra, section 1.2.

36 Au sujet des enjeux légaux entourant le profilage algorithmique voir Wim Schreurs, Mireille Hildebrandt, Els Kindt et Michaël Vanfleteren, « Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector », dans Mireille Hildebrandt et Serge Gutwirth (dir.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Dordrecht, Springer Netherlands, 2008, p. 241–270.

II. PROTÉGER LES GROUPES ALGORITHMIQUES : REDÉFINIR LE DROIT À LA VIE PRIVÉE

II.1. *MANTELERO* : LA DIMENSION COLLECTIVE DE LA PROTECTION DES DONNÉES

[12] Le *Median Equivalency Score* est une notation algorithmique créée par la firme Experian[37] qui cherche à prédire le risque de crédit des habitants d'une même région géographique sur la base de l'analyse de centaines de variables[38]. Les individus sont catégorisés non pas en fonction de leurs caractéristiques personnelles, mais plutôt selon la cote agrégée de leur milieu socio-économique. Du point de vue individuel, une personne peut n'avoir aucune réticence à ce que ses données personnelles soient collectées afin d'établir sa capacité d'emprunt, mais au niveau collectif, il demeure dans l'intérêt général d'une communauté de ne pas voir ses membres être stigmatisés comme de potentiels mauvais débiteurs sur la base d'une évaluation algorithmique potentiellement biaisée et discriminatoire[39]. Ces processus décisionnels, qui ne considèrent plus les individus pour ce qu'ils sont, mais selon la catégorie dont ils font partie bon gré mal gré, ont un impact significatif sur la vie des individus lorsqu'ils interviennent dans le domaine du crédit, mais également dans celui du logement, de l'assurance, de l'emploi, de la justice criminelle ou de la santé[40].

[13] Dans cette optique, Alessandro Mantelero soutient que la vie privée des groupes a pour fonction de protéger les intérêts collectifs non agrégés d'un groupe donné[41]. Ainsi, l'auteur soutient qu'il existe des priorités collectives en matière de protection de la vie privée notamment en ce qui concerne les risques de discrimination découlant du profilage

37 Experian, *Summarized Credit Statistics*, 2014, en ligne :<https://www.experian.com/small_business/pdf/fall03_catalog_summarized_credit.pdf>.

38 Voir le rapport de Pam Dixon et Robert Gellman,« The scoring of America: How secret consumer scores threaten your privacy and your future », *World Privacy Forum*, 2014.

39 La chercheuse Nikita Aggarwal souligne qu'un algorithme d'apprentissage automatique, entraîné à partir de données provenant d'une population à prédominance blanche peut donner lieu à des biais discriminatoires décourageant les prêts à l'égard des populations non blanches (Nikita Aggarwal, « Law and Autonomous Systems Series: Algorithmic Credit Scoring and the Regulation of Consumer Credit Markets », *Oxford Law Faculty*, 2018, en ligne : <https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/law-and-autonomous-systems-series-algorithmic-credit-scoring-and>).

40 Au sujet des effets pervers des algorithmes de recommendation, voir Hannah Fry, Hello World: Being Human in the Age of Algorithms, 1st edition, New York, Norton & Compa¯ny, 2018 et Cathy O'Neil, Weapons of math destruction: how big data increases inequality and threatens democracy, 1st edition, New York, Crown, 2016.

41 Des intérêts collectifs peuvent être partagés par l'ensemble d'un groupe sans qu'il y ait de divergence de points de vue entre ses membres (intérêts agrégés) ou avec des opi¯nions contraires entre les membres (intérêts non agrégés) (Alessandro Mantelero, « Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collec¯tive Dimension of Data Protection » (2016) 32-2 *Computer Law & Security Review* 238–255, p. 249) .

algorithmique[42]. Par conséquent, il décrit la vie privée des groupes comme le droit, pour un groupe, d'être protégé face aux préjudices potentiels pouvant être causés par un traitement invasif et discriminatoire des données[43].

[14] Cette conception propose d'élargir la portée « classique » du droit à la vie privée afin de tenir compte du fait que celui-ci constitue un garde-fou visant la protection d'intérêts sociétaux plus larges[44]. Cette approche rejoint celle du Commissaire à la vie privée du Canada (ci-après « CPVP ») qui définit la vie privée comme une condition préalable à l'exercice d'autres droits fondamentaux, notamment la liberté, l'égalité et la démocratie[45]. Cette conception élargie du droit à la vie privée évoque l'interprétation qui a été faite de l'article 8 de la *Convention européenne des droits de l'Homme* (ci-après « CEDH »)[46] dans une récente affaire mettant en cause le droit des générations à un environnement sain.

II.2. L'AFFAIRE URGENDA : UNE INTERPRÉTATION NOVATRICE DU DROIT À LA VIE PRIVÉE

[15] Le 9 octobre 2018, la Cour d'appel de La Haye a fait les manchettes en confirmant une ordonnance qui oblige l'État néerlandais à réduire ses émissions de GES d'au moins 25 % d'ici 2020 à la suite d'une procédure intentée par l'ONG de défense de l'environnement Urgenda[47]. L'ONG alléguait qu'en raison de son laxisme en matière de réduction des GES, le gouvernement manquait aux devoirs de diligence exprimés par les articles 2 (droit à la vie) et 8 (droit au respect de la vie privée et familiale) de la CEDH.

[16] Il importe de souligner deux aspects importants de cette décision. Premièrement, la Cour a reconnu à Urgenda l'intérêt juridique d'agir pour le compte de la génération actuelle et des générations futures de Néerlandais qui devront faire face aux effets négatifs du changement

42 Soulignons que le CPVP considère que le profilage algorithmique des individus donnant lieu à un « traitement injuste, contraire à l'éthique ou discriminatoire » constitue une pratique inacceptable au sens du par. 5 (3) de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

43 A. Mantelero, préc. note 41, p. 246.

44 "Privacy has long been known to safeguard societal interests broader than privacy interest" (Ignacio N. Cofone, « Antidiscriminatory Privacy » (2019) 72 *SMU L. Rev*. 139, 147).

45 Commissariat à la protection de la vie privée du Canada, Rapport annuel au Parlement 2018-2019 concernant la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques, 2019, Gatineau, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201819/ar_201819/>.

46 Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, STCE n° 005.

47 ECLI:NL:GHDHA:2018:2610, 9 octobre 2018, en ligne : <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2018:2610>.

climatique au cours de leur vie si les émissions mondiales de GES ne sont pas réduites[48]. Deuxièmement, la Cour affirme que les changements climatiques constituent une réelle menace qui risque de profondément perturber notre mode de vie et que par conséquent, l'État néerlandais doit réduire ses émissions de GES afin de se conformer à son devoir de diligence envers le bien-être de ses citoyens présents et futurs[49].

[17] L'affaire *Urgenda* illustre comment un droit collectif à la vie privée peut concrètement bénéficier aux groupes. D'une part, la décision reconnait que des groupes dont la composition est instable (les générations présentes et futures) peuvent faire valoir leur intérêt collectif d'être protégé face à un préjudice potentiel et hypothétique (les conséquences du réchauffement climatique). De l'autre, elle propose une interprétation novatrice des droits fondamentaux qui tient compte de l'impact des changements climatiques sur le collectif et non seulement sur l'individu afin de déterminer si un droit reconnu par la CEDH est violé et si les États doivent prendre action.

[18] Cette approche permet d'entrevoir la possibilité pour les groupes algorithmiques de bénéficier également d'un droit à la vie privée *au sens fort*. En effet, la composition abstraite du groupe ne devrait pas l'empêcher de faire valoir son intérêt réel d'être protégé contre un préjudice potentiel. Ainsi, même si les groupes algorithmiques sont en constante mutation, les risques que leurs membres soient victimes d'atteintes à la vie privée et de discrimination à la suite du traitement algorithmique des données demeurent. Le devoir de diligence de l'État à l'égard de ses citoyens milite en faveur de l'adoption de mesures concrètes permettant de les protéger adéquatement. La prochaine section s'y attarde.

II.3. *COFONE* : LA VIE PRIVÉE ANTIDISCRIMINATOIRE

[19] La théorie de la vie privée antidiscriminatoire, développée par Ignacio Cofone, soutient que les règles en matière de protection de la vie privée peuvent servir à lutter efficacement contre la discrimination lorsqu'elles limitent l'accès aux renseignements que les lois en matière de non-discrimination considèrent être dommageables dans le cadre d'un

48 *Id.*, par. 34 à 38.

49 *Id.*, par. 73.

processus décisionnel[50]. Cofone part du constat que le droit à l'égalité intervient généralement *ex post*, c'est-à-dire après le préjudice causé par un acte discriminatoire. Or, comme il vaut mieux prévenir que guérir, l'auteur propose d'empêcher l'*acquisition*, par le décideur, de données sensibles[51] plutôt que de contrer l'*utilisation* discriminatoire de ces données[52].

[20] Des recherches ont toutefois mis en lumière que des décisions prises sur la base d'un traitement algorithmique peuvent être discriminatoires même lorsque toutes les données sensibles ont été retirées d'un ensemble de données[53]. En effet, les algorithmes d'apprentissage automatique peuvent tirer des inférences à partir de certaines données qui agissent comme intermédiaires (*proxy*) pour *révéler* une caractéristique protégée par les lois anti-discrimination. Ainsi, le code postal peut servir d'intermédiaire à une discrimination raciale[54] et les « J'aime » d'un profil Facebook peuvent révéler l'appartenance religieuse, les convictions politiques, l'orientation sexuelle d'une personne[55]. Par conséquent, Cofone souligne que la vie privée antidiscriminatoire passe également par le fait d'identifier et de bloquer les données servant d'intermédiaires[56].

[21] Or, il s'avère pratiquement impossible de bloquer toutes les données pouvant servir d'intermédiaires à des données sensibles, car les algorithmes d'apprentissage automatique seront toujours en mesure de tirer de *nouvelles* corrélations entre les données à leur disposition[57]. De plus, un renseignement qui agit comme intermédiaire pour une caractéristique protégée peut également être révélateur d'information utile et légitime. Par exemple, le niveau d'éducation peut être utilisé

50 I. Cofone, préc. note 45, et Ignacio N. Cofone, « Algorithmic Discrimination Is an Information Problem » (2019) 70-6 *Hastings LJ* 1389.

51 Nous utilisons le terme « donnée sensible » pour désigner tout renseignement portant sur l'un des motifs de non-discrimination prévu à l'article 10 de la *Charte des droits et libertés de la personne*, préc. note 21.

52 I. Cofone, préc. note 45, p. 140

53 Solon Barocas et Andrew D. Selbst, « *Big Data's Disparate Impact* », (2016) 104 *Calif. L. Rev.* 671, 675

54 Le "redlining" décrit le fait que les données géographiques sont profondément liées aux pratiques historiques d'exclusion et de discrimination raciales (Maya Sen et Omar Wasow. "Race as a Bundle of Sticks: Designs that Estimate Effects of Seemingly Immutable Characteristics." » (2016) 19 *Annual Review of Political Science* 499-522).

55 Il est possible d'inférer certains attributs personnels comme le genre, l'âge, la race, l'appartenance religieuse, les convictions politiques, la consommation de drogues et d'alcool, l'orientation sexuelle et le statut conjugal à partir de l'analyse de 58 000 « J'aime » sur Facebook (Michal Kosinski, David Stillwell et Thore Graepel, « Private traits and attributes are predictable from digital records of human behavior », (2013) 110-15 *Proceedings of the National Academy of Sciences* 5802.)

56 I. Cofone, préc. note 45, p. 172.

57 I. Cofone, préc. note 50, p. 1414.

comme intermédiaire pour prédire la race d'un individu, mais il peut aussi renseigner sur la performance au travail.

[22] Une autre approche consiste à confier la collecte et la gestion des données sensibles à un tiers de confiance[58]. Une organisation, qui souhaite développer un algorithme de recommandation, ne devrait avoir accès qu'aux données non sensibles nécessaires à l'accomplissement de sa tâche. En parallèle, une organisation tierce peut être chargée de collecter les données sensibles des individus dont les données (non sensibles) servent à l'entrainement de l'algorithme. Doté d'un accès à l'algorithme de l'organisation, le tiers de confiance peut ensuite recouper les résultats de celui-ci avec les données sensibles des individus afin de détecter la présence de biais discriminatoires. Un assureur pourrait par exemple développer un algorithme de recommandation pour l'aider à déterminer les primes de ses clients. Après s'être procuré une nouvelle police d'assurance sur le site web de l'assureur, le client serait alors dirigé vers le domaine d'un organisme de protection des consommateurs où il lui serait demandé de fournir certaines données sensibles afin de s'assurer que la prime générée par l'algorithme de l'assureur n'est pas discriminatoire.

CONCLUSION

[23] Les mégadonnées instaurent un nouveau « régime de vérité »[59] qui conduit les organisations à juger les individus non plus en fonction de leurs caractéristiques propres, mais selon leur appartenance à une segmentation artificielle de la société. Bien que la vie privée des groupes demeure une théorie inachevée, celle-ci nous invite à une réflexion cruciale à la lumière des récents développements technologiques. Le paradigme juridique axé sur les droits individuels apparait de plus en plus dépassé face aux conséquences du profilage algorithmique à l'échelle collective. Le temps semble être venu d'adopter une conception élargie du droit à la vie privée comme condition préalable à la protection et à l'exercice d'autres droits fondamentaux. Cette redéfinition permettrait de protéger les groupes *en tant que groupe* et de reconnaître leur intérêt collectif à ne pas être victime de discrimination basée sur des biais dans le traitement algorithmique des données.

58 Michael Veale and Reuben Binns, « Fairer Machine Learning in the Real World: Mitigating Discrimination Without Collecting Sensitive Data » (2017) 4 *Big Data & Society* 2.

59 A. Rouvroy, préc. note 6, page 9.

LES VULNÉRABILITÉS INHÉRENTES À L'APPROCHE INDIVIDUALISTE DES DONNÉES DE SANTÉ DANS L' « ÈRE BIG DATA »

Fabien LECHEVALIER[1]

1 L'auteur est candidat au doctorat (LL.D) en Droit (Université Laval) / (Ph. D) Droit privé & sciences criminelles (Université Paris-Saclay).

Résumé

Le phénomène Big Data multiplie les pratiques de recueil de données dans tous les secteurs, mais c'est certainement dans le domaine de la santé, que celles-ci suscitent le plus de questions sur leur statut et sur leur partage. En effet, ces données relevant à la fois du bien commun de l'humanité et du plus profond de l'intime, nous poussent à nous interroger sur le régime juridique le plus adapté à leur appliquer afin préserver au mieux la vie privée des personnes. En France, le régime érigé par le RGPD institue le principe d'une interdiction générale de la collecte desdites données qui peut être levée par le consentement éclairé et exprès du patient. Cependant l'efficacité de ce cadre juridique est déjà contestée en doctrine et en pratique.

Alors que la réalité du partage et de l'analyse des données a changé, les théories dominantes de la vie privée limitent leurs analyses à une approche individualiste. Partant, nos objectifs spécifiques sont de discuter du surinvestissement de la théorie de la vie privée dans les théories centrées sur l'individu et de la nécessité pour les décideurs politiques de s'engager pleinement dans le débat d'une gestion collective des droits qui y sont attachés afin d'apporter une solution idoine aux vulnérabilités crées par l'« ère big data ».

Introduction

[1] «Big Data» sont deux petits mots avec une énorme signification sociétale[2]. Ces mots signifient un phénomène complexe qui a fini par définir la deuxième décennie du XXIe siècle. Les mégadonnées sont de vastes quantités d'informations susceptibles d'être collectées, stockées et analysées à grande échelle. À l'aide de ces données, les entreprises et les chercheurs peuvent déployer des algorithmes complexes et des technologies d'intelligence artificielle pour révéler des modèles, des connexions, des comportements, des tendances, des identités et des connaissances pratiques autrement inconnus. Dans le domaine de la santé, le big data correspond à l'ensemble des données socio-démographiques et de santé, disponibles auprès de différentes sources qui les collectent pour diverses raisons[3]. Ces informations proviennent des pratiques gouvernementales et commerciales, des transactions des consommateurs et des applications numériques[4]. Les individus contribuent de manière invisible au Big Data chaque fois qu'ils vivent des modes de vie numérique ou participent à l'économie numérique, comme lorsqu'ils effectuent une transaction à l'aide d'une carte de crédit, se font soigner à l'hôpital, utilisent une application mobile reliée à une montre connectée, recherchent un sujet sur Google ou publient sur Facebook[5]. Le phénomène Big data multiplie ainsi les pratiques de recueil de données dans tous les secteurs, mais c'est certainement dans le domaine de la santé que celles-ci suscitent le plus de questions sur leur statut et sur leur partage. L'exploitation de ces données présente, en effet, de nombreux intérêts dans le cadre de la médecine personnalisée : identification de facteurs de risque de maladie, aide au diagnostic, au choix et au suivi de l'efficacité des traitements, pharmacovigilance, épidémiologie... Mais à côté de ces perspectives très bénéfiques pour la santé publique, il est à craindre que, malgré les contrôles prévus, les données soient exploitées dans un intérêt économique au détriment de l'intérêt public. L'exploitation de nos données de santé pose de nombreux défis techniques et humains, et pose autant de questions éthiques que juridiques. Ces données relevant à la fois du bien commun de l'humanité

2 David Bollier, *The promise and peril of Big Data,* The Aspen Institute, (2010), https://www.emc.com/collateral/ analyst-reports/ 10334-ar-promise-peril-of-big-data.pdf [https://perma.cc/CD6F-ACYZ].

3 Rodolphe Theibaut, Big data en santé: Des défis techniques, humains et éthiques à relever, INSERM, (1er Juin 2016).

4 Jacob Morgan, « A Simple Explanation of « The Internet of Things », *Forbes,* (13 Mai 2014, 12:05 am), http:// www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/ #4a6ee29b6828.

5 Anita Allen, « Protecting One's Own Privacy in a Big Data Economy », (2016), 130:71 *Harvard Law Review Forum* 71.

et du plus profond de l'intime, nous poussent à nous interroger sur le régime juridique le plus adapté à leur appliquer afin de préserver au mieux la vie privée des personnes.

[2] Alors que la réalité du partage et de l'analyse des données a changé, on pourrait craindre que les théories de la vie privée prennent du retard au regard des enjeux colossaux auxquels elles doivent faire face. Cela est d'autant plus le cas dans un contexte où les théoriciens de la vie privée diffèrent notoirement et largement sur la conception appropriée à leur donner[6]. Pourtant, on s'aperçoit que ces nombreuses doctrines ont tendance à partager une hypothèse théorique sous-jacente. Les théories dominantes de la vie privée analysent, en effet, cette notion à travers la lentille de l'individualisme[7]. Elles peuvent, donc, toucher à la dimension sociale de la vie privée[8], mais ne l'engagent pas fortement. Nos objectifs spécifiques sont de discuter du surinvestissement de la théorie de la vie privée dans les théories centrées sur l'individu (I) et de la nécessité pour les décideurs politiques de s'engager pleinement dans le débat d'une gestion collective des droits qui y sont attachés (II).

I. L'INFLUENCE HISTORIQUE DE L'INDIVIDUALISME DANS L'AVIS ET LE CHOIX MODERNE

[3] ILe droit traditionnel à la vie privée envisage le contrôle d'un individu sur les informations qui proviennent de ou portent sur cet individu. Les approches modernes de la vie privée ont développé et intensifié l'accent mis sur la notification individuelle, le choix et le contrôle des flux d'informations[8]. C'est ainsi qu'en France, le régime érigé par le Règlement Général sur la Protection des Données (RGPD) institue le principe d'une interdiction générale de la collecte des données[9] de santé qui ne peut être levée que par le consentement éclairé et exprès du patient[10] (ou bien pour des intérêts de santé publique[11]). La vie privée en tant que

6 Daniel J. Solove, « Conceptualizing Privacy », (2002), *90 California Law Review 1087*, pp. 1099–1123.

7 Robert C. Post, « The Social Foundations of Privacy: Community and Self in the Common Law Tort », (1989), *77 California Law Review 957*, pp. 958.

8 Paul M. Schwartz, « Privacy and Democracy in Cyberspace », (1999), *52 Vanderbilt Law Review. 1609*, pp. 1664.

9 Priscilla M. Regan, L Legislating privacy: technology, social values and public policy 228, University of North Carolina Press, Chapel Hill, (1995), pp. 231.

10 Article 9 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 96/46/CE (règlement général sur la protection des données).

