Notes de service sur les politiques

Commission canadienne sur l'expression démocratique

Séance d'apprentissage 4 : Doit-on tenir responsables les acteurs en ligne? Quels mécanismes juridiques peuvent être utilisés?

Jeudi 4 novembre 2021 | 13 h à 14 h 30 HE (UTC – 16 h)

Événement virtuel sur Zoom

Résumé de la séance

L'utilisation des technologies de recherche de contacts pour la santé publique, des technologies de prédiction du crime pour l'application des lois et l'usage abusif des systèmes de données, ont été mis en place et utilisés dans des environnements déficients de protection de la vie privée et des données, dans des contextes légalement ambigus, et parfois, dans des conditions d'apparence illégale. Ces préjudices reçoivent beaucoup d'attention des législateurs et des groupes de défense d'intérêts qui travaillent à faire en sorte que les entreprises privées soient tenues responsables devant la loi et redevables envers leurs utilisateurs. Les gouvernements et les décideurs politiques qui sont chargés de protéger le public sont aux prises avec un ensemble parallèle de préoccupations épineuses sur le plan juridique et de la mise en application. L'examen de plus en plus approfondi du public relativement aux préjudices en ligne, aux campagnes de désinformation et à l'usage abusif du pouvoir de marché, toutefois, alimente la révolte contre les grandes entreprises de technologies (les « Big Tech »), et soulève d'inévitables questions à savoir qui doit être tenu responsable de la conscience collective.

Questions politiques :

Les gouvernements doivent-ils élaborer et adopter des mesures de responsabilisation juridique pour la désinformation? Dans un tel cas, à quoi ressemblerait le cadre juridique?

Quels sont les défis auxquels d'autres juridictions font face dans la tentative d'application des lois et de politiques pour tenir les plateformes en ligne responsables des risques et préjudices connus?

Cinq façons pour commencer à réglementer les entreprises de technologie sans compromettre la liberté

Kate Klonick, professeure adjointe à l'école de droit St. John's/chercheuse au Brookings Institution et Yale ISP

De quelles manières les gouvernements et le public peuvent-ils inciter des mesures pour une plus grande transparence et responsabilisation afin de minimiser les préjudices potentiels des plateformes en ligne, dont la mésinformation et la désinformation, la haine sur le Web et les atteintes à la vie privée? Au terme de centaines d'heures de recherche à l'intérieur et à l'extérieur des plus grandes sociétés qui régissent les discours en ligne, je crois que cinq solutions réglementaires principales peuvent être envisagées, lesquelles sont des interventions bien articulées pour le bien-être des utilisateurs et peuvent aider à corriger les modèles d'autoréglementation de longue date des entreprises de technologie. Si mon but avec ces concepts a été de les adapter pour qu'ils passent l'examen du premier amendement aux États-Unis, je pense que dans les pays où ces limites constitutionnelles n'existent pas, la faisabilité d'une telle réglementation est une solution encore plus prometteuse et pragmatique.

Portabilité des données. Théoriquement, le droit des utilisateurs individuels de déplacer leurs données d'une plateforme à l'autre leur donne des choix[1] tant sur le plan de la démocratie que sur celui du marché. Au sens de la démocratie, ce choix permet aux utilisateurs de partir ou d'exprimer leurs préférences en apportant leurs données (et donc le potentiel publicitaire) sur d'autres plateformes. De manière indirecte, ceci entraîne aussi un impact sur le marché : les plateformes se feront concurrence pour éviter de perdre des utilisateurs et leurs données; idéalement, les utilisateurs peuvent s'organiser et boycotter une sortie de masse pour forcer un impact sur le marché; et enfin, ceci permet l'innovation et l'émergence de nouvelles plateformes où les utilisateurs peuvent apporter leurs données à de nouveaux endroits qui correspondent mieux à leurs attentes. D'un point de vue pragmatique, bien entendu, ceci est plus facile à dire qu'à faire. Les données qui sont compilées sur tout utilisateur individuel ne sont pas aussi faciles à extraire d'une plateforme (ni ne sont précieuses) que l'on pourrait croire, surtout de plateformes qui ont bâti leur propre code pour interagir avec des signaux de données à leur manière. De plus, en raison des préoccupations en matière de respect de la vie privée, la plupart des données des utilisateurs sont dissociées d'eux de manière identifiable, et ont moins de pouvoir en tant qu'outil de marketing/publicité lorsqu'elles sont dissociées d'un réseau d'autres profils anonymes. Malgré ces limitations, je crois que contraindre les plateformes à donner la priorité à ces difficultés pragmatiques au moyen d'une réglementation est une prochaine étape utile pour faire progresser cet enjeu. Des initiatives semblables comme celle du droit à la portabilité des données a déjà été codifiée dans l'article 20 du Règlement général sur la protection des données (RGPD)[2] de l'Union européenne et proposée dans le ACCESS Act[3] des États-Unis.

