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'autrice 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 et de la Faculté de droit de l'Université Laval.

[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.