11 Article 6 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 96/46/CE (règlement général sur la protection des données).

contrôle est devenue une théorie dominante de la vie privée informationnelle, en partie parce qu'elle promet aux individus (à tort ou à raison) la possibilité de divulguer et de contrôler la diffusion d'informations en ligne[12]. Bien que la vie privée en tant que contrôle ne soit pas une approche incurablement centrée sur l'individu, le développement ultérieur de la théorie et, surtout, son régime opératoire de notification démontrent la dominance de l'individualisme dans le droit moderne de la vie privée[13]. L'avis et le choix dépendent entièrement et explicitement des individus.

[4] Ces régimes tentent de faire en sorte que les individus sachent ce qui est fait de leurs informations et aient le choix quant à la manière dont ces données sont utilisées. Même les critiques de l'avis et du choix tendent à adhérer au paradigme individuel, plutôt qu'à remettre en cause l'hypothèse de base de l'individualité. La réponse traditionnelle aux défauts des régimes de notification et de choix a été que la notification et le choix ne sont pas encore suffisamment solides[14]. En effet, la critique courante est que les consommateurs ne sont pas suffisamment informés de ce qui est fait de leurs informations et qu'ils ne disposent pas de suffisamment de pouvoir discrétionnaire pour contrôler leur vie privée. Une solution idoine consiste donc à faire valoir que la qualité de l'avis et du choix doit s'améliorer. Partant, les conditions d'utilisation et les accords de licence d'utilisateur final sont de plus en plus explicites à la demande des tribunaux et des régulateurs. L'accent mis sur la compréhension et le contrôle est censé permettre au consommateur de mieux comprendre et contrôler les conséquences de la révélation d'informations qu'il propose sur lui-même[15]. À son tour, la tendance réglementaire en matière de protection de la vie privée dès la conception (« Privacy by design ») vise à inciter les entreprises à créer des outils permettant une compréhension et un contrôle individuel[16]. Notre critique ne consiste pas à soutenir que l'avis et le choix ne sont pas utiles, mais simplement que l'éducation et l'autonomisation axées sur l'individu semblent donner des rendements décroissants[17]. Les consommateurs ne

12 *Ibid*.

13 Mark MacCarthy, « New Directions in Privacy: Disclosure, Unfairness and Externalities », (2011), *6 I/S: Journal of Law & Policy for Information Society 425*, pp. 429.

14 Priscilla M. Regan, *op. cit*., note 9.

15 Jeff Sovern, « Opting in, Opting out, or No Options at All: The Fight for Control of Personal Information », (1999), *74 Washington Law Review 1033*, pp. 1094.

16 Kenneth A. Bamberger, Deirdre K. Mulligan, « Privacy on the Books and on the Ground », (2011), *63 Stanford Law Review 247*, pp. 301–02.

17 Ann Cavoukian, Information & Privacy Commissioner of Ontario Privacy by design: The 7 Fundamental principles S 1–2, (2011).

lisent pas assez rationnellement les politiques de confidentialité soigneusement formulées[18]. Dans une étude menée par la Commission européenne, en 2015, seulement 7% des internautes français disaient lire *toujours ou fréquemment* les conditions d'utilisation (comprenant les politiques de confidentialité)[19]. Avec l'arrivée du Big data et du deep learning, la situation s'est encore aggravée puisque tout internaute désirant bénéficier d'un service personnalisé n'a plus la possibilité à l'heure actuelle de s'opposer à la collecte et au traitement de ses données personnelles en raison des configurations techniques des algorithmes. Quand bien même ils les liraient, les audits produits par les entreprises en réponse aux incitations à la protection de la vie privée dès la conception sont souvent mis de côté en raison des coûts, du temps que cela nécessite ou de la complexité de la tâche[20]. Des théoriciens ont toutefois proposé une approche plus relationnelle du consentement dans laquelle la collecte des données serait soumise à un principe de réciprocité qui inviterait les collecteurs à mettre en place des moyens de contrôle intelligents tels que des instruments permettant un paramètrage personnalisé de la confidentialité et un retour intelligible des données sous formes d'alertes, des recommandations ou encore des tableaux de bord de suivi. Ce principe de réciprocité astreint les collecteurs à une obligation de rendre compte à la fois de ce qu'il font pour respecter la vie privée mais aussi des effets sociaux qu'induisent l'usage agrégé de ces données. La réciprocité est ce système de paiement symbolique qui maintient la confiance, tourné vers l'intérêt de l'autre. La question est désormais de savoir quels types de dispositifs permettent de l'exprimer.

[5] Même dans l'hypothèse où l'avis et le choix individualisés produiraient les résultats escomptés – et ce n'est actuellement pas le cas – un problème subsisterait. L'approche individuelle de la vie privée suppose à tort que la personne est l'unité prédominante dans la conversation sur la vie privée, et donc que chaque personne peut et doit gérer les informations uniquement sur elle- même[21]. C'est un oubli[22]. En consentant à la collecte d'informations, un utilisateur devient un canal de

18 Daniel J. Solove, *op. cit.*, note 6.

19 Daniel J. Solove, Woodrow Hartzog, « The FTC and the New Common Law of Privacy », (2014), *114 Columbia Law Review 583*, pp. 667.

20 En 2014, dans le même ordre d'idée, une étude Ipsos France révélait que 67% d'entre eux assuraient lire que *rarement ou jamais* ces conditions d'utilisation. Voir « Les français et le Big Data », *Ipsos-France, Enquête auprès des consommateurs, (2015),* pp. 16 et pp. 28.

21 Emil Protalinski, « Survey: Facebook, Google Privacy Policies Are Incomprehensible », *ZDNET,* (4 Mai 2012).

22 Bamberger, Mulligan, *op. cit.*, note 16.

collecte d'informations sur l'ensemble de son réseau social, qu'il ait ou non consenti de sorte que les données ne sont plus de simples données personnelles, mais des « données en réseaux » qui lient plusieurs personnes les unes avec les autres. En effet, nous interagissons constamment les uns avec les autres de sorte qu'il est de plus en plus difficile d'identifier des données qui sont vraiment « personnelles ». Aujourd'hui, les utilisateurs des nouvelles technologies divulguent constamment des informations, et sur le moindre de leurs mouvements[23] notamment au travers des réseaux sociaux[24]. Les consommateurs le font dans la croyance erronée que les données sont éphémères, ou en raison de promesses trop souvent rompues que les données des consommateurs peuvent être conservées à l'abri d'autres consommateurs ou de tiers malveillants[25]. Les smartphones ou autres appareils intelligents, omniprésents, permettent aux utilisateurs de fournir des informations sur eux-mêmes mais aussi sur les autres à longueur de temps[26]. Les possibilités de contourner les médias sociaux s'amenuisent à mesure que d'autres les emportent avec eux[27]. S'engager avec les médias sociaux n'est donc plus un choix purement individuel mais un résultat inévitable dans presque toutes les situations sociales. L'interconnexion des données va de mise avec leur interdépendance. Par consentement, un individu autorisant la collecte ou le traitement de ses données personnelles empièterait alors sur le droit à la vie privée de ses proches en raison de la nature même de la donnée. Les dérives issues du commerce de données extraites des tests génétiques récréatifs commercialisés à bas coûts sur Internet en sont un exemple flagrant. En 2017, la CNIL publiait son premier « Point CNIL : Les données génétiques »[28], où elle indiquait : *« les données génétiques présentent aussi la particularité d'être non seulement personnelles mais aussi pluripersonnelles car transmissibles et partagées. »*[29]. En effet, les données génétiques sont liées à l'ADN de son porteur et permettent de le

23 Mark MacCarthy, *op. cit.*, note 13.

24 Ils le font sur les commerces qu'ils visitent, les itinéraires qu'ils empruntent, les activités qu'ils réalisent, la nourriture qu'ils ingèrent et les personnes qu'ils rencontrent. Voir Michael Birnhack, « Reverse Engineering Informational Privacy Law », (2013), *15 Yale Journal of Law & Technology 24*, p. 86.

25 Les utilisateurs des réseaux sociaux *taguent* des photos les uns des autres sur Facebook et se référencent dans des publications géolocalisées. Voir James Grimmelmann, « Saving Facebook » (2009), *94 Iowa Law Review 1137*, pp. 1145–46; Voir aussi Nick BILTON, « Disruptions: Indiscreet Photos, Glimpsed Then Gone », *N.Y. Times: Bits,* (6 mai 2012, 5:24 pm); Voir aussi Jason Mazzone, « Facebook's Afterlife », (2012), *90 North Carolina Law Review 1643,* p. 1653.

26 Catherine Shu, « Confirmed: Snapchat Hack Not A Hoax, 4.6M Usernames And Numbers Published », *Techcrunch* (31 Décembre 2013).

27 Thomas H. Chia, « Fighting the Smartphone Patent War with Rand-Encumbered Patents », (2012), *27 Berkeley Technology Law Journal 209*, p. 231.

28 Peter Swire, « Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment », (2012), *90* North California Law Review 1371, pp. 1381–82.

29 Rapport CNIL, *Point CNIL: Les données génétiques,* La documentation française, CNIL, (2017).

distinguer parmi tous les autres êtres humains, mais elles sont également partagées pour partie par plusieurs personnes. Ainsi, même si les régulateurs réussissaient à donner un sens au consentement individualisé à la collecte de données, ils manqueraient l'essentiel. Les individus éduqués et responsabilisés n'ont toujours pas leur mot à dire, car même s'ils sont parfaitement informés et responsabilisés, ils ne contrôlent que leurs propres données et ne peuvent pas influer sur la montagne d'informations à partir desquelles les algorithmes de Big Data fonctionnent. Tant que des informations sont fournies par des tiers, personne ne peut vraiment s'en écarter. Si une personne ne fait pas elle-même partie du réseau, elle abandonne son avantage individuel, tout en supportant (la majeure partie du temps) son coût individuel[30].

[6] Le parti pris de l'individualisme n'est pas exclusif à la législation européenne, il traverse également les principales divisions culturelles et juridiques du droit à la vie privée. Par exemple, les approches de la vie privée semblent à première vue différentes de chaque côté de l'Atlantique[31]. Selon James Q. Whitman, si l'Amérique du Nord se concentrent sur la liberté[32], l'Union européenne, elle, s'appuie sur le concept de dignité humaine[33]. Pourtant, les deux philosophies considèrent la vie privée comme une question qu'il est préférable de résoudre en informant et en responsabilisant les individus[34]. En Europe comme en Amérique du Nord, l'objectif présumé est d'informer les individus sur le consentement à l'utilisation de leurs données personnelles. Néanmoins, le problème demeure : les données n'ont pas d'incidence sur cette personne seule. Sans avoir la prétention de proposer une analyse exhaustive des deux traditions, cet argument souhaite démontrer que l'apparente fracture transatlantique dans la théorie de la vie privée masque une similitude de fait sous-jacente[35]. Dans les deux ordres juridiques, les individus consentent à l'utilisation de données ayant un impact sur des tiers non consentants[36]. Les approches

30 *Ibid*.

31 Joshua A.T. Fairfield, Christoph Engel, « Privacy as a Public Good », (2015), *65:3 Duke Law Review 38.*

32 James Q. Whitman, « The Two Western Cultures of Privacy: Dignity Versus Liberty », (2004), *113 Yale Law Journal 1151*, pp. 1167.

33 *Ibid,* p.1158.

34 *Ibid*, p.1161.

35 Omer Tene, Jules Polonetsky, « To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising », (2012), *13 Minnesota Journal of Law, Science & Technology 281*, p. 287.

36 James Q. Whitman, *op. cit.*, note 32.

de la liberté et de la dignité se concentrent sur l'autonomisation et l'information des individus, plutôt que sur l'amélioration de la coordination de groupe[37]. Les lois nord-américaines et européennes diffèrent selon que les individus doivent accepter ou refuser la collecte et le traitement des données ainsi que sur la portée et le moment du consentement de la personne. Bien qu'héritières d'approches normatives différentes, les deux traditions situent le problème et sa solution autour de l'individu décidant de manière isolée: l'individu doit accepter ou refuser[38] à des utilisations bien souvent hors contexte. C'est en effet le cas puisqu'il devra poursuivre la suppression des données qui le concernent aux différentes phases de la vie de cette donnée. Ceci apparait d'autant plus dérangeant qu'il s'agit de données aussi sensibles que les données personnelles de santé.

[7] La discussion ci-dessus tente de souligner le sérieux parti pris en faveur de la conceptualisation de la vie privée en termes d'informations individuelles, de droits et d'actions. De plus, une succincte comparaison des approches nord- américaine et européenne montre que, malgré d'apparentes différences, ces approches se concentrent toutes les deux sur l'individualisme. En conséquence, cette théorie juridique occulte le dilemme social de la vie privée, comme nous allons, à présent, le développer.

II. L'INFLUENCE ÉMERGENTE DU COLLECTIVISME DANS LE DROIT DES DONNÉES DE SANTÉ

[8] Face à cette conception individualiste de la relation de la personne à ses données et du consentement, certains proposent une vision différente. En effet, les données personnelles, notamment celles relatives à la santé, même si elles relèvent pour chacun d'entre nous de la sphère privée la plus intime, deviennent aussi – par leur mise en commun – les composantes d'un réseau d'informations utiles à l'intérêt général[39]. Ce réseau constituerait un bien « public » ou « commun » relevant d'une protection collective de la vie privée. La justification découle du fait que, dans un réseau, les données deviennent « relationnelles » et ne pourraient donc pas être considérées comme relevant d'un enjeu

37 Omer Tene et Jules Polonetsky, *op. cit.*, note 35.

38 James Q. Whitman, *op. cit.*, note 32.

39 Omer Tene, Jules Polonetsky, « Big Data for All: Privacy and User Control in the Age of Analytics », (2013), *11 Northwestern Journal of Technology & Intellectual Property 239*, pp. 60–62.

purement individualiste. La donnée étant intégrée à un réseau, la protection du réseau serait alors plus adaptée que celle des données de chaque personne composant ce réseau. Pour être efficace[40], une protection relevant d'une conception individualiste imposerait en effet des limites sévères au partage des données, sauf anonymisation pouvant provoquer une dégradation qui priverait le traitement d'une partie de son efficacité. Dans cette approche, les « *données de santé, ne peuvent pas être protégées avec une approche* libérale concentrée sur la maximisation des libertés individuelles mais il serait plutôt nécessaire d'adopter une optique plus communautaire ou collective, qui pourrait exiger une limitation de certaines libertés individuelles, au nom de l'intérêt général et du bien commun »[41].

[6] Au nom de l'intérêt général et de la nécessité de favoriser le progrès, il pourrait être permis de remettre en cause la nécessité même d'un consentement au traitement des données, jugé comme pouvant être un obstacle excessif. D'autres plaident pour un contrôle plus laxiste et estiment que le consentement individuel pourrait être écarté s'il existe une forte probabilité que le traitement contribue à l'amélioration de la santé de la personne et, au-delà, à celle de la collectivité, lorsque le risque d'atteinte est proportionnellement plus faible. Une troisième conception intermédiaire fut proposée, celle d'une forme d'autonomie interactive et relationnelle, dans laquelle la personne gère ses données mais est intégrée dans une collectivité qui met en oeuvre un projet collectif qui la protège[42]. Cette dernière conception se fonde sur une littérature américaine florissante[43] qui propose d'explorer la valeur collective de la vie privée, proposant des exégèses originales des notions tirées de l'économie publique pour la qualifier de bien collectif à part entière.

[7] Néanmoins les concepts regroupés sous le vocable de biens collectifs sont polysémiques et ne recouvrent pas *de facto* les mêmes définitions selon qu'ils sont analysés par des philosophes, des politologues, des juristes ou des économistes. Certains auteurs soutiennent que la vie

40 *Loi n° 2016-1321* du 7 octobre 2016 pour une République numérique pose les premiers jalons d'une reconnaissance de la valeur collective des données.

41 Yann Joly, *et al, «* Are data sharing and privacy protection mutually exclusive? », (2016), *Cell 167,* p. 1150.

42 Danièle Bourcier, Primavera De Filippi. « Vers un droit collectif sur les données de santé », (2018), *Revue de Droit sanitaire et social*, pp. 444-56.

43 Voir nos travaux sur les fiducies de données qui offrent de belles perspectives d'une gestion collective des données: Fabien Lechevalier, *Les fiducies de données personnelles de santé*, Mémoire de maitrise, Université Laval, 2020.

privée serait un véritable bien public[44] car sans intervention mesurée, les décisions relevant de la vie privée personnelles d'individus pleinement informés tendent à réduire la vie privée d'autres individus. La littérature juridique n'est pas entièrement exempte de la suggestion selon laquelle la vie privée peut être étudiée de manière rentable comme un véritable bien public[45]. Par exemple, Paul Schwartz ou encore Joshua A.T. Fairfiel et Christoph Engle notent que la confidentialité des informations fonctionne comme tout autre type de bien public, à savoir comme l'air pur ou la défense nationale[46] et que la vie privée, d'un point de vue constitutif, est aussi un « bien public ». Schwartz ajoute que les informations privées sont en quelque sorte des « biens communs » qui nécessitent un certain degré de contrôle social[47]. Dans cette formulation il instaure cependant un doute sur la qualification qu'il donne auxdites informations : bien public pur ou bien commun[48] ? C'est dans cette même perspective que Priscilla Regan discute de la « *valeur collective* » de la vie privée, qu'elle tire quant à elle du concept des économistes de biens communs[49]. Elle suggère plus largement que la reconnaissance du fait que la vie privée possède certaines caractéristiques d'un bien commun rendrait plus clair d'une part, les intérêts institutionnels dans les informations personnelles et d'autre part, les faiblesses d'une solution de marché pour fournir une meilleure protection de la vie privée[50]. L'analyse de Regan pourrait trouver son positionnement dans le mouvement des *communs*[51] qui s'est développé ces dernières années au sein de la communauté scientifique. Pour le chercheur américain David Bollier, il s'agit d'une *« nouvelle manière de penser et de prendre soin des ressources qui n'appartiennent ni à un acteur*

44 Stefaan G. Verhulst, « Leveraging Private Data for Public Good. A Descriptive Analysis and Typology of Existing Practices », *GOVLAB*, (2019). En ligne: https://thelivinglib.org/leveraging-private-data-for-public-good- a-descriptive-analysis-and- typology-of-existing-practices/ ; Pricilla M. Regan, « Privacy as a Common Good in the Digital World », (2002), *5:3 Information, Communication & Society 382* ; Anita Allen, « Protecting One's Own Privacy in a Big Data Economy », (2016), *130:71 Harvard Law Review Forum 71* ; Joshua A.T. Fairfield, Christoph Engel, « Privacy as a Public Good » (2015), *65:3 Duke Law Review 38* ; Priscilla M. Regan, « Response to Privacy as a public good », (2016), *65 Duke Law Review 51* ; Mariana Mazzucato, « Let's make private data into public good », (27 Juin 2018), *MIT Technology Review,* En ligne: https:// www.technologyreview.com/s/ 611489/lets-make-private-data-into-a-public-good/ ; Julia Lane, Helen Nissenbaum, Victoria Stodden, Stefan Bender (éd.), *Privacy, Big Data, and the Public Good,* Cambridge University Press, (2016) ; Julie E. Cohen, T*urning Privacy Inside Out* (April 12, 2018). etc.

45 Si un bien public pur (définis par Samuelson en 1954) est un bien non rival et non exclusif, le coût de son financement est tel qu'aucun intérêt privé n'accepterait de le financer n'ayant pas de certitude quant à la rentabilité de l'investissement.

46 Edward J. Janger, Paul M. Schwartz, « The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules », (2002), *86 Minnesota Law Review 1219*, pp. 1253–54.

47 Schwartz, *op. cit. ;* Fairfield, Engel, *op. cit.*

48 Edward J. Janger et Paul M. Schwartz, *op. cit.*, note 46.

49 Les propriétés de rivalité et de non exclusion définissent *les biens en commun*. On considère qu'ils ont des externalités positives et pour cette qualité, il faut les protéger via la puissance publique. Voir François Lévêque, *Les théories de la réglementation*, Ed. La découverte, Collection Repères, (2005).

50 Priscillia M. Regan, *op. cit.*, note 9.

51 Mark MacCarthy, *op. cit.*, note 13.

privé, ni à un acteur public, et qui sont partagées et gérées par une communauté qui en définit les droits d'usage (accès, partage, circulation) »[52].