Interopérabilité au niveau des fonctionnalités des produits. Plusieurs de ces mots effraient les gens parce qu'ils ne connaissent pas leur signification. Permettez-moi de proposer une définition et de donner un exemple. De manière générale, le terme « interopérabilité » réfère à la capacité d'un aspect du service d'une plateforme de fonctionner d'un appareil à l'autre, ou d'une plateforme à l'autre, dont les deux sont fabriqués par différents manufacturiers tant au niveau du matériel informatique que de celui du logiciel.[4] Prenons un exemple. À la fin des années 1990 et au début des années 2000, la Commission fédérale des communications des États-Unis a examiné une fusion entre America Online (AOL; le navigateur dominant à l'époque et mécanisme de connexions en ligne) et Time Warner

(TW; a fournisseur dominant dans le domaine des nouvelles par câble).

---

[1] *See e.g.* ALBERT 0. HIRSCHMAN, EXIT, VOICE, AND LOYALTY (Harvard University Press).

[2] Article 20 du RGPD - *Right to data portability*.

[3] Texte - H.R.3849 -117th Congress (2021-2022): ACCESS Act of 2021 (2021).

[4] Stephen O'Connor, *What Is Interoperability, and Why Is It Important?* https://www.adsc.com/blog/what-is-interoperability-and-why-is-it-important (dernière consultation, 1er novembre 2021).

[5] En dépit de nombreux détails techniques et de nombreux litiges, la fusion a finalement été approuvée, à condition qu'AOL se sépare de son service de messagerie instantanée.[6] Que furent les retombées de cette décision pour les utilisateurs? Concrètement, cela voulait dire soudainement qu'en utilisant leur identifiant personnel (pseudonyme), ils pouvaient échanger des messages avec leurs réseaux d'amis par l'entremise d'applications de code source libre[7] à l'échelle des services propriétaires. Tout d'un coup, les gens n'avaient plus à se connecter à la fois sur ICQ, AOL et MSN pour clavarder avec leurs amis. Ils pouvaient converser avec tous leurs contacts à partir d'un seul service de code source libre. La technologie de messagerie instantanée est devenue relativement une chose du passé avec la montée des messages textes, mais pas les leçons. Le pouvoir dominant d'AOL sur le marché s'est lentement affaibli après la fusion – en partie parce qu'elle a perdu des utilisateurs qui ne se connectaient que pour clavarder avec leurs amis sur d'autres services de code source libre - et n'est plus aujourd'hui que l'ombre de l'entreprise de technologie qu'elle était. D'un point de vue de la réglementation, l'interopérabilité des services ou des fonctionnalités des produits a fait l'objet de discussions aux États-Unis sur le plan de solutions antitrust et de contrôle réglementaire. Je suis d'avis qu'il s'agit de l'un des meilleurs points d'intervention qui permet aux goulots d'étranglement de se détendre naturellement sans détruire des entreprises de haut en bas, et de poursuivre l'innovation.

Intergiciel au niveau des préférences des consommateurs. L'autre endroit où il est possible de niveler le choix et le contrôle des utilisateurs est de laisser les utilisateurs choisir les fonctionnalités et les préférences, mais de faire en sorte que ce choix soit offert *en plus* des fonctionnalités naturelles d'une plateforme. Ceci permet aux utilisateurs de personnaliser une expérience – une chose que peut-être seuls les utilisateurs les plus expérimentés pourraient être en mesure de faire – et aussi de consolider les préférences qui pourraient correspondre aux solutions en matière d'intergiciels qui ont été retenues. Comment rendre les intergiciels obligatoires? De manière générale, cela signifierait que les plateformes permettraient un niveau d'interaction entre leur plateforme et une couche externe de personnalisation. Je compare cela à commander un hamburger « avec une sauce spéciale » (c'est-à-dire, la recommandation du « secret commercial » de la plateforme ou des algorithmes de classement) ou de le commander sans sauce spéciale (fil d'actualité chronologique peut-être) ou de le commander avec des cornichons ou des oignons ou du ketchup ou de la moutarde (chacun des condiments étant un intergiciel externe que les utilisateurs peuvent ajouter pour améliorer leur expérience). La faisabilité de l'intergiciel en tant que solution au problème de mésinformation, de désinformation et de haine en ligne[8] suscite de plus en plus d'enthousiasme chez les universitaires, mais peu de réformes réglementaires sont proposées dans ce sens.

Contrôle. Les utilisateurs interagissent à plusieurs niveaux avec les plateformes pour contrôler les discours qu'ils voient et les politiques qui les entourent, mais mon travail au cours des six dernières années a principalement porté sur ce qui se passe en privé à l'intérieur des entreprises après que des personnes ont été exposées à du contenu d'autres utilisateurs qu'elles jugent nuisible à leur égard, et nuisible à la société. En pratique, les principaux éléments qui contrôlent l'examen post hoc des discours préjudiciables sont les politiques des plateformes qui ont une longue tradition d'opacité,

[5] *America Online & Time Warner Instant Messaging Interoperability,* FEDERAL COMMUNICATIONS COMMISSION, https://www.fee.gov/america-online-time-warner-instant-messaging-interoperability (dernière consultation le 30 octobre 2021). [6] La messagerie instantanée était une application de messagerie texte-navigateur utilisée avant la messagerie texte/messagerie directe avant les téléphones cellulaires. Le service de messagerie instantanée de AOL était le service propriétaire de AOL, mais plusieurs autres étaient offerts de manière indépendante (ICQ par exemple) ou par l'entremise de concurrents (MSN Messenger par exemple).

[7] ADIUM, une application de bureau code source libre qui permettait aux utilisateurs de converser simultanément sur plusieurs plateformes de messagerie instantanée, est un exemple.

[8] Francis Fukuyama et al., *Report of the Working Group on Platform Scale* (Nov. 2020).

[9] de manque de personnel, de conception déficiente et d'environnement de travail exécrable.[10] Au cours des trois dernières années, dans l'effort d'adopter ouvertement un modèle de gouvernance pour la façon dont elle étudie les discours en ligne à l'échelle mondiale, Facebook a créé le Comité de surveillance (Oversight Board)[11], un groupe composé de 20 personnes, financées de manière indépendante, pour revoir ses décisions en matière de contenu et d'émettre des directives d'application et parfois de politique générale à l'intention de l'entreprise.[12] Malgré un scepticisme initial, le groupe a lentement gagné la confiance du public ainsi que sa légitimité, surtout pour sa décision très médiatisée dans le cadre de l'examen du cas visant à bloquer l'accès de Donald Trump à Facebook.[13] À l'heure actuelle, aucune autre plateforme n'envisage la formation d'un comité de surveillance, et selon les conversations dans l'industrie auxquelles j'ai participé, ceci est attribuable en grande partie au fait que les plateformes croient qu'elles n'ont pas eu à faire face à une « pression similaire du public » ou à des « catastrophes de relations publiques » comme celles auxquelles Facebook a été confrontée et qui pourraient les contraindre à poser un tel geste. Je pense qu'il s'agit d'un moment véritablement transformateur dans l'établissement de normes mondiales et dans la transparence des plateformes et qu'une pression du public ou du marché sur les plateformes ne devrait pas être le seul élément déclencheur de l'imposition de ce type d'autoréglementation. Les mandats qui exigent la mise en place de tels organismes au sein des plateformes dont le produit principal est spécifiquement composé de discours générés par les utilisateurs, lesquels créent à la fois la sphère numérique et la sphère publique actuelles, devraient tenir les plateformes responsables de mettre en place de tels organismes.