[8] Les *communs* existent sous une diversité de formes et d'arrangements institutionnels, comme l'ont démontré l'ensemble des travaux d'Elinor Ostrom, Prix Nobel d'économie, et d'autres chercheurs qui ont étudié l'action collective et la gestion des biens communs. Menés durant plusieurs décennies, les travaux d'Ostrom démontrent que l'action collective peut être un moyen efficace de gérer des ressources de manière équitable et pérenne, tout en renforçant les liens sociaux qui tissent des communautés résiliantes et durables[53]. Envisager les données, et à fortiori les données de santé, sous le prisme de biens collectifs permettrait de reconnaitre leur valeur publique tout en prenant en compte les enjeux collectifs de la vie privée préalablement identifiés.

[8] Ces approches divergentes montrent que le point de friction demeure la sempiternelle évolution du rapport entre l'individuel et le collectif, entre l'autonomie accrue de chacun et la protection que nécessite l'utilisation généralisée des technologies de traitement de données de masse. Les progrès de l'une inspire le renforcement de la seconde. Leur concordance ne va pas sans heurts et suscite de vives tensions car intérêt individuel et collectif ne coïncident pas nécessairement. Conceptions individuelle, collective ou relationnelle peuvent contribuer à la recherche d'un point d'équilibre à constamment assortir aux progrès technologiques et à l'évolution des modes de vie.

52 Concrètement, un commun peut prendre la forme d'une ressource naturelle (forêt, pâturage), matérielle (voiture, musée) ou immatérielle (logiciel libre, article scientifique). Le plus célèbre d'entre tous, c'est bien sûr l'encyclopédie en ligne Wikipédia, avec ses milliers d'administrateurs et ses millions d'usagers.

53 David Bollier, « Elinor Ostrom Remembered (1933-2012) », *blog personnel,* (12 juin 2012).

LES DONNÉES PERSONNELLES À L'ÉPREUVE DE L'*OPEN DATA* DES DÉCISIONS DE JUSTICE : ENTRE PRINCIPE DE TRANSPARENCE DE LA JUSTICE ET DROIT À LA VIE PRIVÉE

Flora DORNEL[1]

1 L'auteure est candidate à la Maîtrise avec mémoire à l'Université Laval, cheminement bi-diplômant avec l'Université Paris-Saclay, programme Propriété Intellectuelle Fondamentale et Technologies Numériques.. E-mail : floradornel@gmail.com

Résumé

Que ce soit en France ou au Canada, les données judiciaires font l'objet d'une législation en faveur de l'open data. Les données judiciaires (décisions de justice, plumitifs…) sont mises à la disposition des citoyens gratuitement et de manière électronique, sur Internet. Or, ces données judiciaires comportent une multitude de renseignements personnels. La question qui est au cœur du problème est alors l'affrontement de deux valeurs fondamentales : d'un côté, le droit du public à la transparence de l'administration de la justice, qui justifie que les données judiciaires soient consultables, et de l'autre, le droit de l'individu à la protection de sa vie privée, qui pourrait se retrouver en situation de vulnérabilité.

[1] Le mouvement global de l'open data prend de l'ampleur[2], sans épargner le domaine judiciaire : on constate aujourd'hui, que ce soit en France ou au Canada, que les données judiciaires font l'objet d'une législation en faveur de l'open data, c'est-à-dire de la donnée ouverte, publique, gratuite, accessible par tous, et réutilisable[3]. L'équilibre préexistant entre deux principes fondamentaux, à savoir le principe de transparence de la justice et le droit à la vie privée, s'en trouve bouleversé.

I - L'*OPEN DATA* AU SERVICE DU PRINCIPE FONDAMENTAL DE LA TRANSPARENCE DE LA JUSTICE

[2] Comme le dit l'adage, « justice is not only to be done, but to be seen to be done ». Non seulement la justice doit être rendue, mais en plus l'on doit voir qu'elle est rendue : une justice secrète ne permettrait pas un régime démocratique. Ce principe de la transparence de la justice est traduit par l'exigence de publicité des débats judiciaires : « là où il n'y a pas de publicité, il n'y a pas de justice »[4]. Et l'open data est présentée comme un bon moyen pour renforcer ce principe de transparence de la justice. En France, le sujet est particulièrement actuel : la Loi de 2016 *pour une République numérique*, puis la Loi de 2019 de *programmation et de réforme pour la justice,* viennent prévoir l'application de l'open data aux décisions de justice. Un projet de décret pour la mise en application a été rendu public en décembre 2019, mais a été source de vives contestations[5]. En effet, l'un des arguments principaux soulevé par les professionnels du droit concerne les risques d'atteinte au droit à la vie privée[6] qu'engendre l'électronique au vu du nombre de données personnelles contenues dans ce type de documents mis en ligne. Le décret a été publié le 30 juin dernier, sans modification des dispositions qui faisaient l'objet des contestations[7].

2 Partenariat Open Government Partnership, regroupant 78 pays dans le monde, en ligne : <https://www.opengovpartnership.org/about/>

3 Loïc CADIET, « l'open data des décisions de Justice », Rapport de la mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, novembre 2017.

4 *A.G. (Nova Scotia) c. MacIntyre*, 1982 CanLII 14 (CSC), [1982] 1 RCS 175, <http://canlii.ca/t/1lpbp>.

5 Communiqué commun des syndicats de la magistrature, 6 février 2020, en ligne : <https://www.usma.fr/communiques/communique-commun-aux-syndicats-de-magistrats-tendant-au-retrait-du-projet-de-decret-sur-l-open-data>

6 *Ibid*.

7 Décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives, en ligne : <https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000042055251>.

[3] Dans l'optique de renforcer la confiance des citoyens dans les cours et tribunaux, M. le rapporteur Christophe-André Frassa dit à propos des articles 20 et 21 de la Loi du 7 octobre 2016 qu'ils « visent un même objectif extrêmement important : garantir l'ouverture, le partage et la réutilisation, autrement dit l'open data des décisions de justice. Ces décisions de justice sont toutes rendues au nom du peuple français et sont publiques. Il apparaît donc opportun de prévoir la mise à disposition de toutes les décisions, et pas seulement de celles publiées par la Cour de cassation ou le Conseil d'État, car elles feraient jurisprudence »[8]. Le principe est alors renversé : toutes les décisions de justice doivent avoir le mérite d'être rendues accessibles. Ainsi décidé, il serait intéressant de mener une étude analysant les conséquences sur la jurisprudence… Sur la confiance que doit entraîner l'open data vis-à-vis des citoyens, Mme Axelle Lemaire, ancienne secrétaire d'État au numérique et à l'innovation ayant porté les articles 20 et 21 de la Loi du 7 octobre 2016, justifie l'open data par le renforcement démocratique que cette technique peut permettre par la transparence dont elle fait preuve[9].

II- ACCÈS ÉLECTRONIQUE : UN FACTEUR DE BOULEVERSEMENT POUR LA VIE PRIVÉE

A. LA DISPARITION DE L'« OBSCURITÉ PRATIQUE »

[4] L'électronique vient chambouler l'équilibre préexistant entre le droit à la vie privée et la transparence de la justice : la facilité d'accès aux renseignements contenus dans les plumitifs et les décisions de justice n'a plus rien à voir avec la situation antérieure, où il fallait fournir l'effort de se rendre en personne au Palais de justice afin de consulter les documents. Cette démarche, qualifiée d'« obscurité pratique »[10], disparaît puisque la consultation des informations judiciaires est numérisée. Chacun pourra, en théorie, consulter les données judiciaires depuis son poste informatique. Et cette possibilité est confortée par le mouvement *open data*.

[5] On note ici une différence entre l'approche canadienne et l'approche française. Au Canada, face à la « friction » entre le droit à la vie privée et la

8 Séance du Sénat du 27 avril 2016, propos de M. Christophe-André Frassa.

9 Revue pratique de la prospective et de l'innovation, n° 2, oct. 2017, entretien n°4, p. 9, en ligne : <http://www.tendancedroit.fr/wp-content/uploads/2017/10/ITW-ppi1702-3.pdf>.

10 Lynn E. SUDBECK, « Placing Court Records Online: Balancing Judicial Accountability with Public Trust and Confidence: An Analysis of State Court Electronic Access Policies and A Proposal for South Dakota Court Records », 51 S.D. L. REV. 81, 83 (2006).

transparence de la justice, la position de la Cour suprême est plutôt claire : sauf cas exceptionnels prévus par les textes, la transparence de la justice prime sur la vie privée des individus[11]. Et l'introduction de l'électronique n'en change pas le principe. On peut d'ailleurs avoir accès aux plumitifs et aux décisions de justice à partir d'un simple site Internet[12]. Mais quels sont les risques pour les individus de voir leur identité divulguée de la sorte, notamment dans les plumitifs où des tiers peuvent également apparaître ?

[6] En France, il est prévu que la mise à disposition sous forme électronique - qui ne concerne que les décisions de justice - doit se faire en analysant le risque de « réidentification »[13]. Il faut donc comprendre que les décisions judiciaires feront l'objet d'une dépersonnalisation, avant leur mise en ligne, au nom du respect au droit à la vie privée des individus.

B. LES RISQUES DE RÉUTILISATION DES RENSEIGNEMENTS PERSONNELS

[7] L'électronique vient modifier la situation que l'on avait avant, endossant alors un rôle menaçant pour le respect du droit à la vie privée : on peut penser dans un premier temps aux « prédateurs potentiels » ou aux « voisins fouineurs »[14] qui iront chercher des informations sans aucune justification légitime. Mais ces comportements, bien que parfois dérangeants, sont souvent peu préjudiciables de manière sérieuse, et ne sont pas la raison de la principale inquiétude véhiculée par l'électronique. La source d'inquiétude plus importante est celle qui concerne les sociétés privées[15], telles que les banques, les courtiers de données, les compagnies d'assurance, etc. Ces organisations auraient alors accès à des données qu'elles n'auraient jamais eues avant, et pourraient être à

11 A.G. (Nova Scotia) c. MacIntyre, [1982] 1 RCS 175 ; Edmonton Journal c. Alberta (Procureur général), [1989] 2 RCS 1326, ; Vickery c. Cour suprême de la Nouvelle-Écosse (Protonotaire), [1991] 1 RCS 671 ; F.N. (Re), [2000] 1 RCS 880 ; Sierra Club du Canada c. Canada (Ministre des Finances), [2002] 2 RCS 522.

12 Site SOQUIJ <https://soquij.qc.ca/fr/services-aux-professionnels/catalogue/plumitifs>.

13 Article 21 al.2 de la Loi de 2016 *pour une République numérique* : « Cette mise à disposition du public est précédée d'une analyse du risque de ré-identification des personnes ».

14 Nicolas VERMEYS, « Privacy v. Transparency: How Remote Access to Court Records Forces Us to Re-examine Our Fundamental Values » dans Karim BENYEKHLEF et al, dir, *eAccess to Justice*, University of Ottawa Press, 2016, 123–154, en ligne : JSTOR <https://www.jstor.org/stable/j.ctt1wn0qx3.9>.

15 Kristin MAKAR, « Taming Technology in the Context of the Public Access Doctrine: New Jersey's Amended Rule 1:38 », *Seton Hall Law Review (2011),* Vol. 41 : Iss. 3 , Article 7, en ligne : <https://scholarship.shu.edu/shlr/vol41/iss3/7>.

l'origine d'un changement de comportement de leur part, en fonction des renseignements personnels qu'elles pourraient trouver[16].

[8] Bien évidemment, récupérer et utiliser des renseignements personnels sans le consentement des individus est interdit par la Loi *sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[17]. Mais surveiller le respect de ce principe de manière concrète semble difficile à concilier avec la mise à disposition publique des données judiciaires, et ne permet pas de prévenir de potentielles situations de vulnérabilité dans laquelle se retrouveront certains individus. Il existe une multitude d'illustrations de réutilisation des renseignements personnels qui peuvent être citées, en dehors du cadre exclusif des documents judiciaires[18]. L'accès électronique peut devenir une faille juridique permettant le traitement de renseignements personnels et dont la finalité est totalement détournée. Il faut alors s'interroger sur le cadre juridique existant actuellement. Il n'est plus à prouver que la présence des renseignements personnels trouvés en lignes sont nombreux et qu'il est relativement aisé, en pratique, de se les procurer pour s'en servir à d'autres fins que celles prévues initialement.

III- PUBLICITÉ ET OPEN DATA : DIFFÉRENCE D'APPROCHE ENTRE LE CANADA ET LA FRANCE

[9] La France et le Canada n'envisagent pas le principe de publicité et celui de la publication de la même manière (A). Ainsi, il y a divergence quant à la réutilisation des renseignements personnels trouvés dans les documents judiciaires mis à disposition du public (B).

A. DIVERGENCE ENTRE LE CANADA ET LA FRANCE QUANT À L'APPRÉCIATION DE LA PUBLICITÉ ET DE LA PUBLICATION

[10] Au Canada, il semblerait que la publicité va de pair avec la publication, ou plus précisément, que la publication renforce la publicité.

16 Daniel J. SOLOVE, « Access and Aggregation: Privacy, Public Records, and the Constitution », 86 Minn. L. Rev. 1137 (2002) p.1149 : ChoicePoint Inc a compilé et regroupé des données sur des millions de personnes à partir de divers documents publics, que le gouvernement et les employeurs utilisent pour filtrer et enquêter sur les salariés actuels et potentiel.

17 Annexe 1 de la Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, c5 : « Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire ».

18 Etude par Synovate, « Federal Trade Commission - Identity Theft Survey Report » (2003), en ligne : <http://www.ftc.gov/os/2003/09/synovatereport.pdf> ; voir aussi « Federal Trade Commission Overview of the Identity Theft Program - October 1998-September 2003 » (2003), en ligne : <http://www.ftc.gov/os/2003/09/timelinereport.pdf>, Daniel J. SOLOVE, préc., note 16, p. 1149.

En effet, le juge LaForest indique dans l'arrêt *SRC c. N.-B. (Procureur général)*[19] que l'accès aux tribunaux « se rattache intégralement au concept de démocratie représentative et à l'importance correspondante de la publicité des débats en justice ». Et pour veiller à l'efficacité de cette publicité, le juge reconnaît que les médias jouent, par la collecte et la diffusion d'informations sur les tribunaux, un rôle essentiel dans l'information du public, et plus largement, que « les médias ont un rôle primordial à jouer dans une société démocratique »[20]. Ainsi dit, la diffusion, donc la publication, vient bien soutenir l'exigence de publicité, et *in fine*, la transparence de la justice.

[11] En France, l'interprétation est différente. En effet, il faut distinguer entre accès et diffusion, c'est-à-dire entre publicité et publication. À ce propos, les dernières décisions des Cours de justice affirment que « l'open data n'a pas pour vocation de porter une nouvelle forme de publicité »[21]. Et d'après Yannick MENECEUR, la Loi 2018-2022 de programmation et de réforme pour la justice « ne remet pas en cause le régime de publicité des audiences et des décisions, et ne fait qu'organiser une nouvelle forme de délivrance au public des décisions de justice »[22]. Ainsi, un nouveau mode de diffusion est permis grâce à l'open data, c'est-à-dire une nouvelle forme de publication, mais cela n'est pas à confondre avec l'obligation de publicité, qui, elle, sera remplie par l'accès physique à la salle d'audience par exemple[23]. Il semble justifié qu'un nouveau moyen de publication ne devrait pas empiéter plus que nécessaire sur la vie privée des individus, et qu'il est alors évident que les décisions mises en ligne soient dépersonnalisées.

[12] On peut en effet se demander si l'accès à l'identification des individus dans les décisions en ligne permettrait de remplir davantage l'obligation de transparence de la justice.

19 *Société Radio-Canada c. Nouveau-Brunswick (Procureur général)*, 1991 CanLII 50 (CSC), [1991] 3 RCS 459, <http://canlii.ca/t/1fsh4>.

20 *Supra* note 19.

21 CA Paris, pôle 2 - ch. 1, 18 déc. 2018, n° 17/22211. Lire en ligne : <https://www.doctrine.fr/d/CA/Paris/2018/CBD628309EEBD087B10BA> et Cour d'appel de Paris, pôle 2, chambre 1, 25 juin 2019, n° 19/04407, en ligne : <https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2019/07/19-04407.pdf>.

22 Yannick MENECEUR, « Open data des décisions de justice - Pour une distinction affirmée entre les régimes de publicité et de publication », *JCP E*, n°37, 12 septembre 2019, 1415.

23 Article 6§1 de la Convention Européenne des Droits de l'Homme.

B. DIVERGENCE ENTRE LA FRANCE ET LE CANADA QUANT À LA RÉUTILISATION DES INFORMATIONS TROUVÉES DANS LES DOCUMENTS JUDICIAIRES MIS À DISPOSITION DU PUBLIC

[13] Concernant la réutilisation de l'identité des magistrats, cela fait l'objet, aux yeux d'une partie de pays étrangers, d'une « bizarrerie » française. En effet, si l'identité des magistrats reste publique à tous, la réutilisation de cette information est strictement interdite. Cela est expressément prévu à l'article 33 II. 1° alinéa 3 de la loi programmation 2018-2022 et de réforme pour la justice, qui dispose : « Les données d'identité des magistrats et des membres du greffe ne peuvent faire l'objet d'une réutilisation ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées. La violation de cette interdiction est punie des peines prévues aux articles 226-18,226-24 et 226-31 du code pénal (…) ».

[14] Cette disposition peut surprendre à l'étranger : par exemple, aux États-Unis et au Royaume-Uni, les juges semblent avoir accepté la pratique consistant à analyser leurs décisions. Cela laisse le champ libre aux *legaltechs* pour essayer de trouver des modèles qui prévoiraient quel serait le comportement d'un juge donné[24], donc, en d'autres termes, le « profilage » est autorisé. La position française se démarque drastiquement en rendant cette éventualité tout simplement illégale. Cela peut s'expliquer en gardant en tête la finalité pour laquelle l'open data a été pensée et mise en œuvre : davantage de transparence et un accès aux décisions facilité. Mais sûrement pas dans l'idée de donner de la matière, non filtrée, aux *legaltechs*, qui pourraient en user de manière éthiquement discutable. Si l'on essaie de se projeter un tant soit peu, on peut en effet craindre que le jeu de profilage, de « prédiction » en fonction d'un litige donné, restreigne la liberté d'exercer du magistrat, et débouche sur un effet « moutonnier » des magistrats. Il faudra beaucoup de volonté et d'assurance de la part de ces derniers pour statuer différemment de ce que la technologie aurait prévu, et différemment de leurs collègues. Pourtant, on sait bien que chaque affaire peut être distincte, et qu'une décision d'un juge est également rendue *in concreto*, c'est-à-dire en prenant en compte le contexte dans lequel s'inscrit le litige. Et heureusement que les juges ont la liberté d'être à l'origine de revirement de jurisprudence en toute bonne conscience !

24 Artificial Lawyer, « France Bans Judge Analytics », 4 juin 2019, en ligne : <https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison-for-rule-breakers/>..

[15] Concernant les parties au litige, leur identité est occultée. Nous avons déjà étudié les risques pour elles si leurs données à caractère personnel étaient rendues accessibles à tous facilement. Là encore, cette exigence d'occulter les noms des parties dans les décisions en France se démarque à l'étranger, et notamment au Canada. Pour ces derniers, la divulgation de l'identité des individus fait partie des obligations à accomplir pour le principe de publicité. Mais en France, tel n'est pas le cas. La conception française distingue là où le Canada ne le fait pas forcément : la mise à disposition est une publication, un moyen de diffusion de l'information. Ce n'est pas une des conditions à remplir pour respecter le principe de publicité. On l'a dit, ce principe sera rempli autrement. Alors faut-il considérer que le principe de publicité est davantage rempli lorsque la publication est totale, sans occultation aucune ? La transparence de la justice nécessite-elle que les individus soient identifiés, identifiables dans les décisions de justice ?

IV- UN NOUVEL ÉQUILIBRE ENTRE LA TRANSPARENCE DE LA JUSTICE ET LE DROIT À LA VIE PRIVÉE ?

[16] Quelles pourraient être les pistes de réflexion afin de trouver un équilibre entre le principe de la transparence de la justice et celui du droit à la vie privée, à l'ère du numérique ? La solution française réside dans la technique de la pseudonymisation (A). Elle est mentionnée comme technique de dépersonnalisation par le Règlement Général sur la Protection des Données. Ce règlement propose également d'autres instruments pour trouver un équilibre entre la diffusion d'informations judiciaires et le droit à la vie privée des individus (B).