Transparence et disponibilité des données pour les chercheurs. Jusqu'à présent, deux mécanismes ont évolué pour les recherches sur les plateformes numériques : les recherches qui sont menées avec le consentement des plateformes (comme les banques de données remises aux chercheurs, l'intégration permise pour les chercheurs externes, etc.) ou celles dont la récupération ou la collecte de données est effectuée sans consentement par des chercheurs externes des plateformes. Les deux mécanismes comprennent des avantages et des inconvénients. La recherche menée avec le consentement des plateformes peut donner lieu à des données compromises et à un manque de vraie transparence; mais elle peut aussi signifier que des renseignements personnels permettant d'identifier une personne sont plus faciles à retirer et à cacher et que les ensembles de données sont plus grands et moins dispersés. À l'opposé, des chercheurs qui n'ont pas le consentement des plateformes ont la capacité de collecter des données que même les plateformes elles-mêmes ne recueillent pas, et peuvent prendre tout ce qu'ils peuvent récolter sans interventions des plateformes. Les inconvénients de ces mécanismes sont que la collecte s'effectue dans le désordre (et le temps qu'il faudra pour « nettoyer » les données pour les utiliser), la quantité de renseignements personnels dans les données qui permettent d'identifier une personne et les tailles des échantillons qui ne sont pas représentatifs ou trop petits. La meilleure solution en matière de réglementation qui comprend ces modèles a été proposée par le professeur de droit Nathaniel Persily à Stanford, dont le projet de loi est en cours d'élaboration pour adoption par les sénateurs américains Rob Portman et Chris Coons.

[9] *Voir exemple* - REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM (Édition réimprimée, Basic Books, avril 2013); TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET (Yale University Press 2018); SARAH T. ROBERTS, BEHIND THE SCREEN (Yale University Press 2019); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech,* 131 HARV. L. REV. 1598 (2017-2018).

[10] GILLESPIE, *supra* note 9; ROBERTS, *supra* note 9; Adrian Chen, *The Laborers Who Keep Dick Pies and Beheadings Out of Your Facebook Feed,* (23 octobre 2014) (Wired), https://www.wired.com/2014/10/content-moderation/;Jeffrey Rosen, *The Delete Squad,* THE NEW REPUBLIC (29 avril 2013), https://newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules; Casey Newton, *The Secret Lives of Facebook Moderators in America,* THE VERGE (25 février 2019), https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator- interviews-tra uma-working-conditions-arizona.

[11] Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression,* 129 YALE L.J. 2418 (2019-2020).

[12] Kate Klonick, *Inside the Making of Facebook's Supreme Court,* (12 février 2021) (The New Yorker), https://www.newyorker.com/tech/annaIs-of-technology/inside-the-making-of-fa cebooks-supreme-court.

[13] Jack M Balkin & Kate Klonick, *Facebook's Oversight Board Was Supposed to Let Facebook off the Hook. It Didn't., Washington Post* (5/6/21) https://www.washingtonpost.com/outlook/2021/05/06/facebook-oversight-board-trump/.

Conclusion. J'ai passé les premières années de ma recherche et de ma carrière à m'abstenir de proposer des solutions aux « problèmes des préjudices causés par des discours en ligne et du respect de la vie privée ». Il en fut ainsi parce qu'à titre d'universitaire et de chercheuse en sciences sociales, je ne croyais pas que nous étions en position de comprendre entièrement ce qu'étaient les préjudices, encore moins les meilleurs moyens de s'y attaquer de haut en bas. L'une des critiques les plus courantes à l'égard des « Big Tech » est l'introduction d'une nouvelle technologie avec peu ou pas de recherche ou de préoccupations quant à l'impact des changements qui en découlent dans la vie des gens dans le monde en dehors du bien immédiat qu'elle est censée offrir. Je ne souhaite pas l'intervention des gouvernements, laquelle a toujours eu l'intention d'être plus délibérée et réfléchie, pour commettre les mêmes erreurs avec des lois précipitées et créer encore plus de torts. Dans cette intention, il s'agit des solutions qui à mon avis sont les plus optimales et prometteuses pour l'avenir.