A. LA SOLUTION FRANÇAISE ACTUELLE : LA PSEUDONYMISATION

[17] La pseudonymisation est la technique encouragée au sein de l'Union européenne, bien qu'elle puisse par certains aspects se retrouver limitée dans son efficacité (1). Comment pseudonymisation et open data évoluent-elles ensemble ? (2)

1. LA PSEUDONYMISATION ENCOURAGÉE MAIS LIMITÉE DANS SON EFFICACITÉ

[18] Le RGPD propose la pseudonymisation comme illustration de mesures techniques et organisationnelles appropriée pour la protection des données, et c'est la technique que la France a décidé de mettre en

œuvre pour diminuer le risque d'atteinte à la vie privée. Selon la Commission nationale de l'informatique et des libertés (CNIL), « c'est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires »[25]. Il ne faut pas confondre la technique de la pseudonymisation avec celle de *l'anonymisation*. Cette dernière est « un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible »[26]. C'est donc l'irréversibilité de l'opération qui caractérise l'anonymisation.

[19] La pseudonymisation semble être adéquate en théorie. Cependant, en pratique, il est souvent aisé de retrouver l'identité des individus grâce au croisement de données : dans le rapport Cadiet[27], il est bien spécifié que les décisions de justice « contiennent un nombre très important de données réidentifiantes, particulièrement au sein de la motivation de la décision, qui comprend de nombreux éléments de contexte pouvant conduire, notamment par des croisements avec d'autres bases de données, à une réidentification des personnes »[28]. Pour illustrer cela, on peut faire référence à une étude[29] réalisée par des chercheurs du *Massachusetts Institute of Technology* : elle a mis en évidence, dans le cadre d'un travail réalisé sur les transactions des cartes bancaires d'1,1 million de personnes ne comportant aucun élément d'identification, que quatre données spatio-temporelles (coordonnées géographiques, dates, heures) permettaient à elles seules de réidentifier 90 % des individus. La pseudonymisation ne paraît donc pas la solution optimale pour garantir de manière absolue le respect au droit à la vie privée des individus.

25 CNIL, « L'anonymisation des données, un traitement clé pour l'open data », 17 octobre 2019, en ligne : <https://www.cnil.fr/fr/lanonymisation-des-donnees-un-traitement-cle-pour-lopen-data>.

26 *Ibid.*

27 Rapport sur « "l'open data" des décisions de Justice », dit *Rapport CADIET,* 9 mai 2018

28 *Ibid*.

29 Y.-A. de MONTJOYE, L. RADAELLI, V. Kumar SINGH et A. PENTLAND, « Unique in the shopping mall : on the reidentifiability of credit card metadata », *Science*, 30 janvier 2015, en ligne : <https://science.sciencemag.org/content/347/6221/536?sid=9b47355e-d1da-4f56-b745-c876999ea9e3>

2. PSEUDONYMISATION ET OPEN DATA

[20] Les craintes des syndicats[30] de la magistrature française, suite à la publication du projet de décret en décembre 2019[31], se trouvent fondées : en effet, ils exigeaient « le retrait du projet de décret relatif à la mise en œuvre de l'open data des décisions de justice » en raison du manque d'évaluation de la charge de travail additionnelle, alors même que la justice est déjà surchargée. Et pourtant, la publication de ce décret le 29 juin 2020[32] définit les conditions de la diffusion des décisions des juridictions judiciaires et administratives, en chargeant les magistrats d'occulter les éléments permettant l'identification des individus (autre que les noms et prénoms)[33].

B. L'APPROCHE *PRIVACY BY DESIGN* PRÉVUE PAR LE RGPD

[21] L'article 25 alinéa 2 du Règlement Général sur la Protection des Données[34] prévoit que « le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées ». Il peut sembler opportun de s'intéresser aux apports de cette approche, d'origine canadienne[35], et consacrée dans le droit européen : pourquoi ne pas envisager d'appliquer, dès la création des documents, un système pour évacuer le maximum de données personnelles qui ne participent pas davantage à la transparence de la justice, et qu'il ne serait pas nécessaire de trouver en ligne. Évidemment, le débat sur ce principe de finalité est constamment en évolution, et il s'agira de mener une analyse approfondie sur la limitation, en ligne, du principe de la transparence de la justice face à la vie privée des personnes.

[22] La privacy by design dans le cadre de l'*open data* peut être un mode de régulation séduisant puisqu'il intègre la protection des données à

30 *Supra*, note 5.

31 Projet de décret relatif à l'open data des décisions de justice relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives, 13 décembre 2019, en ligne : <http://www.justice.gouv.fr/le-ministere-de-la-justice-10017/projet-de-decret-relatif-a-lopen-data-des-decisions-de-justice-32835.html>.

32 Décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives.

33 Nouvel article R111-12 du *Code de l'organisation judiciaire*.

34 Article 25 alinéa 1 du 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).

35 Ann CAVOUKIAN, « Privacy by Design : The 7 Foundational Principles », 2009 (Janvier 2011), *Information and Privacy Commissionner of Ontario,* en ligne : https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

caractère personnel dès la conception des outils de collecte, de traitement ou d'exploitation des données. On peut comparer cette technique à une sorte de filtre, à la charge du fabriquant, ou même à la charge du diffuseur de la base de données. La PbD s'inscrit dans une logique d'analyse de risque, participant à la consécration de l'accountability. Cela signifie qu'il y a obligation de rendre des comptes et de justifier des garanties mises en œuvre pour prévenir tout risque ou y remédier en cas de survenance (par exemple en cas de faille de sécurité). Alors comment la PbD peut venir en soutien pour empêcher que les données transmises par les administrations aux exploitants puissent être réutilisées de manière préjudiciable pour les individus[36] ?

CONCLUSION

[23] L'*open data* a été pensée dans l'objectif d'améliorer la transparence au profit des citoyens, et de permettre l'innovation. En effet, pour entraîner un algorithme, plus on pourra le nourrir de données, plus il sera performant. L'*open data* semble alors être une technologie très pertinente. Cependant, bien que l'open data puisse être louable dans le domaine judiciaire, puisque cela permet, entre autres, de participer à la transparence de la justice, et *in fine* à la confiance du public dans la justice, il ne faudrait pas perdre de vue les éventuelles atteintes aux autres droits et libertés des personnes qu'elle pourrait engendrer. Un raisonnement davantage global semble approprié, car une fois les données mises en ligne, il ne sera plus question de frontières étatiques. Des acteurs du monde entier pourront y accéder, et il est alors important de cerner ces enjeux à temps pour pouvoir les appréhender. N'attendons pas que la vulnérabilité des personnes se cristallise pour agir.

36 Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal modifiée par l'ordonnance n°2015-1341 du 23 octobre 2015 transposant la directive 2013/37, article 13.

APPRÉHENDER LES INÉGALITÉS D'ACCÈS À LA JUSTICE PAR LES MÉDIAS SOCIAUX : UNE PERSPECTIVE EMPIRIQUE SUR L'INFORMATION JURIDIQUE

Alexandra BAHARY-DIONNE[1]

1 Candidate au doctorat en droit, Université d'Ottawa. E-mail : abaha101@uottawa.ca

Résumé

Au même moment où les bénéfices, risques et limites de l'information juridique en ligne sur le plan de l'accès à la justice font l'objet de discussions multiples, la nature et la structure de cette information numérisée évoluent elles-mêmes à travers les mutations d'Internet et l'avènement des médias sociaux.

Ce texte fera ainsi état d'une recherche empirique sur les pratiques informationnelles des personnes ayant des questionnements juridiques à travers une analyse ethnographique de leurs échanges sur deux groupes Facebook d'entraide. Nous verrons que, d'une part, le Web social traduit des réalités émergentes dans la production et l'accès à l'information juridique telles que la mise en commun de l'information et des expériences avec le droit facilitée par l'interactivité, mais aussi la prolifération de la désinformation et des bulles informationnelles, dont les risques sont décuplés au détriment des groupes marginalisés. D'autre part, ces mêmes espaces numériques offrent des espaces de visibilité inédits en mettant à l'avant-scène la parole et les pratiques citoyennes. Les méthodes de recherche en ligne permettent alors d'éclairer des problèmes d'accès à la justice qui précèdent le numérique, mais qui sont difficiles à cartographier pour la recherche en droit, notamment les difficultés d'appropriation de l'information juridique.

Afin de comprendre dans quelle mesure le droit pourrait répondre aux défis du numérique dans toute leur complexité sociotechnique, il convient alors d'appréhender le numérique tant comme un amplificateur qu'un révélateur des inégalités sociales et, à ce chapitre, au prisme de ses possibilités méthodologiques pour la recherche en droit. Autrement dit, serait-il possible d'appréhender les défis et limites du droit *par* le numérique?

1. JUSTICE ET MÉDIAS SOCIAUX : ENTRE OBJET ET OUTIL DE RECHERCHE

[1] L'accès à la justice est une préoccupation croissante au Québec comme ailleurs au Canada. Sur une période de trois ans, près de la moitié de la population canadienne expérimentera un ou plusieurs problèmes juridiques[2]. Les personnes concernées se heurtent à la fois aux difficultés d'accès aux services juridiques et aux barrières de compréhension du droit[3]. Au-delà de l'accès aux tribunaux, on estime que le problème d'accès à la justice est beaucoup plus répandu et difficile à cartographier en raison de son caractère privé et diffus, pour ne penser qu'aux personnes qui « méconnaissent la dimension juridique de leur situation, ne trouvent pas réponse à leurs questions, abandonnent des recours[4] ou ignorent qu'[elles] en ont »[5]. Nous savons toutefois que c'est non seulement l'accès aux avocat.es qui est limité[6], mais également la capacité à connaître, à trouver, à comprendre et à utiliser l'information juridique disponible plus généralement[7].

[2] C'est dans ce contexte que plusieurs initiatives d'information juridique en ligne voient le jour dans un objectif de fournir des ressources plus intelligibles et accessibles au public[8]. Alors que les bénéfices, risques et limites de cette information numérisée font l'objet de discussions multiples, sa nature et sa structure évoluent à travers les mutations d'Internet. Les médias sociaux en particulier[9] suggèrent des manières émergentes de produire et d'accéder à l'information et aux ressources juridiques[10]. En 2016, au Québec, plus de 67 % des adultes avaient un

2 Trevor C. W. Farrow, Ab Currie, Nicole Aylwin, Lesley Jacobs, David Northrup et Lisa Moore, *Everyday Legal Problems and the Cost of Justice in Canada: Overview Report*, Toronto, Canadian Report on Civil Justice, 2016, p. 2.

3 Ainsi, 79% de la population admet avoir du mal à comprendre les lois, 61% ne pas être en mesure de saisir ce qui se passe devant les tribunaux et 70% conçoivent le système judiciaire comme un véritable « labyrinthe » : Pierre Noreau, *Révolutionner la justice: constats, mutations et perspectives*, Montréal, Éditions Thémis, 2010, p. 5.

4 Ce que feraient d'ailleurs la majorité des gens : Pierre-Claude Lafond, *L'accès à la justice civile au Québec: portrait général*, Cowansville, Yvon Blais, 2012, p. 15.

5 Emmanuelle Bernheim, Dominique Bernier, Alexandra Bahary-Dionne, Laurence Guénette, Louis-Philippe Jannard et Richard-Alexandre Laniel. « L'autoreprésentation et le plaideur citoyen » dans Pierre Noreau et al. (dir), *22 chantiers pour l'accès au droit et à la justice*, Cowansville, Yvon Blais, 2020 à la p 7.

6 Pierre-Claude Lafond, L'accès à la justice civile au Québec: portrait général, Cowansville, Yvon Blais, 2012, p. 120-22.

7 Jane Bailey, Jacquelyn Burkell et Graham Reynolds, « Access to Justice for All: Towards an Expansive Vision of Justice and Technology », (2013) 31 *Windsor B Access Just* 181.

8 James E. Cabral, Abhijeet Chavan, Thomas M. Clarke et John Greacen, « Using technology to enhance access to justice », (2012) 26 *Harv JL Tech* 241.

9 L'expression « médias sociaux » regroupe sous la même enseigne les blogues, les wikis et les sites de réseautage social comme Facebook : Alexandre Coutant et Thomas Stenger, « Médias sociaux: clarification et cartographie pour une approche sociotechnique », *Décisions Mark.* 2013.70.107, p. 115.

10 J. E. Cabral, A. Chavan, T. M. Clarke et J. Greacen, préc., note 8, p. 254.

compte actif sur un ou plusieurs médias sociaux[11]. Contrairement aux sites traditionnels, les médias sociaux exemplifient « l'idéologie participative du web social » en mettant à l'avant-scène « les amateurs, les citoyens, les utilisateurs *lambda* »[12]. Pour certain.es, ils pourraient alors faciliter « l'autogestion juridique »[13], voire même « démocratiser » l'information juridique et ainsi amoindrir les barrières financières et informationnelles de l'accès aux droits[14].

[3] Il existe cependant peu de connaissances quant à comment les non-juristes s'informent juridiquement et comment on les informe sur les médias sociaux. Comme on le constatait quelques années plus tôt à propos des forums de santé15, ces usages sont souvent abordés à partir de leurs conséquences alors qu'ils restent en soi peu définis et compris. C'est ce qui m'amené à étudier, à partir d'observations directes, les usages des médias sociaux spécifiquement à des fins de recherche et de partage d'information juridique. J'ai choisi de me pencher plus précisément sur le cas de deux groupes destinés au partage d'information juridique sur le média social Facebook dans l'objectif d'identifier les pratiques informationnelles des internautes que donnent à voir de tels espaces ainsi que les similitudes et les disparités entre les deux groupes à cet égard. Au Québec, le taux d'utilisation de Facebook est de 64 %[16] et il s'agit du principal média social utilisé pour accéder à de l'information en 2016[17]. Sa popularité, doublée de sa pluralité d'usages, sous-tend un intérêt dual : dans le contexte où une partie importante des personnes ayant des questionnements juridiques ne se retrouvent pas devant les instances formelles de résolution de conflits, les médias sociaux peuvent à la fois être objets de recherche et outils de recherche alors qu'ils ont le potentiel de rendre visibles l'expérience citoyenne avec le droit, et notamment les barrières de compréhension qui peuvent être difficiles à

11 « Médias sociaux et économie de partage en ligne au Québec », *CEFRIO NETendances 2016* 7:9 (2017), en ligne : CEFRIO NETendances 2016 https://cefrio.qc.ca/media/1228/netendances_2016-medias-sociaux-et-economie-de-partage-en-ligne-au-quebec.pdf.

12 Serge Proulx, Mélanie Millette et Lorna Heaton (dir.), *Médias sociaux: Enjeux pour la communication*, Québec, Presses de l'Université du Québec, 2012, p. 2.

13 Suzanne Bouclin et Marie-Andrée Denis-Boileau, « La cyberjustice comme réponse aux besoins juridiques des personnes itinérantes : son potentiel et ses embûches », (2013) 31-1 *Windsor B Access Just* 23, 35.

14 Cassandra Burke Robertson, « The Facebook Disruption: How Social Media May Transform Civil Litigation and Facilitate Access to Justice », (2012) 65 *Ark Rev* 75.

15 Joëlle Kivitz, « Les usages de l'Internet-Santé », dans Christine Thoër et Joseph J. Lévy (dir.), *Internet et santé: Acteurs, usages, appropriations*, Québec, Presses de l'Université du Québec, 2012, p. 37 à la page 39.

16 « Médias sociaux et économie de partage en ligne au Québec », préc., note 11.

17 *Internet pour s'informer et communiquer*, Volume 7-Numéro 7, coll NETendances 2016, CEFRIO, 2017, en ligne : <https://cefrio.qc.ca/fr/enquetes-et-donnees/netendances2016-internet-pour-sinformer-et-communiquer/>.

dégager autrement. En prenant un pas de recul par rapport aux initiatives numériques émanant de la communauté juridique, cette perspective « hors champ » cherche à alimenter la réflexion sur les choix futurs quant à la conception de telles initiatives à travers une documentation des pratiques qui existent déjà sur le terrain[18].

2. UNE PERSPECTIVE CENTRÉE SUR LES USAGES

[4] La volonté d'appréhender la technologie à partir de ses usages par les justiciables invite à centrer notre regard sur les pratiques et les représentations de ces derniers à propos du droit et de la technologie au moyen de méthodes empiriques. C'est ce que permettent de faire les *Legal Consciousness Studies*[19] et la sociologie des usages numériques.

[5] La sociologie des usages suit une tendance selon laquelle, dans les dernières années, les sociologues de la communication et de l'information ont transposé leur intérêt depuis *les effets des technologies sur la société* vers *ce que les individus peuvent faire avec les technologies*[20], un intérêt que l'interactivité du Web social a contribué à renforcer[21]. Étudier les usages d'une technologie consiste à observer, à décrire et à expliquer ce que les individus font avec les dispositifs techniques[22]. L'objectif est de rompre à la fois avec les postures du déterminisme technique et du déterministe social : d'une part, la technologie ne jouit pas d'une autonomie propre et est constamment modelée par l'interaction humaine; d'autre part, toute technologie possède des *affordances* spécifiques qui suggèrent certaines utilisations plutôt que d'autres[23]. Au demeurant, les études d'usages mettent en exergue le fait que les technologies sont des constructions humaines à la fois déterminantes et déterminées et que leur rapport au

18 Au sujet d'une telle approche à la conception des technologies, lire Sasha Costanza-Chock, *Design Justice. Community-Led Practices to Build the Worlds We Need*, Cambridge, MA, MIT Press, 2020.

19 La « conscience du droit » réfère aux manières dont le droit est compris et appliqué par les personnes non socialisées au droit. Ce courant théorique part du principe qu'il est possible d'appréhender le droit non pas seulement à partir de l'étude « *d'un droit qui s'imposerait de facto à la société* », mais « *également à partir de ce que les citoyens font, pensent, voire, dans certains cas, ignorent du droit* » (Jacques Commaille et Stéphanie Lacour, « Les Legal Consciousness Studies comme laboratoire d'un régime renouvelé de connaissance sur le droit », (2018) 100-3 *Droit Société* 547, 551.) Pour une application en contexte technologique, lire Georges Azzaria et Hélène Zimmermann, « Pratiques et représentations des internautes québécois en matière de consentement, de vie privée et de droit d'auteur », *Lex Electron.* 2018.23.1.

20 Notamment à la suite des écrits de Michel de Certeau sur l'usage des techniques : *L'invention du quotidien, I : Arts de faire*, coll. Folio Essais, Paris, Gallimard, 1991.

21 Par exemple, les usagers et usagères des médias sociaux peuvent se conformer aux prescriptions d'usage émanant des concepteurs et conceptrices, mais aussi opérer des stratégies de détournement.

22 Francis Jauréguiberry et Serge Proulx, Usages et enjeux des technologies de communication, Toulouse, Érès, 2011, p. 24.

23 La notion d'affordance renvoie à la capacité d'un objet à suggérer sa propre utilisation : Donald A. Norman, « Affordance, Conventions, and Design », (1999) 6-3 *Interactions* 38.

social est dialectique. Ce faisant, son projet est non pas seulement de décrire l'usage, mais de le replacer dans son contexte social et ainsi de mettre en évidence « la disparité des usages et des usagers en montrant la construction sociale de l'usage »[24]. Ce « déplacement de l'intérêt centré sur la technologie vers les usagers » implique un recours aux méthodologies de types ethnographiques et microsociologiques[25].

[6] Sur ce plan, la volonté de comprendre l'identification de besoins juridiques et l'usage des médias sociaux à cette fin *dans son contexte* requiert d'observer des pratiques – formulation de besoins juridiques et réponses à ces besoins – qui existent déjà dans un environnement donné. C'est pour ces raisons que j'ai eu recours à l'approche ethnographique, qui vise à réaliser une « description dense et détaillée »[26] d'un phénomène social en s'appuyant sur des observations personnelles issues d'une immersion prolongée dans le milieu observé. L'ethnographie en contexte numérique en particulier consiste à utiliser des traces numériques aux fins de l'étude descriptive et analytique des interactions en ligne[27]. Dans un ouvrage séminal sur cette méthode, Christine Hine soutient que la démarcation entre les univers en ligne et hors-ligne serait moins à propos tandis qu'ils se confondent, interagissent et se transforment l'un et l'autre[28]. Ceci implique de faire de l'ethnographie *pour* Internet, ou encore à travers *Internet* plutôt que *de* l'Internet[29], au sens où il est possible d'analyser un phénomène social comme l'accès à la justice à partir de ses manifestations en ligne[30]. En l'espèce, j'ai cherché à prendre le numérique comme un observatoire du social, soit afin de comprendre comment les personnes se démènent dans un contexte des problèmes d'accès à la justice.

24 Florence Millerand, « Usages des NTIC: les approches de la diffusion, de l'innovation et de l'appropriation (2e partie) », (1998) 3-1 *Commposite* 54, 3.

25 *Ibid*., *Commposite* 54, 8.

26 Clifford Geertz, « La description dense. Vers une théorie interprétative de la culture », *Enq. Arch. Rev. Enq.* 1998.6.73.

27 Josiane Jouët et Coralie Le Caroff, « L'observation ethnographique en ligne », dans *Manuel d'analyse du web en sciences humaines et sociales*, 2ème éd, Paris, Armand Colin, 2016, 156.

28 Angela Cora Garcia, Alecea I. Standlee, Jennifer Bechkoff et Yan Cui, « Ethnographic Approaches to the Internet and Computer-Mediated Communication », (2009) 38-1 *J. Contemp. Ethnogr.* 52.

29 Christine Hine, Ethnography for the Internet: Embedded, Embodied and Everyday, Londres, Bloomsbury Academic, 2015.

30 Voir Richard Rogers, *Digital Methods*, Cambridge, MIT Press, 2013. À condition d'en reconnaître les limites, notamment au chapitre des fractures numériques ou tout simplement des personnes qui sont en ligne mais qui n'y interagissent pas publiquement.

[7] J'ai circonscrit le terrain de recherche à deux groupes Facebook[31]. Mon intérêt de recherche pour les interactions entre « profanes » m'a amenée à analyser des groupes (plutôt que des pages ou des comptes personnels) puisque les échanges y sont en principe plus horizontaux. Une veille exploratoire de contenus a permis de délimiter le terrain de recherche à deux groupes accessibles publiquement : un groupe de propriétaires de logements qui échangent leurs questionnements en droit du logement et de l'immobilier (environ 30 000 membres), et un groupe de parents dont les enfants sont pris en charge par la Directrice de la protection de la jeunesse (DPJ) (environ 10 000 membres). Si ces groupes sont à priori très distincts en termes de domaines de droit, mais aussi en termes de profil socioéconomique, leur sélection a permis d'intégrer un volet comparatif à mon analyse[32].

[8] J'ai effectué la collecte de données en deux temps : 1) l'observation de l'ensemble des contributions sur une période de deux mois, jusqu'à saturation, avec prise de notes dans un journal de bord, puis 2) la constitution d'un corpus issu de ces contributions en vue d'analyse (comprenant 210 conversations pour le groupe de propriétaires et 120 pour le groupe de parents, le nombre de commentaires par conversation variant entre 1 et 157). Sur ces deux groupes, des conversations liées à l'information juridique avaient lieu presque tous les jours, allant d'une à treize conversations par jour. Leur format était généralement textuel, mais comportait aussi des hyperliens, des photos, des vidéos, des documents d'information juridique et des modèles rédigés par les internautes[33].

[9] Sur le plan des contenus, sur le groupe de propriétaires, les internautes qui formulent des besoins juridiques vont généralement décrire une situation concernant un locataire et s'enquérir des recours juridiques possibles ou des autres options envisageables. Sur le groupe de parents, on cherche souvent à évaluer si les actes posés par la travailleuse sociale impliquée dans le placement de l'enfant sont légaux

31 Cette étape a été précédée d'une revue de littérature sur trois thèmes : 1) l'accès à la justice et aux services juridiques au Québec ; 2) les solutions déployées en réponse aux problèmes d'accès à la justice dans le contexte où ces solutions sont axées notamment sur l'information juridique et les outils numériques et 3) le cas particulier de l'information juridique sur les médias sociaux.

32 Les familles faisant l'objet d'interventions de la DPJ sont en majorité pauvres ou très pauvres : Québec, Protecteur du citoyen, *Rapport sur la contribution financière au placement des mineurs*, Québec 2013 à la p 15 cité dans Emmanuelle Bernheim, « De petite fille abusée à mère négligente: protection de la jeunesse et matrice de domination », (2015) 27-2 *Can. J. Women Law* 184.

33 Ceci a par exemple permis de faire une analyse de l'information juridique échangée à partir des hyperliens.

et, dans le cas contraire, les recours envisageables, ou encore à se préparer à une audience.

3. LES PRATIQUES INFORMATIONNELLES SUR LES GROUPES FACEBOOK D'INFORMATION JURIDIQUE

[10] L'analyse de l'information partagée sur les groupes révèle que les internautes, lorsqu'ils répondent aux questions juridiques posées, sont à la fois producteurs de contenus inédits (leurs expériences ou leurs opinions) et relayeurs de contenus disponibles ailleurs en ligne. Ces réponses s'appuient ainsi principalement sur trois fondements 1) le recours à des ressources externes (comme des articles d'information juridique ou la législation) ; 2) des opinions (réponses par oui ou non sans précision ou réponse de type directif) et 3) des témoignages expérientiels (des réponses basées sur sa propre expérience avec le droit).

[11] De tels « savoirs d'expérience »[34] relatifs au droit occupent une place importante au sein des pratiques observées. À l'instar des usages de l'Internet santé, il apparaît que les groupes observés permettent aux membres qui ont des questionnements juridiques de rejoindre des personnes qui ont vécu une expérience similaire. Ils mettent ainsi en scène des réseaux de liens faibles[35] de personnes qui partagent des préoccupations similaires et une sympathie mutuelle. Ce faisant, ils facilitent l'accès à des ressources en dehors de son réseau social proche et à des points de vue potentiellement plus nombreux et diversifiés[36]. Afin d'opérationnaliser une telle mise en commun des ressources et des expériences, les internautes capitalisent sur les affordances de *connectivité* des médias sociaux, par exemple la fonctionnalité consistant à « identifier » un individu dans une conversation où il est question d'une situation juridique similaire à une expérience qu'il aurait lui-même vécue.

[12] Or, de telles fonctionnalités de mise en commun opèrent dans un contexte où une forte majorité de questions posées supposent une infinité de réponses possibles, ou à tout le moins un certain niveau d'interprétation. Une typologie des questions posées sur les groupes révèle ainsi la forte présence de questions ouvertes (soit de type *que faire?*

34 Christopher McAll, « Des brèches dans le mur : inégalités sociales, sociologie et savoirs d'expérience », (2017) 49-1 *Sociol. Sociétés* 89.

35 Mark S. Granovetter, « The Strength of Weak Ties », (1973) 78-6 *Am. J. Sociol.* 1360.

36 Dominique Cardon, *Culture numérique*, Presses de Sciences Po, 2019, p. 174.

ou *à quoi m'attendre?*) ou nécessitant une forme d'interprétation (*est-ce que je peux faire ça?*) par opposition aux questions plus circonscrites, qui sont plus ponctuelles (*comment faire?* ou *qu'est-ce que ça veut dire?*). Les questions posées visent souvent à requérir de l'information précise alors que les réponses recherchées supposent la plupart du temps la réalisation de différentes étapes. En effet, les questions formulées de manière plus circonscrite supposent souvent la maîtrise de connaissances juridiques préalables. Sur le groupe de parents, plusieurs questions posées révèlent d'ailleurs que certains internautes ignorent l'existence de certaines lois, comme la *Charte des droits et libertés de la personne*, ainsi que le fait qu'il est possible de les lire les lois en ligne.

[13] À l'instar des questions formulées par les internautes, les réponses apportées comprennent des degrés de précision variés. Par exemple, si certain.es répondent en s'appuyant sur « la loi » ou une loi de manière générale, d'autres réfèrent à un article de loi ou un jugement en particulier, ou encore à un article d'information juridique traitant spécifiquement de la question posée. Si certain.es répondent simplement par oui ou par non, d'autres réponses prennent compte des variables spécifiques à la situation de l'internaute et capitalisent sur plusieurs allers-retours entre les personnes afin d'aboutir à une information personnalisée. Or, l'analyse des réponses sous l'angle de leur degré de précision révèle que les réponses apportées sur le groupe de propriétaires y sont généralement beaucoup plus spécifiques que sur le groupe de parents.

[14] S'il est nécessaire d'analyser les questions et les réponses à l'échelle individuelle pour identifier la nature de l'information partagée, c'est dans un second temps une analyse à l'échelle collective, soit de la structure des conversations elles-mêmes, qui permet de relever les spécificités et les limites des stratégies informationnelles déployées. Ici, les groupes Facebook témoignent d'un processus de mise en commun des différents types d'informations évoquées (ressources, opinions et expériences) permettant la confrontation des différents savoirs théoriques et expérientiels mobilisés au moyen de dynamiques de validation et de contestation de l'information. Lorsque ces modalités de validation, de désaccord, mais aussi de précision, sont juxtaposées, l'information devient une forme de construction collective qui se fonde sur

l'accumulation d'interventions[37]. Autrement dit, c'est la conversation qui devient en soi une information. Ce processus de mise en commun peut par exemple permettre d'estimer ses chances de gain ou encore une fourchette de montants, comme ceux qu'il est possible de s'attendre à verser au locataire dans le cas d'une reprise de logement à la fois à partir du droit applicable et des expériences d'autrui à travers ce que j'appelle un mécanisme de *jurisprudence de l'expérience*. Au demeurant, l'information est co-construite par les internautes, les ressources externes mobilisées et les fonctionnalités du média social favorisant la connectivité.

[15] Les pratiques observées ont manifestement plusieurs limites du point de vue informationnel. Entre autres, les informations erronées ou dé-contextualisées peuvent être publiées et ne pas être effacées même si quelqu'un soulève leur manque de fiabilité. Facebook se distingue en effet des plateformes de *crowdsourcing* spécifiquement destinées à l'agrégation d'information comme Wikipédia pour lesquelles une norme procédurale permet de valider ou d'invalider l'information[38]. Ainsi, lorsqu'un avocat corrige une information sur une vidéo publiée par un internaute, une personne commente sur la même conversation une semaine plus tard « Merci pour le beau vidéo instructif ». Sur le groupe de parents, on peut même parler d'informations erronées qui reviennent de manière ponctuelle sans qu'elles ne soient remises en question par quiconque. Par exemple, un nombre abondant de membres pensent que l'avocat.e de l'enfant est payée ou choisi.e par la DPJ. Or, il s'agit d'un.e avocat.e qui est spécifiquement chargé.e, par le tribunal ou l'enfant lui-même, de conseiller et de représenter l'enfant[39] et qui est rémunéré.e par l'aide juridique[40]. Au-delà de la dichotomie vrai-faux, on relève des affirmations dont la simplification masque certaines nuances ou un

37 Viviane Clavier, M. Caterina Manes-Gallo, Evelyne Mounier, Céline Pagnanelli, Hélène Romeyer et Adrian Staii, « Dynamiques interactionnelles et rapports à l'information dans les forums de discussion médical », dans Florence Millerand, Serge Proulx et Julien Rueff (dir.), *Web social : mutation de la communication*, Québec, Presses de l'Université du Québec, 2010 à la page 300.

38 Florence MILLERAND, Lorna HEATON et David MYLES, « Les reconfigurations sociales de l'expertise sur Internet » François CLAVEAU et Julien PRUD'HOMME, dir, *Experts, sciences et sociétés*, Montréal, Les Presses de l'Université de Montréal, 2018, 153, 158.

39 *Loi sur la protection de la jeunesse*, RLRQ c P-34.1, art. 80. Voir aussi *Code civil du Québec*, RLRQ c CCQ-1991, art. 2135 et *Protection de la jeunesse – 083,* 2008 QCCQ 757.

40 Loi sur l'aide juridique et sur la prestation de certains autres services juridiques, arts 4.1 et 4.7(6); Règlement sur l'aide juridique, RLRQ c A-14, r 2 art. 39.

certain contexte, par exemple lorsque l'on affirme que l'enfant peut décider où il souhaite vivre à partir de douze ans[41].

[16] De manière plus subtile, une limite aux stratégies informationnelles en jeu réside dans le fait que les situations juridiques partagées sur les groupes laissent place à beaucoup d'interprétation. Ainsi, il apparaît parfois impossible de répondre aux questions en raison de la spécificité des faits en jeu, même à la suite de demandes de précision. Parfois, l'émergence d'un désaccord permet de mettre en lumière le fait que chaque situation est différente, ce qui met en lumière les limites liées au fait de mobiliser sa propre expérience. Ces préoccupations font écho aux limites liées à la nature et à la circulation de l'information disponible. Peu structurées et hiérarchisées, les ressources disponibles renverraient à des «*"bundles of facts," while knowledge entails more coherent interpretive packages that contextualize, organize and integrate mere facts* »[42]. Or, en contexte juridique, cet obstacle à l'appropriation de l'information semble se doubler du fait que les informations trouvées à partir de l'expérience des uns ne s'appliquent pas forcément à celle des autres.

[17] Puis, parfois, le collectif n'est pas une limite, mais devient lui-même un facteur de risque sur le plan de la désinformation. Sociologiquement parlant, il faut comprendre l'usage des médias sociaux comme une nouvelle forme de lien social, qui met en lumière de nouvelles manières de construire un réseau d'appartenance[43]. Ici, le lien social encouragé par l'appartenance à un même groupe semble lui-même favoriser une forme d'appartenance à un groupe social plus large, soit les propriétaires de logement et les parents ayant des liens avec la DPJ. Or, cette appartenance sociale semble susciter un biais favorable à la catégorie de personnes qui composent le groupe (propriétaires et parents) et défavorables à d'autres (locataires et DPJ et ses intervenantes ou ses avocat.es), impliquant des biais sur le plan informationnel. Il apparaît

41 Lorsque le tribunal est saisi d'une demande mettant en jeu l'intérêt de l'enfant, celui-ci doit avoir la possibilité d'être entendu si son âge et son discernement le permettent (*Code civil du Québec*, RLRQ c CCQ-1991, art. 34). En matière de garde d'enfant, dès 12 ans, l'opinion de celui-ci est largement déterminante : *Droit de la famille – 07832,* 2007 QCCA 548 (CanLII), au para 28. Or, le juge peut faire primer d'autres facteurs dans l'intérêt de l'enfant. En matière de placement, le tribunal décide des mesures en question et doit prendre une décision dans le meilleur intérêt de l'enfant. L'enfant doit avoir l'occasion d'être entendu et d'être consulté (*Loi sur la protection de la jeunesse*, RLRQ c P-34.1, arts 3, 6-7 et 91 et ss.).

42 Sheldon Ungar, « Misplaced Metaphor: A Critical Analysis of the "Knowledge Society" », (2003) 40-3 *Can. Rev. Sociol.* 331, 337.

43 Antonio Casilli, Les Liaisons numériques. Vers une nouvelle sociabilité?, Paris, Le Seuil, 2010.

toutefois important de préciser que ce phénomène de « bulle de filtre »[44] précède le web social. Ce faisant, les groupes ne sont peut-être que le reflet, ou à tout le moins l'amplificateur, d'une telle tendance plutôt que leur cause[45].

4. LES MÉDIAS SOCIAUX COMME ESPACE DE MISE EN VISIBILITÉ DES INÉGALITÉS DANS L'ACCÈS À L'INFORMATION JURIDIQUE

[18] À l'instar de l'Internet santé, si les échanges en ligne permettent « de confronter des avis différents dans un espace et un temps réduits », cette pratique n'est pas exempte de risques : conseils fragmentaires, illusion de pouvoir les appliquer à toutes les situations, risque de simplification[46] et présence de bulles informationnelles. Les résultats de cette enquête démontrent que certains de ces avantages et risques sont universels aux deux groupes étudiés ; or ils mettent également en lumière certaines disparités entre les pratiques observées et, de ce fait, certaines inégalités préexistantes en termes d'accès à la justice, y compris à l'information juridique.

[19] Selon Josiane Jouët, « la seule médiation de la technique paraît souvent impuissante à créer du lien social ». Ce lien social se ressource dans des facteurs sociaux préexistants, à commencer par « des réseaux sociaux préconstruits »[47]. Si les médias sociaux « permettent d'élargir la sociabilité de proximité à la périphérie des relations plus distantes »[48], la périphérie de ces liens faibles se bute à ses propres frontières. Pour danah boyd, les médias sociaux ont tendance à reproduire et à magnifier une certaine « homophilie » des réseaux sociaux préexistants : « *In a networked world, people connect to people like themselves. What flows across the network flows through edges of similarity*. » Or, « *[i]nformation can and does flow*

44 Ce terme réfère à la personnalisation croissante du Web alimentée par des moyens algorithmique : Eli Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin Books Limited, 2011.

45 Adrien Sénécat, « Dominique Cardon : « Ce ne sont pas les réseaux sociaux qui ont créé des bulles informationnelles » », *Le Monde* (21 octobre 2018). Cependant, l'algorithme du fil de nouvelles de Facebook aurait augmenté cet effet de bulle de filtre (E. Pariser, préc., note 44.).

46 Christine Bruchez, Maria Del Rio Carral et Marie Santiago-Delefosse, « Coconstruction des savoirs autour des contraceptifs dans les forums de discussion sur Internet », dans Joseph J. Lévy, Christine Thoër et Bertrand Lebouché (dir.), *Médias, médicaments et espace public*, Québec, Les Presses de l'Université du Québec, 2009, p. 245, 265-266.

47 Josiane Jouët, « Retour critique sur la sociologie des usages », (2000) 18-100 *Réseaux* 487, 506–507.

48 D. Cardon, préc., note 36, p. 173.

in ways that create and reinforce social divides. »[49] En l'espèce, il apparaît qu'au sein des groupes, les disparités préexistantes, en termes de compréhension du droit, mais aussi de réseau social, ont un impact sur l'appropriation de l'information. Par conséquent, les groupes semblent plus utiles sur le plan informationnel aux personnes qui ont des connaissances préalables sur le droit, mais surtout qui disposent d'un accès à un réseau social de personnes susceptibles d'avoir de telles connaissances. Le groupe traduit lui-même la présence d'un réseau social, qu'il contribue à reproduire malgré l'augmentation de la densité de liens faibles.

[20] Ensuite, il convient de mettre en relation de telles disparités avec la littérature sur l'accès à l'information juridique et l'accès à la justice plus généralement. Selon Patricia Hugues, le déploiement de solutions standardisées, notamment en matière d'information juridique, risque de constituer un vecteur d'exclusion supplémentaire pour les personnes marginalisées[50]. Si les groupes Facebook ne font pas partie de ces ressources, ils mettent en scène le partage et l'interprétation de plusieurs d'entre elles par les internautes. Certes, les résultats démontrent que ce ne sont pas seulement les personnes et groupes dits vulnérables qui ont de la difficulté à comprendre et appliquer l'information. Cela dit, l'effet collectif du groupe atténue ces difficultés dans le cas du groupe de propriétaire et contribue autrement à reproduire les inégalités dans l'accès à l'information dans le groupe de parents. À la lumière de tels résultats, je propose que la recherche en ligne a le potentiel de rendre visibles certaines conséquences des inégalités dans le rapport à la justice. Car si Internet reflète et magnifie les dynamiques sociales préexistantes, il permet aussi de les rendre plus visibles selon Danah Boyd :

> *One of the reasons why people fear the technologies we make are because they make thing visible that we don't like. [...] I invite you to think about visibility. What can you see that you couldn't before? How does this make you feel? And what are you going to do about it?*[51]

Quelles en sont les implications en matière de recherche et d'action sur l'accès à la justice ? D'abord, une « vision étendue » de l'accès à la justice

49 « Streams of Content, Limited Attention: The Flow of Information through Social Media », *Web 2.0 Expo*, New York, 17 novembre 2009, p 3.

50 Patricia Hughes, « Advancing Access to Justice through Generic Solutions: The Risk of Perpetuating Exclusion », (2013) 31 *Windsor B Access Just* 1, 12.

51 Danah Boyd, *Do you See What I See?: Visibility of Practices through Social Media*, San Francisco et Paris, Supernova et Le Web, et 10 décembre 2009 à la p 4, en ligne : http://www.danah.org/papers/talks/2009/SupernovaLeWeb.html.

appelle à tenir compte des disparités entre les groupes sociaux au moment d'échafauder des réponses technologiques et à ne pas présumer que les initiatives qui aident certains groupes sont universellement bénéfiques[52]. Ensuite, une telle vision impose davantage de recherche sur l'usage des technologies de cyberjustice par des groupes divers, notamment marginalisés. Or, à la lumière de mes conclusions, il apparaît nécessaire d'inclure également les réseaux informels d'accès à du soutien juridique – soit la cyberjustice informelle[53] – à ce cadre d'analyse « étendu » afin de dégager une meilleure compréhension des bénéfices, risques et limites en jeu, en particulier au prisme des possibilités méthodologiques des médias sociaux de dévoiler des inégalités préexistantes.