[14] Nate Persily, *Persily Proposed Legislation 10* 5 *21,* DROPBOX, https://www.dropbox.com/s/5my9r1t9ifebfz1/Persily%20pro posed%201egislat ion%2010%205 %2021.docx?dl=0 (dernière consultation, 1er novembre 2021).

Commission canadienne sur l'expression démocratique

Sommaire - Ravi Naik

La désinformation n'est pas un acte unique et isolé. La désinformation renferme une variété d'actes et d'acteurs différents. Trois enjeux associés à cette variété requièrent trois règlements différents :

1. Contenu – D'importantes considérations à prendre en compte sur la liberté d'expression, de même que la responsabilité des intermédiaires. Les régimes de responsabilité qui font courir aux entreprises de plateformes un risque juridique pour les activités des utilisateurs en ligne peuvent menacer la liberté d'expression et l'innovation, même lorsqu'il est question de résoudre des problèmes politiques très réels. Il est toutefois important que les plateformes fournissent concrètement une transparence quant aux messages et aux contenus payés - qui a payé, pourquoi et à quelle fin. De telles considérations sont distinctes des questions d'anonymat des utilisateurs en ligne et des questions de sûreté et de sécurité des messages, dont aucune ne doit être compromise sans un examen séparé et détaillé de leurs mérites. Toutefois, les plateformes doivent être tenues d'agir lorsqu'elles ont connaissance d'un contenu illégal, y compris de fournir des moyens concrets et efficaces aux individus pour signaler des contenus préoccupants.

2. Plateformes – Lorsque les plateformes s'engagent dans une démarche active, la responsabilité doit être soulevée. Ceci comprend des systèmes de recommandations et une segmentation automatisée des comportements. Deux considérations politiques : fournir une série de droits individuels sur la façon dont l'information est utilisée, avec des mécanismes et des recours concrets et efficaces. L'accent doit être mis sur des recours pratiques, plutôt que/en plus de réparations pécuniaires. Deuxièmement, les plateformes doivent être ouvertes à un examen indépendant. Deux domaines clés d'élaboration d'une politique : audits algorithmiques et accès plus clair aux chercheurs.

3. Créateurs – Ne se limitent pas aux partis politiques, mais à une gamme d'acteurs.

D’importants outils pour combattre la désinformation : (i) limites sur la quantité de données qui peuvent être collectées et des bases juridiques pour le traitement, et (ii) une transparence significative sur qui a payé pour quel service. Pas de limites temporelles puisque la politique ne se fait pas de manière limitée dans le temps en raison de la vitesse et de l’ampleur des médias sociaux.

Trois considérations plus larges à prendre également en compte :

i. Toute élaboration de règlements requiert une réflexion commune en combinant la protection des données, la réglementation du contenu, les règles de concurrence et les droits de la personne.

ii. Les enjeux de la désinformation et des préjudices peuvent survenir sur quelques grandes plateformes. Toutefois, les incidences élargies de la réglementation se feront sentir au-delà de ces plateformes. Toute réglementation doit être neutre en matière de plateformes plutôt que de tenter de résoudre les enjeux présentés par quelques entreprises, aussi importantes soient-elles.

iii. Les enjeux présentés sont des enjeux mondiaux, et exigent donc des interventions à l’échelle mondiale. Les règlements et les plateformes entraînent des répercussions partout dans le monde. Il faudra que le pays prenne l’initiative de réclamer des règlements internationaux cohérents pour éviter que notre réalité en ligne soit actuellement fragmentée et éclatée.

Mécanismes juridiques : doit-on tenir responsables les acteurs en ligne? Quels mécanismes juridiques peuvent être utilisés?

Emily Laidlaw, titulaire de la Chaire de recherche du Canada en droit de la cybersécurité et professeure agrégée, Faculté de droit, Université de Calgary, octobre 2021

Responsabilité et droit canadien

Contrairement à l'Union européenne et aux États-Unis, il n'existe pas de loi fédérale qui traite largement de la responsabilité des intermédiaires au Canada. Au niveau provincial, la loi québécoise crée une sphère de sécurité conditionnelle.[1] Jusqu'à présent, la responsabilité des intermédiaires s'est principalement étendue aux domaines du droit de la diffamation (common law) et de la loi sur le droit d'auteur (loi).