[21] En définitive, j'espère avoir démontré que les études d'usage permettent de mettre en lumière le caractère à la fois déterminant et déterminé des technologies. Au même titre que le droit, la technologie opère une « mystification » à l'égard des profanes au sens où ces derniers ne peuvent expliquer comment elle a produit un résultat donné[54], impliquant une forme de « réification »[55] de la technique, et notamment de l'espace virtuel[56]. Pourtant, comme l'affirmait Pierre Bourdieu à propos du droit, il n'est pas trop dire que la technologie fait le monde social, mais à condition de ne pas oublier qu'elle est faite par lui[57]. La technologie n'opère pas dans le vide social, mais elle interfère avec des pratiques existantes[58], ce qui lui permet tantôt de magnifier, tantôt de rendre visible des phénomènes sociaux préexistants. Comme le droit, la technologie suppose des usages prescrits, mais aussi des usages détournés, rappelant l'importance d'étudier comment les individus et les groupes utilisent ou n'utilisent pas ce droit et cette technologie. J'espère ainsi avoir démontré que les études d'usages revêtent un potentiel intéressant pour d'explorer les rapports dynamiques entre droit, technologie et société. Comme l'a fait la recherche socio-juridique avec le droit, peut-être devient-il incontournable de penser le numérique et son cadre juridique

52 J. Bailey, J. Burkell et G. Reynolds, préc., note 7, p. 183.

53 S. Bouclin et M.-A. Boileau, préc., note 13, p. 35.

54 Pierre Bourdieu, « La force du droit : Eléments pour une sociologie du champ juridique », (1986) 64-1 *Actes Rech. En Sci. Soc.* 3.

55 Patricia Ewick et Susan S. Silbey, *The Common Place of Law. Stories From Everyday Life*, Chicago, University Of Chicago Press, 1998, p. 91-93.

56 Madeleine Pastinelli, « Pour en finir avec l'ethnographie du virtuel !: Des enjeux méthodologiques de l'enquête de terrain en ligne », (2011) 35-1–2 *Anthropol. Sociétés* 35, 43.

57 P. Bourdieu, préc., note 57, p. 13.

58 Florence Millerand, « Usages des NTIC: les approches de la diffusion, de l'innovation et de l'appropriation (1ère partie) », (1998) 2-1 *Commposite* 1.

non pas selon le prisme d'une technologie qui s'imposerait de facto à la société, mais plutôt celui d'une technologie *en* société, activée par les acteurs sociaux.

VULNÉRABILITÉS + CONTRAT ÉLECTRONIQUE : L'EXEMPLE DU CONSENTEMENT ÉLECTRONIQUE

Ledy Rivas ZANNOU[1]

1 L'auteur est candidat au doctorat en droit des technologies nouvelles à la Faculté de droit de l'Université de Montréal. Il assume actuellement, les fonctions de coordonnateur de la Chaire L.R. Wilson en droit des technologies de l'information et du commerce électronique.

Résumé

L'appréhension juridique du consentement en tant que pilier du contrat électronique s'est faite sans égard aux spécificités propres au medium grâce auquel se nouent les relations contractuelles. Faisant suite à ce constat, il sera question dans cette contribution d'analyser le décalage entre la conception législative ou théorique du consentement électronique avec la réalité pratique de son expression dans le contrat électronique. Ainsi, nous évaluerons la place du « vouloir » en mettant en perspective les obstacles qui menacent son intégrité. Une fois cet état des lieux établi, nous prospecterons les avenues possibles afin que le consentement exprimé puisse émaner effectivement de la volonté du contractant c'est-à-dire ; qu'il le manifeste en toutes connaissances de cause.

INTRODUCTION

[1] Autonomie de la volonté et contrat électronique. Substrat de la théorie de l'autonomie de la volonté[2] – fortement portée par la doctrine – qui est à l'origine du consensualisme, le consentement occupe une place de choix dans la formation du contrat. Très tôt, le législateur a cru bon lui accorder une place prépondérante dans la formation du contrat à tel point qu'il l'a soumis à certaines conditions de validité[3]. En tant que pilier du contrat, le consentement est donc un précepte juridiquement appréhendé[4] dont la conception théorique a été systématiquement transposée dans le contrat électronique suivant le principe d'équivalence fonctionnelle[5].

[2] Problématique. Cette approche fait fi des complexités techniques que recouvre l'environnement numérique car si la réalité dans l'univers du papier peut permettre de garantir facilement l'intégrité du consentement, tel n'est pas le cas dans l'univers du numérique. Les modalités de conclusion du contrat électronique diffèrent[6] et point n'est besoin de préciser que celles de l'expression du consentement changent avec elles[7]. En considération de l'environnement de conclusion et des modalités d'expression du consentement, il sied de s'interroger sur la qualité et les effets du consentement sous le prisme des vulnérabilités auxquelles s'expose celui qui consent.

[3] Plan. C'est pourquoi notre contribution tentera de mettre en perspective les éléments qui entravent la garantie d'un consentement électronique de qualité (**1**) en proposant les avenues possibles à explorer

---

2 Pour rappel, voir Aurélien Bamdé, « L'autonomie de la volonté », *A. Bamdé & J. Bourdoiseau* (12 septembre 2016), en ligne : <https://aurelienbamde.com/2016/09/12/lautonomie-de-la-volonte/> (consulté le 10 mai 2020).

3 Sur la qualité du consentement, voir principalement les dispositions de l'article 1399 du Code civil du Québec et les articles 1407 et 1408 du même code en ce qui concerne la théorie des vices du consentement. Les développements doctrinaux sont aussi édifiants à ce sujet : Didier Lluelles et Benoît Moore, *Droit des obligations*, 2e éd., Montréal, Éditions Thémis, 2012, p. 253–470.

4 Sur la qualité du consentement, voir principalement les dispositions de l'article 1399 du Code civil du Québec et les articles 1407 et 1408 du même code en ce qui concerne la théorie des vices du consentement. Les développements doctrinaux sont aussi édifiants à ce sujet : Didier Lluelles et Benoît Moore, *Droit des obligations*, 2e éd., Montréal, Éditions Thémis, 2012, p. 253–470.

5 Pour davantage de développement sur ce concept, voir ce concept Marie DEMOULIN, *Droit du commerce électronique et équivalents fonctionnels: théorie critique*, Bruxelles, Larcier, 2014.

6 M. Ethan KATSH, *Law in a digital world*, New York, New York; Toronto, Oxford University Press, 1995, p. 129. L'auteur nous rappelle que : paper contract is an act ; electronic contract is a process. Autrement dit, les modalités de conclusion des contrats électroniques répondent d'un processus soumis à un formalisme établi par le législateur.

7 Voir sur les modalités d'extériorisation du consentement : Akodah AYEWOUADAN, *Les droits du contrat à travers l'internet*, Bruxelles, Éditions Larcier, 2013, p. 72 et s. En effet, celles-ci procèdent d'une technique exclusive qui s'appuie sur un processus déterminé à savoir : le premier clic qui permet de corriger et de valider la commande et le deuxième clic qui vient confirmer la volonté du contractant.

pour effectivement assurer au contractant-consommateur les conditions d'une expression du consentement non entachée ou à la hauteur de sa confiance (**2**) sachant qu'il ne négocie pas les termes contractuels[8].

1. DU CONSENTEMENT SANS « VOULOIR »[9]… : LES OBSTACLES AU CONSENTEMENT ÉCLAIRÉ

[4] « Vouloir » et pratique contractuelle. La pratique du contrat électronique offre une belle perspective pour apprécier la place de la volonté dans l'expression du consentement électronique. En effet, elle permet d'observer les formes nouvelles qu'adoptent le consentement sans égard à la conception théorique et législative du consentement qui postule que toute manifestation de volonté, fut-elle électronique, doit être de qualité c'est-à-dire qu'elle représente réellement la volonté de chaque partie et qu'elle respecte leur intelligence[10]. Cette affirmation se vérifie-t-elle dès lors qu'on considère l'inflation informationnelle[11] à laquelle le contractant doit faire face (**1.1**) ainsi que les modalités communicationnelles ne garantissant pas la prise de connaissance effective des informations (**1.2**) ?

1.1. UN « VOULOIR » SUBMERGÉ PAR L'INFLATION INFORMATIONNELLE

[5] Symétrie informationnelle et formalisme informatif. En formalisant l'obligation précontractuelle d'information, le législateur a

8 Par choix, nous ne reprendrons pas ici toute la problématique relative aux contrats d'adhésion sachant que leur admission est acquise en droit surtout dans la pratique du commerce électronique où ils sont souvent utilisés. Pour plus de développement sur les contrats d'adhésion, voir Brigitte Lefebvre, « Le contrat d'adhésion », (2003) 105 *Revue du Notariat*, en ligne : <LEFEBVRE Brigitte, « Le contrat d'adhésion » dans Le Code civil du Québec : Bilan d'une décennie 1994-2004, (2003) 105 R. du N. 439-490.,> (consulté le 10 janvier 2019); Gaël Chantepie, Mathias Latina et Vincent Caron, *Le contrat d'adhésion: perspectives franco-québécoises*, coll. Thèmes & commentaires. Actes, Paris, Dalloz, 2018.

9 Voir notamment, Marie-Anne Frison-Roche, « Remarques sur la distinction de la volonté et du consentement en droit des contrats », (1995) 3 *RTD civ.*, 573, en ligne : <http://mafrisonroche.phpnet.org/IMG/pdf/2-2.3_volont_consentement_1995.pdf> (consulté le 15 mai 2020). Le choix d'un tel titre trouve sans doute sa justification dans la précision suivante : « Il faut se rappeler et tirer tout profit du fait que volonté et consentement ne peuvent se réduire l'un à l'autre, qu'échange et rencontre ne doivent pas s'assimiler. La volonté est au cœur de l'humanisme et marque l'intériorité incommensurable de l'homme tandis que le consentement est un objet conséquence de la volonté, symbole et extériorisation de la volonté, mais distinct de la volonté. ».

10 Voir sur la qualité ou l'intégrité du consentement, D. Lluelles et B. Moore, préc., note 3, p. 253–471.

11 Pour en savoir davantage sur la description et l'analyse du formalisme informatif du contrat électronique, voir Vincent GAUTRAIS, « Le nouveau contrat à distance et la Loi sur la protection du consommateur », dans *Le droit de la consommation sous influences*, Cowansville, Québec, Éditions Yvon Blais, 2007 aux pages 122–125 ; En analysant la portée matérielle de l'obligation précontractuelle d'information, les auteurs dénoncent la surcharge informationnelle : Serges Kablan et Arthur Oulaï, « La formalisation du devoir d'information dans les contrats de cyberconsommation : analyse de la solution québécoise », (2009) 54-4 *McGill Law Journal* 627–668, 631–648.

voulu garantir une symétrie informationnelle[12] entre le professionnel et le contractant-adhérent. L'objectif d'un tel formalisme étant d'éclairer le consentement de la partie contractante en la plaçant au même niveau informationnel que le professionnel. Cependant, cet objectif ne semble pas atteint puisque la quantité d'informations à digérer par celui-ci est considérable.

[6] Quantité informationnelle *Vs*. qualité informationnelle. S'il y a un reproche qu'on pourrait formuler à l'encontre du formalisme informatif, c'est bien celui de la profusion d'informations car, en postulant que celle-ci suffisait à garantir l'information du contractant-adhérent, le législateur a cédé à l'illusion conceptuelle[13] selon laquelle la formalisation permettrait au consommateur d'être mieux armé et protégé[14]. Or, il n'en est rien, car le « trop » est l'ennemi du bien[15]. Il en résulte donc de nombreuses pathologies[16] telles que la surcharge informationnelle[17], la pertinence limitée de certaines mentions et la dilution sous-jacentes. Ce faisant, le contractant-adhérent ploie sous le poids d'une quantité informationnelle sachant que celle-ci est censée éclairer son consentement au contrat. Manifestement, c'est tout le contraire qui se

12 Voir les développements des auteurs sur l'objectif de l'obligation d'information précontractuelle : Jean CALAIS-AULOY et Henri TEMPLE, *Droit de la consommation*, 9e édition, coll. Précis. Droit privé, Paris, Dalloz, 2015, p. 61-62 ; Voir également, Guy Raymond, *Droit de la consommation*, 5e éd., coll. Droit & professionnels : droit commercial, 2119-3169, Paris, LexisNexis, 2019, p. 227-228.

13 En ce qui concerne les critiques sur le formalisme informatif, voir Vincent GAUTRAIS, « Le nouveau contrat à distance et la Loi sur la protection du consommateur », dans *Le droit de la consommation sous influences*, Cowansville, Québec, Éditions Yvon Blais, 2007, p121-131; Mustapha MEKKI, « Le formalisme électronique : la « neutralité technique » n'emporte pas « neutralité axiologique » », (2007) 3 *RDC*, 681; Agathe LEPAGE, « Les paradoxes du formalisme informatif », dans *Études de droit de la consommation : Liber amicorum Jean Calais-Auloy*, Dalloz, Paris, Dalloz, 2004, p. 597–620.

14 Pierre-Claude Lafond, « Pour en finir avec la liberté contractuelle du consommateur », (2013) 47-1 *Revue Juridique Thémis*, 10.

15 Charlaine BOUCHARD et Marc LACOURSIÈRE, « Les enjeux du contrat de consommation en ligne », (2003) 33-3 *R.G.D* 373–438, 395, doi : https://www.erudit.org/fr/revues/rgd/2003-v33-n3-rgd01599/1027421ar/. Les auteurs rappellent qu'un consommateur trop informé est aussi un consommateur mal informé; Voir également : Vincent GAUTRAIS et Mouhamadou SANNI YAYA, *Rapport relatif aux changements à opérer auprès de la Loi sur la protection du consommateur au regard du commerce électronique*, Montréal, Chaire UDM en droit de la sécurité et des affaires électroniques, 2008, p. 17–18, en ligne : <https://www.gautrais.com/publications/rapport-relatif-aux-changements-a-operer-aupres-de-la-loi-sur-la-protection-du-consommateur-au-regard-du-commerce-electronique/rapportfinal31082008v2/> (consulté le 26 juillet 2019). Ils rappellent que trop d'informations tue l'information.

16 Pour en savoir davantage sur les pathologies informationnelles, voir les travaux de Vincent GAUTRAIS, « L'encadrement juridique du cyberconsommateur québécois », dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002 à la page 268 ; Vincent GAUTRAIS et Mouhamadou SANNI YAYA, *Rapport relatif aux changements à opérer auprès de la Loi sur la protection du consommateur au regard du commerce électronique*, Montréal, Chaire UDM en droit de la sécurité et des affaires électroniques, 2008, en ligne : <https://www.gautrais.com/publications/rapport-relatif-aux-changements-a-operer-aupres-de-la-loi-sur-la-protection-du-consommateur-au-regard-du-commerce-electronique/rapportfinal31082008v2/> (consulté le 26 juillet 2019) ; Vincent GAUTRAIS, « Réécrire l'écrit », dans Alain PRUJINER et Sylvette GUILLEMARD, *Mélanges en l'honneur du professeur Alain Prujiner : Études de droit international privé et de droit du commerce international*, coll. CÉDÉ, Cowansville, Québec, Éditions Yvon Blais, 2011, p. 113–141 ; Vincent Gautrais, « Rapport québécois aux journées internationales Henri Capitant, « Contrat et immatériel », Journées espagnoles, Barcelone, (05/2014) »,, en ligne : <https://www.gautrais.com/publications/1370/> (consulté le 10 septembre 2019) ; Vincent GAUTRAIS, « Contrat électronique : plus de 20 ans certes mais pas encore adulte », dans *Études en l'honneur du Professeur Jérôme Huet*, Issy-les-Moulineaux, France, LGDJ, Lextenso éditions, 2017

17 Serges KABLAN et Arthur OULAÏ, « La formalisation du devoir d'information dans les contrats de cyberconsommation : analyse de la solution québécoise », (2009) 54-4 *McGill Law Journal*, 636.

produisit. Le choix de la qualité informationnelle aurait permis d'exiger du professionnel les informations essentielles.

[7] Inflation informationnelle et consentement. La fonction informative qui est assignée au formalisme informatif peut-elle se réaliser et déterminer le consentement du contractant-adhérent ? À l'évidence, la réponse est négative tant la doctrine foisonne sur les risques évidents de lourdeur[18] ainsi que le leurre[19] que pourraient occasionner une telle inflation. Or, l'établissement d'un formalisme informatif présuppose non seulement de la correction d'un déséquilibre situationnel entre les parties mais également, de la nécessité d'éclairer le consentement qui sera donné à la conclusion du contrat. Cette prise en otage[20] du consentement par la surcharge informationnelle illustre la vulnérabilité du contractant-adhérent malgré la bonne volonté du législateur qui a cru par ce mécanisme, pouvoir garantir l'intégrité du consentement. Outre l'inflation informationnelle, il y a aussi la communication contractuelle qui menace l'intégrité du consentement

1.2. UN « VOULOIR » MENACÉ PAR LA COMMUNICATION CONTRACTUELLE

[8] Spécificités techniques et communication contractuelle. L'œuvre de compensation[21] entre les supports papier et numérique s'est réalisé par le truchement des principes de neutralité technologique[22] et d'équivalence fonctionnelle[23]. Par ailleurs, dès lors qu'on interroge cette œuvre de compensation à la lumière du contrat électronique, on peut s'apercevoir qu'elle n'a pas totalement intégré les complexités entre les spécificités techniques du medium Internet et la communication contractuelle. Plusieurs éléments que nous présenterons ci-dessous illustrent bien ce constat.

[9] Communication informationnelle et hyperliens. Si la lettre de l'article 54.4 in fine fait obligation au commerçant de présenter les

18 Pierre-Yves GAUTIER, « L'équivalence entre supports électronique et papier, au regard du contrat », dans *Droit et technique : études à la mémoire du professeur Xavier Linant de Belle*˜ *fonds*, Paris, Litec, 2007 à la page 195.

19 M. MEKKI, préc., note 13, 681.

20 Voir en effet : M.-A. FRISON-ROCHE, préc., note 9, 575.

21 Voir les développements de Vincent GAUTRAIS, Le contrat électronique international: encadrement juridique, 2e éd. rev., Louvain-la-Neuve, Bruylant-Academia, 2002.

22 Voir Vincent GAUTRAIS, Neutralité technologique: rédaction et interprétation des lois face aux changements technologiques, Montréal, Éditions Thémis, 2012.

23 Pour en savoir davantage sur ce principe : M. DEMOULIN, préc., note 5.

renseignements de manière évidente et intelligible et les porter expressément à la connaissance du consommateur[24] (nos soulignements), il est fréquent d'observer que la divulgation des informations se fait dans la pratique du commerce électronique au moyens des hyperliens. Si cette modalité communicationnelle semble acquise, elle est tout de même porteuse de déliement contractuel [25]puisque les hyperliens induisent des voyagements vers des ailleurs – sortie, détour et retour – dans le texte électronique. Bien que la Cour suprême du Canada ait décidé dans l'affaire *Dell*[26] qu'ils font partie intégrante du contrat, il convient de rappeler qu'ils soumettent à rude épreuve, l'attention[27] du contractant-adhérents dans la prise de connaissance effective des informations.

[10] Lisibilité et visibilité. Les qualités de lisibilité varient d'un support à un autre. Or, en contexte électronique, l'écran n'offre pas le même confort de lisibilité[28] et de visibilité[29] qu'une page papier[30] et la pratique de la lecture[31] dans un tel environnement est singulière et dynamique. En effet, la typographie des clauses ou informations – taille, police, espacement, etc. – sur l'écran ne facilite pas une lecture pouvant garantir une prise de connaissance effective et, leur disposition ou affichage sur l'écran n'y participe pas également.

[11] Longueur et juridisme du contrat. En tant qu'outils de communication, il est loisible de remarquer que les documents contractuels sont exagérément longs sachant que leur reproduction sur

---

24 Loi sur la protection du consommateur, RLRQ c P-40.1.

25 Stéphane LARRIÈRE, « Contrat et hypertexte: l'hyperlien qui délie ? », *La Loi des Parties*, sect. En pratique (19 novembre 2017), en ligne : <http://laloidesparties.fr/contrat-hyper-texte> (consulté le 30 décembre 2019).

26 *Dell Computer Corp. c. Union des consommateurs*, [2007] CSC 34, 2007 2 R.C.S. 801, 284 D.L.R. 577 [*Dell* avec renvois aux R.C.S.].

27 Vincent GAUTRAIS, « Les contrats de cyberconsommation sont presque tous illégaux ! », 2005, 625, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/1357> (consulté le 25 janvier 2020). L'auteur met l'accent sur le risque de distraction que pourrait générer les hyperliens.

28 Marshall McLUHAN, *Pour comprendre les médias: les prolongements technologiques de l'homme*, coll. Collection Points. Essais, n°83, Paris, Éditions Points, 2015, p. 26–40. Sans adhérer au point de vue extrême de l'auteur qui affirme que le message c'est le médium, nous observons tout de même que le médium a une influence sur le message et que par conséquent, il s'agit de deux entités interdépendantes.

29 Il convient de rappeler que les propriétés du texte affiché sur un écran subissent ainsi une série de transformation spatiales et temporelles qui en modifient la perception. Voir à cet effet, Thierry BACCINO, *La lecture électronique*, coll. Sciences et technologies de la connaissance, Grenoble, Presses universitaires de Grenoble, 2004, p. 71.

30 Claire BÉLISLE, « Du papier à l'écran : Lire se transforme », dans *Lire dans un monde numérique*, coll. Papiers, Villeurbanne, Presses de l'Enssib, 2017, p. 112–162, en ligne : <http://books.openedition.org/pressesenssib/1091> (consulté le 8 avril 2020).

31 Anthony GRAFTON, *La page, de l'Antiquité à l'ère du numérique: histoire, usages, esthétiques*, coll. La Chaire du Louvre, Paris, Hazan : Louvre éditions, 2012, p. 28. L'auteur en fait la description suivante : « [le lecteur] regarde d'abord latéralement le haut de la page, [il] descend ensuite rapidement le long de la marge gauche, puis [il] lit en travers à nouveau avant de continuer à descendre le long de la marge gauche ».

support papier s'étalerait sur plusieurs centaines de pages[32]. En effet, la longueur du contrat électronique rebute voire « répugne » de sorte que peu de contractant-consommateur le lisent[33] avant de consentir. À cela s'ajoute l'hyper-technicité de la grammaire juridique utilisée par les cybercommerçants. En d'autres termes, la qualité rédactionnelle laisse à désirer puisque la compréhension n'est pas toujours aisée dès lors qu'on considère la littératie des personnes qui contractent.

[12] Communication contractuelle et « vouloir ». Une petite précaution s'impose puisque notre propos ne compte pas reprendre les développements sur l'évolution de la manifestation du consentement contractuel en matière électronique[34]. De ce qui précède, le vouloir est quasiment absent – dans de telles conditions en tout cas – du consentement devenu mécanique par le conditionnement des spécificités techniques et ergonomiques du medium au moyen duquel il est exprimé. Ainsi, la question de son intégrité – au sens d'absence d'altération quelconque – est posée dès lors qu'on considère le vouloir dans le consentement comme un élément protecteur pour la partie qui la manifeste. C'est pourquoi, il serait difficile de soutenir que le consentement du contrat électronique résulte du vouloir et qu'il est exprimé en parfaite connaissance de cause. Les contingences inhérentes aux spécificités techniques du medium – bien qu'étant extra-juridiques – ainsi que les pratiques contractuelles désincarnées[35], renseignent suffisamment sur les vulnérabilités auxquelles s'exposent le contractant-adhérent. Il est clair que celles-ci n'ont pas été considérées dans la conception originelle du consentement électronique qui déifie un vouloir qui n'a d'existence que dans l'imaginaire du législateur. Face à un tel constat, quelles avenues pourrait-on explorer pour que le consentement électronique traduise véritablement le vouloir de celui qui l'exprime ?

32 V. GAUTRAIS, préc., note 27, 5.

33 Voir les résultats de l'enquête menée par Georges AZZARIA et Hélène ZIMMERMAN, « Pratiques et représentations des internautes québécois en matière de consentement, de droit à la vie privée et de droit d'auteur », *Lex Electronica* 2019.24, 17–18, en ligne : <https://lexelectronica.openum.ca/files/sites/103/Lex_24_Azzaria_Zimmermann_1_VF-1.pdf> (consulté le 5 mars 2020).

34 Voir les développements et références bibliographiques proposés par V. GAUTRAIS, préc., note 4 aux pages 87–96.

35 Au sujet de la désincarnation des pratiques contractuelles, voir la conférence introductive prononcée par le Professeur Vincent GAUTRAIS intitulée : « La mort du consentement numérique : acharnement thérapeutique ou aide médicale à mourir ? » lors de la table ronde sur : **La mort du consentement numérique ?**, en ligne : https://www.lesconférences.ca/videos/la-mort-du-consentement-numerique-contrat/ (consulté le 14 mai 2020).

2. … AU « VOULOIR » AVEC CONSENTEMENT : PLAIDOYER POUR UNE RÉINVENTION CONTEXTUELLE

[13] Quelles avenues pour réinventer le « vouloir » ? Par choix, nous n'engagerons pas le débat de l'abrogation[36] du vouloir car, ce n'est pas l'objectif de notre propos. Nous insisterons plutôt sur ce qu'il faudrait faire pour réhabiliter le vouloir qui, est de moins en moins considéré comme étant la force obligatoire du contrat[37] électronique. Sans ambages, il sied de reconsidérer la conception du consentement de manière à ce que le vouloir puisse effectivement le déterminer. Pour ce faire, quelques avenues peuvent être explorées pour cette réinvention contextuelle dans laquelle, la technologie (**2.2**) prendra une part active. Aussi, le dynamisme de l'environnement numérique doit être considérée dans la formulation de l'exigence légale informationnelle (**2.1**). Ainsi, la réinvention du « vouloir » peut s'opérer en alliant à la fois, l'exigence de sécurité juridique avec les « réalités » techniques et technologiques. Sans prétention d'exhaustivité, nous présenterons les modalités d'une telle réinvention.

2.1. UN « VOULOIR » ADAPTÉ AU DYNAMISME NUMÉRIQUE

[14] « Vouloir » aseptisé. La quantité informationnelle du formalisme informatif est en cause et il serait intéressant que les informations non utiles ou nécessaires à la compréhension et à la connaissance du bien ou du service soient éliminées de la liste des informations obligatoires. En d'autres termes, seuls les informations essentielles doivent être requises afin de faire immerger le « vouloir » du contractant-adhérent. Cette aseptisation ne doit pas être que cosmétique mais audacieuse et l'initiative peut d'ailleurs provenir des professionnels eux-mêmes puisque cela s'inscrirait dans une perspective de « marketing contractuel »[38]. Plus la qualité informationnelle sera privilégiée par les acteurs du commerce électronique, mieux le contrat électronique guérira de son « obésité » nuisible au consentement. La modalité d'une telle aseptisation peut s'envisager au moyen des pictogrammes résumant chacune des étapes en référence aux clauses essentielles[39]. D'ailleurs, une approche similaire est

36 Pour en savoir davantage sur l'abrogation du « fétichisme consensuel », voir BROWNSWORD R., « The Cult of Consent : Fixation and Fallacy » KCLJ, 2004, 15, 223-224. Cité par V. GAUTRAIS, préc., note 16 à la page 203.

37 V. GAUTRAIS, préc., note 21, p. 21–80.

38 Vincent GAUTRAIS, préc., note 27, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/1357> (consulté le 25 janvier 2020).

39 Voir les références en rapport avec cette solution dans V. GAUTRAIS, préc., note 15 à la page 205.

déjà effective dans les six licences prévues par *Creative Commons*[40] sachant que celle-ci peut être inspirante dans la pratique du contrat électronique.

[15] « Vouloir » *designé*. Un constat d'ordre général s'impose : la manifestation du consentement dépend en partie de la communication contractuelle qui, mérite d'être repensée sur certains aspects. En ce sens, il est important de réviser la structure de présentation en recourant au « *design by conception* » du vouloir. Ce faisant, on pourrait par exemple exiger des professionnels de simplifier leur contrat en référant aux normes[41] de lisibilité et de clarté. Les objectifs communicationnels de l'information divulguées devront être clairement définis[42] dès leur conception afin qu'ils répondent aux configurations des interfaces numériques. Cela supposerait donc de travailler sur des standards conformes à l'architecture[43] et au *design* interactif[44] de l'information en prenant appui par exemple sur la technologie calme[45]. Ainsi, l'ergonomie de l'écran – support par excellence du medium – sera considérée dans la présentation des informations, du document ou des termes contractuels pour faciliter leur visibilité et leur lisibilité.

[16] « Vouloir » humanisé. Dans l'optique d'humanisation, le recours à la communication multimodale des termes contractuels peut être envisagé. Cette solution trouve sa justification dans le taux élevé d'analphabétisme fonctionnel, qui est d'environ 53%[46] au Québec, sachant que ces personnes contractent et manifestent leur consentement en ligne. Dès lors, il serait concevable de « traduire » vocalement[47] le contrat au moyen des technologies d'assistance vocale en s'inspirant des normes et

40 Pour en savoir davantage sur l'approche, voir en ligne : [https://creativecommons.fr/licences/] (consulté le 15 mai 2020).

41 Nous pensons ici à l'article 1436 du Code civil du Québec et l'article 25 de la Loi sur la protection du consommateur.

42 Voir les recommandations relatives aux objectifs communicationnels : Stéphanie ROY, Clément CAMION et Éducaloi, « Des contrats clairs et utiles pour les consommateurs : vers un nouveau standards », dans Pierre-Claude LAFOND et Vincent GAUTRAIS (dir.), *Le consommateur numérique : une protection à la hauteur de la confiance ?*, Montréal, Éditions Yvon Blais, 2016 aux pages 55–59.

43 Alessandra PONTE, *Architecture et information 2.0. 2018*, Montréal, Québec, École d'architecture, Faculté de l'aménagement, Université de Montréal, 2018; Jean-Michel SALAÜN et Benoît HABERT (dir.), *Architecture de l'information: méthodes, outils, enjeux*, coll. Information & stratégie, Louvain-la-Neuve, De Boeck, 2015.

44 Benoît DROUILLAT, Le design interactif: du web design aux objets connectés, Paris, Dunod, 2016.

45 Voici la définition qui en est donnée : « La technologie calme désigne le caractère non-intrusif d'un dispositif. La technologie calme permet de réduire le bruit de la surcharge informationnelle dans une interface en laissant l'utilisateur définir quelle est l'information à placer au centre de son attention et quelle est l'information à laisser en périphérie ». APCI et Designers interactifs, *Le design des interfaces numériques en 170 mots-clés : Des interactions Homme-Machine au design interactif*, Dunod, 2013, p. 138–139.

46 Bien que plusieurs voix se soient levées pour dénoncer le caractère abusif, réducteur et autocentré de ce pourcentage, nous nous y référons puisqu'ils émanent d'une étude impliquant des institutions gouvernementales provinciale et internationale. En ligne : [https://www.stat.gouv.qc.ca/statistiques/education/alphabetisation-litteratie/peica.pdf] (consulté le 15 mai 2020).

47 V. GAUTRAIS, préc., note 16 à la page 205.

standards d'accessibilité du *W3C*[48]. Le choix du format sonore pourrait aider à la compréhension du contenu contractuel non seulement long mais également trop technique. Toujours dans la perspective d'humanisation, on pourrait inciter à la manifestation d'un « vouloir » vrai qui prendra la forme de l'individualisation du contrat[49] de sorte que les noms des personnes contractantes soient insérés dans le contrat.

2.2. UN « VOULOIR » SOUTENU PAR LES TECHNOLOGIES NOUVELLES

[17] « Vouloir » « technologisé ». Les technologies nouvelles tels les algorithmes d'intelligence artificielle peuvent être mobilisées dans cette entreprise de réinvention du « vouloir ». Leur omniprésence tant dans la gestion des contrats que dans l'aide à la décision peut être instrumentalisée au service d'une « épuration » du contrat électronique. En effet, la « technologisation »[50] du « vouloir » peut s'opérer de deux façons : d'abord, au niveau de la rédaction contractuelle et ensuite, au niveau de la prise de connaissance effective des termes contractuels.

[18] Rédaction contractuelle « algorithmisée ». Les *Legaltech* ont démocratisé le contrat en travaillant à son accessibilité, à son automatisation et à sa gestion. Autrement dit, le recours aux algorithmes d'intelligence artificielle dans la rédaction contractuelle pourrait permettre d'**«** épurer **»** le contrat des pathologies qui gangrènent son existence. Les clauses ou informations superflues pourraient être éliminées en privilégiant des modèles de contrat plus clair et intelligible. Ainsi, le contrat jouera pleinement son rôle d'outil de communication et de prévision du futur. D'ailleurs, cette solution peut être davantage intéressante si l'obligation d'explicabilité[51] qui prévaut en matière de prise de décision au moyen de l'IA est mise en œuvre.

[19] Vers une prise de connaissance contractuelle « algorithmisée » ? Pour s'assurer d'une prise de connaissance effective des informations contractuelles, les outils algorithmiques pourrait être mis à contribution en procédant à la synthèse des clauses contractuelles en mettant en

48 Pour plus d'informations sur ces normes, en ligne : <https://www.w3.org/WAI/standards-guidelines/fr> (consulté le 03 août 2020).

49 V. GAUTRAIS, préc., note 16 à la page 205.

50 Au sujet de la « technologisation » du vouloir, voir la conférence prononcée par Charles LESIEUR intitulée : « The Internet's Biggest Myth : « I agree to the Terms & Conditions » » lors de la table ronde sur : **La mort du consentement numérique ?**, en ligne : https://www.lesconferences.ca/videos/la-mort-du-consentement-numerique-5eme-intervention/ (consulté le 14 mai 2020).

51 Voir notamment, Xavier VAMPARYS, « Expliquer « l'explicabilité » », en ligne : <http://www.revue-banque.fr/management-fonctions-supports/article/ethique-intelligence-artificielle-expliquer-explic>, (consulté le 2 septembre 2020).

perspective celles qui sont essentielles et nécessaires à la compréhension du contractant-consommateur. Il faut souligner que la mise en place d'une telle solution doit veiller à anticiper les éventuels biais inhérents à la programmation des algorithmes ainsi que leur mise à disposition gratuite pour les consommateurs. Cela étant, ces avenues constituent très sommairement, une ébauche de systématisation de la forme d'un consentement de qualité résultant d'un « vouloir » vrai.

CONCLUSION

[20] L'exemple du consentement électronique est illustratif des vulnérabilités auxquelles s'exposent le contractant-consommateur lors de la conclusion du contrat électronique. D'un point général, notre contribution a tenté de mettre en perspective les entraves à l'expression d'un consentement résultant d'un « vouloir ». Ces entraves pour la plupart, sont inhérentes à l'inflation informationnelle ainsi qu'aux spécificités techniques du medium générant un dysfonctionnement de communication contractuelle. La conséquence, bien que déplorable, est monnaie courante dans les contrats électroniques. Afin de redonner au « vouloir » la place qui est la sienne dans l'expression d'un consentement de qualité, nous avons esquissé quelques solutions qui potentiellement pourraient permettre d'en finir avec le consentement pathologique dans le contrat électronique

LA VULNÉRABILITÉ DES ENGAGEMENTS PRIS PAR LES ÉTATS POUR PROTÉGER ET PROMOUVOIR LA DIVERSITÉ DES EXPRESSIONS CULTURELLES DANS L'ENVIRONNEMENT NUMÉRIQUE : QUELLE(S) STRATÉGIE(S) POUR LES PARTIES À LA CONVENTION DE 2005 ?

Clémence VARIN[1]

1 L'auteure est candidate au doctorat en droit en cotutelle internationale dans les facultés de droit de l'Université Laval (Canada) et de l'Université Rennes 1 (France).

Résumé

La *Convention sur la protection et la promotion de la diversité des expressions culturelles* adoptée en 2005 par l'UNESCO reconnaît notamment le pouvoir souverain des États de mettre en place les politiques et mesures qu'ils jugent appropriées pour protéger et promouvoir la diversité des expressions culturelles sur leur territoire, ainsi que la double nature - économique et culturelle - des biens et des services culturels. Face aux nouveaux défis posés par le numérique et à la vulnérabilité auxquelles sont exposés leurs engagements en vertu de la Convention, les Parties se sont dotées de *Directives opérationnelles* pour préciser la mise en œuvre de ce traité dans l'environnement numérique.

Cette contribution vise à mettre de l'avant certaines de ces vulnérabilités et, plus particulièrement, à souligner le rôle, à la fois positif et négatif, que peuvent jouer les autres enceintes internationales que l'UNESCO dans l'atteinte des objectifs de cette Convention. L'environnement numérique pousse en effet les Parties à la Convention à établir un plan d'action clair afin que l'accès à une diversité d'expressions culturelles demeure dans cet environnement.

INTRODUCTION

[1] Les avancées dans le domaine des nouvelles technologies impactent la plupart des secteurs de l'économie. Celui de la culture ne fait pas exception puisque le numérique a profondément transformé les modes de création, production, distribution, diffusion et consommation des expressions culturelles. Si le numérique présente de nombreux avantages et opportunités dans le domaine culturel, il présente aussi de nombreux défis et rend la protection et la promotion de la diversité des expressions culturelles particulièrement vulnérable dans cet environnement[2]. La place des grandes plateformes numériques, telles que *Netflix* ou *Spotify*, et les technologies qu'elles utilisent font émerger de nombreux défis quant aux pouvoirs et responsabilités des États en matière de protection et de promotion de la diversité des expressions culturelles dans cet environnement[3]. Elles font émerger un certain nombre d'inégalités en concurrençant directement les acteurs « traditionnels » du monde analogique et menacent l'atteinte d'objectifs légitimes ayant justifié la mise en place de certaines normes et politiques. En effet, alors que certains acteurs sont soumis à des obligations relatives à la mise en place de quotas ou de financement de la création nationale par exemple, l'application de telles obligations est moins évidente pour les nouveaux acteurs numériques.

[2] Cette contribution s'inscrira dans le cadre de la mise en œuvre de la *Convention sur la protection et la promotion de la diversité des expressions culturelles*[4] dans l'environnement numérique. Adoptée en 2005 par l'UNESCO, elle compte à ce jour 149 Parties et reconnaît notamment le pouvoir souverain des États de mettre en place les politiques et mesures qu'ils jugent appropriées pour protéger et promouvoir la diversité des expressions culturelles sur leur territoire, ainsi que la double nature - économique et culturelle - des biens et des services culturels[5]. Pour faire

2 Octavio Kulesz, « Les défis du numérique » dans UNESCO, *Re|Penser les politiques culturelles. 10 ans de promotion de la diversité des expressions culturelles pour le développement*. Rapport mondial de la Convention 2005, Paris, UNESCO, 2015, p. 75, à la page 78.

3 *Ibid.* Voir également : UNESCO, *La diversité des expressions culturelles à l'ère numérique : réflexion canadienne et québécoise*, document d'information, septième session ordinaire du Comité intergouvernemental pour la protection et la promotion de la diversité des expressions culturelles, Paris, Siège de l'UNESCO, 10-13 décembre 2013 ; Octavio Kulesz, « Les politiques culturelles à l'ère des plateformes numériques » dans UNESCO, *Re|Penser les politiques culturelles. La créativité au cœur du développement*, Rapport Mondial de la Convention 2005, Paris, UNESCO, 2017, p. 69.

4 *Convention sur la protection et la promotion de la diversité des expressions culturelles,* 20 octobre 2005, (2010) 2440 R.T.N.U. 311 (entrée en vigueur : 18 mars 2007) [ci-après : « Convention de 2005 »].

5 Cette dimension culturelle renvoie « au sens symbolique, à la dimension artistique et aux valeurs culturelles qui ont pour origine ou expriment des identités culturelles » et justifie que ces biens et services soient traités différemment dans le cadre du commerce international. Voir l'article 4.2. de la Convention de 2005.

face aux nouveaux défis qui pèsent sur la diversité des expressions culturelles, les Parties à la Convention se sont dotées en 2017 de *Directives opérationnelles* pour sa mise en œuvre dans l'environnement numérique. Celles-ci précisent les engagements des Parties pour, notamment, adapter leurs politiques existantes à ces nouveaux enjeux, et mettent également l'accent sur le fait que toute action en matière de diversité des expressions culturelles dans l'environnement numérique ne doit pas se limiter uniquement au secteur de la culture.

[3] Cette intervention visera à démontrer en quoi les engagements pris par les États pour protéger et promouvoir la diversité des expressions sont particulièrement vulnérables dans l'environnement numérique. Cette situation requiert plusieurs types d'actions de la part des Parties à plusieurs niveaux afin de s'assurer que l'accès à une diversité d'expressions culturelles subsiste dans cet environnement (**I**). La promotion des objectifs et principes de la Convention s'avère en outre particulièrement cruciale et fera l'objet d'une analyse particulière (**II**).