- Droit de la diffamation : Dans la pratique, il sert de sphère de sécurité conditionnelle ou de régime d'avis et de retrait selon lequel l'intermédiaire risque d'être tenu responsable de la diffamation s'il a connaissance et le contrôle du contenu illicite et ne le retire pas.
- Loi sur le droit d'auteur : La loi sur le droit d'auteur[2] met en place un cadre d'avis et avis selon lequel un titulaire de droits peut envoyer un avis de violation du droit d'auteur à un fournisseur d'accès Internet (FAI), lequel aurait l'obligation de transmettre à l'utilisateur lié à l'adresse IP. Si le FAI n'envoie pas la lettre, le risque en est un de dommages-intérêts d'origine législative plutôt que la responsabilité du tort sous-jacent.

L'article 19.17 de l'entente Canada–États-Unis-Mexique, oblige vraisemblablement le Canada à mettre en œuvre une large immunité semblable au *US Communications Decency Act,* s. 230.[3] L'article 19.17 se limite à la responsabilité civile, les cadres réglementaires et les recours équitables sont donc susceptibles de se trouver hors de portée.[4]

La proposition de préjudices en ligne pourrait créer un nouvel organisme de réglementation – une commission de sécurité du numérique – composé d'un commissaire (semblable au rôle du commissaire fédéral à la protection de la vie privée), d'un conseil de recours (organisme juridictionnel pour les décisions de modération de contenu) et d'un conseil consultatif.[5] Des organismes de réglementation ont été proposés ou créés dans d'autres juridictions, dont au Royaume-Uni, en Australie et à l'Union européenne.[6]

---

[1] *Act to establish a legal framework for information technology*, CQLR *c* C-1.1.

[2] RSC 1985, *c* C-42 modifié par le *Copyright Modernization Act*, 2012, *c* 20, ss. 41.25-41.27.

[3] 47 USC§ 230.

[4] Réf. : recours équitables, voir Vivek Krishnamurthy et Jessica Fjeld, *CDA 230 Goes North American? Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States* - CIPPIC (Juillet 2020), https://cippic.ca/en/news/CDA_230_goes_north_american.

[5] Voir guide de discussion et article technique sur https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.

[6] Voir *Draft Online Safety Bi/12021* (Royaume-Uni) sur https://www.gov.uk/government/publications/draft-online-safety-bill, Commission de sécurité en ligne de l'Australie, https://www.esafety.gov.au/, et le *Digital Services Act,* proposé par l'Union européenne, lequel créerait un Conseil européen pour les services numériques, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.

D'autres lois à prendre en compte sont les obligations en matière de retrait de contenu dans le *Code criminel*[7], le droit d'être retiré de la liste conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques*[8] et une loi pour punir la diffusion d'images intimes.[9]

Considérations

Les mécanismes doivent minutieusement équilibrer plusieurs éléments : l'innovation et la promotion de la concurrence, la protection des droits de la personne, la protection contre les préjudices, la liberté des entreprises et la responsabilisation, et l'accès à la justice. Toutes les plateformes sont internationales. En conséquence, tout mécanisme juridique potentiel doit être analysé dans le contexte des droits internationaux de la personne et être compris dans son contexte mondial.

L'expression légitime, mais affreuse, est à la base de ce qui devient une expression illicite. La loi ne doit aborder que *directement* les discours illicites, mais elle peut réglementer *indirectement* les préjudices découlant des discours légitimes en mettant l'accent sur les façons dont une loi peut inciter la responsabilité d'entreprise, la standardisation de l'industrie, l'accès à des mécanismes de recours et ainsi de suite.[10] En bref, le modèle ou le système commercial peut être ciblé pour réduire indirectement les discours préjudiciables.

S'attaquer aux préjudices en ligne requiert plusieurs stratégies, notamment de nature technique, légale, éducative, normative, de marché, comportementale et sociale. La loi peut être une avenue pour donner vie à ces stratégies. Les modèles juridiques traditionnels (sphère de sécurité par exemple) sont enrichis ou remplacés par des solutions créatives : devoir de vigilance, traitements différenciés des plateformes, rapports de transparence, signaleurs de confiance, exigences d'équité procédurale.