I. LA MISE EN ŒUVRE DE LA CONVENTION DANS L'ENVIRONNEMENT NUMÉRIQUE : UN ENGAGEMENT DES PARTIES À PLUSIEURS NIVEAUX

[4] Les *Directives opérationnelles pour la mise en œuvre de la Convention dans l'environnement numérique* visent à offrir un « cadre stratégique pour la compréhension, l'interprétation et la mise en œuvre [du traité] dans un environnement numérique où les biens et services culturels sont créés, produits, distribués, diffusés, consommés et/ou stockés par voie électronique »[6]. Elles précisent les différents engagements des États pour sa mise en œuvre dans l'environnement numérique et « doivent être interprétées et appliquées en relation avec la Convention dans son ensemble »[7].

6 Voir §1, UNESCO, Textes fondamentaux de la Convention de 2005 sur la protection et la promotion de la diversité des expressions culturelles, 2017 à la page 96 [ci-après : « Directives opérationnelles sur le numérique »].

7 *Ibid,* §6. Il convient de préciser que ces directives sont complétées depuis juin 2019 par une *Feuille de route ouverte* permettant aux Parties d'être « mieux outillées pour mettre en œuvre la Convention dans l'environnement numérique », voir : § 8-9, UNESCO, *Point 13 de l'ordre du jour provisoire : Feuille de route pour la mise en œuvre des directives opérationnelles destinées à promouvoir la diversité des expressions culturelles dans l'environnement numérique*, septième session ordinaire de la Conférence des Parties à la Convention pour la protection et la promotion de la diversité des expressions culturelles, Paris, Siège de l'UNESCO, 4-7 juin 2019, DCE/19/7.CP/13 (2 mai 2019).

I.1. L'ADAPTATION DES POLITIQUES ET MESURES NATIONALES RELATIVES AUX BIENS ET SERVICES CULTURELS DANS L'ENVIRONNEMENT NUMÉRIQUE

[5] Les technologies numériques ont profondément transformé certaines pratiques et façons d'accéder aux contenus culturels, et nécessitent la révision de certaines mesures mises en place jusqu'à présent par les Parties afin de remplir leurs obligations en vertu de la Convention. Or, cette étape n'est pas aisée. Certaines politiques, telles que les aides d'État visant à soutenir la création, peuvent être assez facilement élargies aux nouvelles façons de créer, alors que d'autres nécessitent d'être repensé au regard des spécificités liées à l'environnement numérique[8]. La mise en place de quotas est un exemple particulièrement probant à cet égard. Historiquement mis en place pour assurer l'accès à une diversité d'œuvres et notamment la présence d'œuvres nationales au cinéma ou encore à la radio, sa simple transposition à l'environnement numérique ne permettrait pas l'atteinte du résultat escompté en raison de la masse de contenus présents en ligne. À ceci s'ajoutent, les difficultés qui pourraient être rencontrées pour rendre applicables ce genre d'obligations aux plateformes numériques qui dominent le marché et qui sont, pour la plupart, établies en dehors du pays concerné. La directive européenne de services de médias audiovisuels[9], révisée en 2018 et élargie entre autres aux plateformes numériques, offre une réponse possible à cette problématique[10].

[6] La directive européenne, une fois transposée en droit national, les États européens pourront en effet imposer un quota d'au moins 30% d'œuvres européennes sur les plateformes qui ciblent leur territoire, assorti d'une obligation de mise en valeur de celles-ci. Ce dernier aspect est particulièrement intéressant dans la mesure où il vise à éviter que ces œuvres européennes ne se retrouvent « noyées » dans le large catalogue de contenus proposés par la plateforme[11]. Il constitue une adaptation à la

8 Véronique Guèvremont, Clémence Varin et Iris Richer, « Les nouveaux modes d'intervention de l'État visant à protéger et à promouvoir la diversité des expressions culturelles sur les plateformes numériques », dans Alexandra Bensamoun et Françoise Labarthe (dir.), *Culture et numérique – Rencontre franco-québécoise*, Paris, Mare & Martin, 2020, à la page 174.

9 Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services médias audiovisuels »), compte tenu de l'évolution des réalités du marché, J.O. L303/69, 28 novembre 2018, en ligne : <https://eurlex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018L1808&from=EN>.

10 Véronique Guèvremont, Clémence Varin et Iris Richer, préc., note 8, à la page 178.

11 *Ibid.*, voir également : Véronique Guèvremont, « Réflexion préliminaire sur la mise en œuvre de la Convention sur la protection et la promotion de la diversité des expressions culturelles à l'ère numérique », étude présentée lors de la quatrième session ordinaire de la Conférence des Parties à la Convention sur la protection et la promotion de la diversité des expressions culturelles, Paris, Siège de l'UNESCO, 11-14 juin 2013, à la page 22.

spécificité du numérique et au modèle d'affaires de ces plateformes reposant pour la plupart sur des recommandations algorithmiques. La combinaison de ces deux derniers éléments – quotas et mise en valeur – permettrait donc d'assurer une meilleure *découvrabilité* des contenus nationaux, et dans ce cas régionaux[12]. L'Union européenne opère ainsi avec cette directive un « changement de paradigme » où « le fait de « cibler » les spectateurs sur le territoire d'un État est suffisant » pour leur imposer de telles obligations[13]. Cette directive se base sur cette même idée pour permettre aux États membres d'exiger de ces plateformes qu'elles participent au financement de la création – auquel la plupart échappent actuellement – dès lors que de telles obligations sont déjà en place sur leur territoire.

I.2. DES MESURES QUI NE PEUVENT SE LIMITER AU SECTEUR CULTUREL ET À L'ÉCHELLE NATIONALE

[7] Or, si l'adaptation des politiques au niveau national est primordiale pour atteindre les objectifs de la Convention, elle n'est pas suffisante dans l'environnement numérique notamment en raison de sa nature à priori dépourvue de frontière. Les Parties doivent également veiller à la cohérence de leurs engagements au niveau international dans tout secteur qui n'est pas exclusivement culturel.

[8] Les *Directives opérationnelles sur le numérique* mettent d'ailleurs l'accent sur le fait que toute action en matière de diversité des expressions culturelles dans l'environnement numérique ne doit pas se limiter uniquement au secteur de la culture, dans la mesure où certaines décisions prises dans d'autres secteurs peuvent avoir un impact sur la diversité des expressions culturelles[14]. Cet aspect est d'autant plus important que certaines décisions prises dans d'autres enceintes pourraient permettre aux Parties d'adapter leurs politiques et mesures au niveau national ou bien les inspirer. On peut citer à cet égard l'émergence du concept de « présence numérique significative » (par opposition à la présence territoriale) qui vise à taxer à l'endroit où la valeur est générée[15]. Ce concept pourtant issu du domaine fiscal pourrait « être repris dans la

12 L'Union Européenne est la seule organisation régionale partie à la Convention de 2005.

13 Véronique Guèvremont, Clémence Varin et Iris Richer, préc., note 8, aux pages 177 et 178.

14 Voir § 19 des Directives opérationnelles sur le numérique. Voir également : Véronique Guèvremont, « Réflexion préliminaire sur la mise en œuvre de la Convention sur la protection et la promotion de la diversité des expressions culturelles à l'ère numérique », préc., note 11, à la page 16.

15 Véronique Guèvremont, Clémence Varin et Iris Richer, préc., note 8, à la page 179.

révision des lois en vigueur dans d'autres secteurs, y compris dans le domaine de la culture », notamment pour fixer des obligations de financement de la création ou « des exigences de contenus nationaux »[16].

[9] Il convient donc pour les Parties d'identifier ces enceintes pertinentes et de veiller à la cohérence de leurs actions au niveau international alors qu'on observe une interdépendance croissante des secteurs dans l'environnement numérique[17]. Cet aspect est d'autant plus important que certaines décisions prises au niveau international pourraient avoir des conséquences directes sur le pouvoir souverain des Parties d'intervenir en faveur de la diversité des expressions culturelles.

II. LA PROMOTION DES OBJECTIFS ET PRINCIPES DE LA CONVENTION DANS D'AUTRES ENCEINTES INTERNATIONALES : UN ENGAGEMENT CRUCIAL DES PARTIES DANS L'ENVIRONNEMENT NUMÉRIQUE

[10] L'article 21 de la Convention engage les Parties à promouvoir les objectifs et principes de ce traité dans d'autres enceintes internationales et à se consulter le cas échéant. Sa mise en œuvre a, par ailleurs, été jugée cruciale pour l'avenir de la diversité des expressions culturelles dans cet environnement dans la mesure où elle « pourrait compromettre la réalisation des objectifs fondamentaux de la Convention »[18]. Alors que les engagements pris par les Parties sont particulièrement vulnérables dans certaines enceintes, à l'instar de celle commerciale, elles peuvent également être d'importants leviers pour diffuser les objectifs et les principes de la Convention[19].

II.1. LA VULNÉRABILITÉ DES ENGAGEMENTS PRIS PAR LES PARTIES AU REGARD DE LA CONVENTION DANS D'AUTRES ENCEINTES INTERNATIONALES : L'EXEMPLE DES ACCORDS DE COMMERCE

[11] La Convention de 2005 et l'enceinte commerciale entretiennent une relation particulière. Avant son adoption, les règles du système

16 *Ibid.* On peut noter que la Directive de services de médias audiovisuels précédemment présentée se base également sur ce concept.

17 Véronique Guèvremont, « Réflexion préliminaire sur la mise en œuvre de la Convention sur la protection et la promotion de la diversité des expressions culturelles à l'ère numérique », préc., note 11, à la page 28.

18 Véronique Guèvremont, « La Convention dans les autres enceintes internationales : un engagement crucial » dans UNESCO, *Re|Penser les politiques culturelles. La créativité au cœur du développement*, Rapport Mondial de la Convention 2005, Paris, UNESCO, 2017, p. 143, à la page 161.

19 Véronique Guèvremont, « Promouvoir la Convention dans les enceintes internationales » dans UNESCO, *Re|Penser les politiques culturelles. 10 ans de promotion de la diversité des expressions culturelles pour le développement*, Rapport Mondial de la Convention 2005, Paris, UNESCO, 2015, p. 135, à la page 137.

commercial multilatéral requéraient notamment des États qu'ils traitent les produits culturels comme n'importe quel autre produit, ce qui été particulièrement problématique pour ceux souhaitant conserver leur pouvoir d'intervention dans ce domaine[20]. La Convention a permis de reconnaitre le droit souverain des États « d'adopter et mettre en œuvre les politiques et mesures qu'ils jugent appropriées pour la protection et la promotion de la diversité des expressions culturelles sur leur territoire »[21], mais malheureusement ce droit est loin d'être acquis. Certaines Parties pouvant effectivement, dans certains cas, limiter ce pouvoir qu'elles se sont elles-mêmes reconnu en faveur de la diversité des expressions culturelles.

[12] La conclusion d'accords de commerce régionaux et bilatéraux contenant des engagements relatifs au commerce électronique est un exemple particulièrement probant à cet égard. En effet, tout engagement pris par une Partie à la Convention qui ne prendrait pas en compte la spécificité des biens et services culturels dans le cadre du commerce électronique pourrait l'empêcher de mettre en place des politiques et mesures pour la protection et la promotion de la diversité des expressions culturelles dans l'environnement numérique au risque d'être sanctionné[22]. Une telle situation pourrait avoir des effets désastreux dans certains pays en raison des règles de libre-échange. En outre, ce risque est particulièrement palpable aujourd'hui dans l'enceinte de l'Organisation mondiale du commerce alors que se poursuivent des négociations en matière de commerce électronique. L'issue de celles-ci pourrait remettre en cause la reconnaissance de la double nature des biens et services culturels dans cet environnement, certains États voulant que le principe de non-discrimination s'applique au commerce

20 Ivan Bernier et Hélène Ruiz Fabri, *Évaluation de la faisabilité juridique d'un instrument international sur la diversité culturelle*, Groupe franco-québécois sur la diversité culturelle, Gouvernement du Québec, Ministère de la Culture, 2002, à la page 23.

21 Article 1 h) de la Convention de 2005.

22 Ce manque de prise en compte de la spécificité des biens et services culturels dans l'environnement numérique est une réalité, comme en attestent plusieurs accords de commerce bilatéraux ou régionaux récents qui libéralisent le chapitre sur le commerce électronique, voir par exemple : The United-States-Korea Trade Agreement, signé en le 30 juin 2007 et entrée en vigueur le 15 mars 2012, et United States-Australia Free Trade Agreement (AUSFTA), signé le 18 mai 2004 et entrée en vigueur le 1er janvier 2005. Voir à ce sujet : Véronique Guèvremont et Ivana Otasević , *La culture dans les traités et les accords : la mise en œuvre de la Convention de 2005 dans les accords commerciaux bilatéraux et régionaux*, Série Politique & Recherche, Paris, UNESCO, 2017 ; Véronique Guèvremont et al., Commentaires présentés par la Chaire UNESCO sur la diversité des expressions culturelles dans le cadre des Consultations en prévision de négociations éventuelles sur le commerce électronique à l'Organisation mondiale du commerce (OMC) à la Direction de la politique commerciale sur les services (TMS), Affaires mondiales Canada, Chaire UNESCO sur la diversité des expressions culturelles, 25 avril 2019.

électronique[23]. Il est donc primordial pour les Parties de veiller à préserver ce pouvoir d'intervention en faveur de la culture dans ce cadre. La coordination entre les ministères en charge de la culture et de la négociation de tels accords notamment, et entre les Parties dans une certaine mesure, est plus que jamais pertinente pour veiller à respecter les engagements que les Parties se sont fixées au regard de la Convention[24].

[13] L'article 21 impose ainsi une obligation de cohérence dans les actions entreprises par les Parties au niveau international. Les directives opérationnelles rappellent par ailleurs que conformément à leurs obligations au titre de cet article, les Parties sont encouragées à promouvoir « la complémentarité et la cohérence entre les divers instruments juridiques portant sur la diversité des expressions culturelles dans l'environnement numérique »[25]. Or, la mise en œuvre de l'article 21 ne se résume pas à la seule enceinte commerciale, et de nombreuses autres enceintes ont été identifiées par les Parties dans le cadre de plusieurs consultations effectuées par le Secrétariat de la Convention de 2005[26]. Le traité a également été évoqué à plusieurs reprises dans d'autres enceintes internationales par plusieurs Parties, et des références directes à la Convention sont apparues notamment dans des affaires judiciaires, des résolutions et déclarations adoptées dans le cadre de réunions internationales, etc. Cependant, un certain nombre d'enceintes se penchent sur les technologies numériques et leur encadrement. Il parait dans ce cadre légitime de s'interroger sur leur rôle particulier en tant que levier de diffusion des objectifs et principes de la Convention dans l'environnement numérique.

II.2. LE RÔLE DE CERTAINES ENCEINTES INTERNATIONALES DANS L'ATTEINTE DES OBJECTIFS DE DIVERSITÉ DES EXPRESSIONS CULTURELLES DANS L'ENVIRONNEMENT NUMÉRIQUE

23 Véronique Guèvremont et al., Commentaires présentés par la Chaire UNESCO sur la diversité des expressions culturelles dans le cadre des Consultations en prévision de négociations éventuelles sur le commerce électronique à l'Organisation mondiale du commerce (OMC) à la Direction de la politique commerciale sur les services (TMS), préc., note 22, à la page 19.

24 § 19.3 des Directives opérationnelles sur le numérique.

25 *Ibid*., § 19.1.

26 Il peut s'agir par exemple d'organisations internationales (telle que l'Organisation mondiale de la propriété intellectuelle), intergouvernementales (telles que l'OCDE, l'Organisation internationale de la Francophonie), des organisations non gouvernementales, etc. Voir : UNESCO, *Point 11 de l'ordre du jour provisoire - Traitement préférentiel et Concertation et coordination internationales : rapport sur la mise en œuvre et l'impact des articles 16 et 21 de la Convention,* CE/15/5.CP/11, cinquième session ordinaire de la Conférence des Parties à la Convention sur la protection et la promotion de la diversité des expressions culturelles, Paris, Siège de l'UNESCO, 10-12 juin 2015 (23 avril 2015), à la page 10 et 11.

[14] La Convention adopte une définition large des enceintes internationales ce qui permet d'y inclure une multitude d'autres fora formels, informels, composés d'acteurs étatiques ou non[27]. Elle ne formule en outre aucune liste exhaustive d'enceintes pouvant faire l'objet de la promotion des objectifs et principes de la Convention. Dans un tel contexte, il semble donc pertinent de s'intéresser à toute enceinte internationale « dont les travaux sont susceptibles de se répercuter sur l'évolution de l'environnement numérique »[28], et particulièrement celles qui ont trait à l'encadrement des technologies numériques. En effet, toute discussion entourant la suppression de la neutralité d'Internet pourrait, par exemple, affecter l'accès à certains contenus culturels et à en désavantager certains par rapport à d'autres.

[15] L'intérêt grandissant de certaines technologies comme l'intelligence artificielle, les algorithmes ou encore le recours croissant aux données dans le secteur culturel, ainsi que les opportunités et possibles effets néfastes associés à leur utilisation poussent à s'interroger sur le rôle que pourraient jouer certaines enceintes qui s'interrogent sur l'encadrement du développement de ces technologies. L'intelligence artificielle, par exemple, est un domaine où prolifère un certain de nombre de déclarations, codes d'éthique, etc. qui suscitent une interrogation sur l'action qui devrait être menée par les Parties à la Convention à cet égard. Devraient-elles saisir l'occasion pour faire la promotion de façon plus ciblée des objectifs et principes de la Convention au sein de ces instruments, afin qu'ils contribuent favorablement à la diversité des expressions culturelles dans l'environnement numérique et ne restreignent pas l'accès des individus à une telle diversité ? L'inclusion de certains objectifs et principes de la Convention au sein de ces technologies pourrait être explorée afin qu'elles concourent elles-mêmes, dans une certaine mesure, à la diversité des expressions culturelles dans l'environnement numérique.

[16] Quelles que soient les enceintes choisies par les Parties, la même finalité demeure : les Parties doivent s'assurer de la cohérence entre les

27 Peter-Tobias Stoll, « Article 21: International Consultation and Coordination » dans Sabine von Schorlemer et Peter-Tobias Stoll (dir.), *The UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions, Explanatory Notes*, Springer-Verlag Berlin Heidelberg, 2012, p. 545, à la page 547.

28 Véronique Guèvremont, préc., note 11, à la page 28.

différents instruments élaborés en leur sein[29] et veiller à ce qu'ils n'aillent pas à l'encontre des objectifs et principes de la Convention. Mais le numérique pose de nouvelles interrogations qu'il convient d'explorer.

CONCLUSION

[17] Les politiques et mesures prises par les Parties quant à la protection et la promotion de la diversité des expressions culturelles s'avèrent particulièrement vulnérables à l'ère numérique, poussant les Parties à la Convention de 2005 à les adapter aux différents défis posés par cet environnement. Ces actions s'effectuent à plusieurs niveaux et concernent une variété de secteurs, culturel ou non, qui peuvent avoir un impact sur celui-ci.

[18] Or, la mise en œuvre de l'article 21 de la Convention, qui vise à promouvoir les objectifs et principes de la Convention dans d'autres enceintes internationales, s'avère également cruciale dans cet environnement où les secteurs de sont de plus en plus interdépendants. Il engage en effet les Parties à prêter une attention particulière aux initiatives prises en dehors de l'UNESCO qui pourraient avoir un impact sur la diversité des expressions culturelles. Il incite ainsi les Parties à être cohérentes dans leurs engagements afin qu'ils n'aillent pas à l'encontre des objectifs et principes de la Convention de 2005. Cependant, l'environnement numérique est un terrain particulièrement fécond en termes d'initiatives visant à réglementer l'émergence de ces nouvelles technologies, ce qui requiert plus que jamais une certaine concertation et coordination des Parties à la Convention - également prévu par l'article 21 - afin de s'assurer que l'accès à une diversité d'expressions culturelles demeure dans cet environnement.

29 L'article 20 de la Convention, qui forme avec l'article 21 le Chapitre V de la Convention relatif à la relation entre la Convention et les autres instruments, il vise à souligner les conflits qui pourraient éventuellement surgir entre les engagements issus de la Convention et ceux découlant d'autres instruments internationaux. Voir : Peter-Tobias Stoll, préc., note 27, aux pages 545 et 546.