Recommandations

Recommandations générales

- Recommandation d'un cadre de responsabilité civile et création d'une commission (pour les mécanismes juridiques et non juridiques). Ceux-ci servent différentes fins qui sont également complémentaires.
- Idéalement, la résolution de litiges en ligne doit être disponible contre la prise de décision par la plateforme et l'individu qui a affiché le contenu. Ou des processus judiciaires simplifiés peuvent être envisagés pour certains types de préjudices, dont la diffusion d'images intimes.[11]
- Différents types de préjudices doivent être traités différemment. La responsabilisation algorithmique doit être abordée séparément.
- À moins d'être adéquatement équipé de ressources et soigneusement conçu, un organisme de réglementation n'améliorera pas la responsabilisation des plateformes ni la transparence. Enjeux à prendre en considération : plaintes spécieuses, volume et vitesse, processus, mécanismes de protection des droits de la personne et fardeau de la preuve.
- Les mécanismes de plaintes des plateformes et les organismes de contrôle interne sont des mécanismes d'entreprise cruciaux pour s'attaquer aux discours préjudiciables, trouver des solutions techniques et organisationnelles et démontrer du respect pour les droits de la personne.

[7] RSC 1985, c C-46, exemple, propagande terroriste (s. 83.222), une image intime, enregistrement voyeuriste et pornographie juvénile (s. 164.1) et propagande haineuse (s. 320.1).

[8] SC 2000, c 5; *References Re Subsection 18.3(1) of the Federal Courts Act,* 2021 FC 723.

[9] L'Alberta, la Saskatchewan, le Manitoba, la Nouvelle-Écosse et Terre-Neuve-et-Labrador ont adopté des lois sur la diffusion d'images intimes, mais aucune ne traite explicitement de la responsabilité des intermédiaires. L'accent des lois porte sur la responsabilité des premiers transgresseurs qui ont partagé les images intimes sans consentement.

[10] Emily B. Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (CUP, 2015), chapitre 6.

[11] Voir Emily B. Laidlaw, *Re-Imagining Resolution of Online Defamation Disputes* 56(1) OHLJ (2018) 162 et Emily B. Laidlaw and Hilary Young, *Creating a Revenge Porn Tort,* 96(2) SCLR (2020).

Ils ne remplacent pas un mécanisme basé sur l'état, mais un important complément à celui-ci.

Enjeux particuliers

- La préparation de rapports concrets de transparence est difficile. Les obstacles comprennent un manque de mécanisme d'application, la sélection des données qui doivent être incluses dans les rapports, le contrôle visant à assurer des rapports rédigés de bonne foi et l'incitation à la responsabilisation et non pas seulement à l'explication. Une option est d'élargir la responsabilisation à une diligence raisonnable obligatoire.[12]
- Exploration de ce qu'est un cadre pour la prise de décisions raisonnables et d'un système tampon pour les erreurs.[13] Les plateformes peuvent être une source de solutions novatrices, et chacune des plateformes est différente. Il faut envisager différentes obligations pour les différents types de plateformes. La *Législation sur les services numériques*[14] établit une distinction entre les plateformes et les très grandes plateformes en fonction du nombre d'utilisateurs actifs sur une base mensuelle.
- Examen du cadre de responsabilité civile adéquat pour les torts. Bien qu'incertain, un modèle de devoir d'agir de manière responsable/devoir de vigilance est attrayant parce qu'il cible le système de modération de contenu de la plateforme.[15] Hilary Young et moi proposons un cadre d'avis et avis pour la diffamation.[16] L'intermédiaire serait requis d'acheminer les avis aux créateurs de contenu, et si le créateur de contenu répond, l'intermédiaire n'entreprend aucune démarche. Si le créateur de contenu ne répond pas, alors l'intermédiaire devrait désactiver l'accès au contenu avec un risque de dommages-intérêts d'origine législative à défaut de le faire.
- C'est la multitude de petites décisions qui comptent, car collectivement elles peuvent créer un écosystème Internet qui équilibre les droits. Par exemple, les procédures de retour, les déclarations de bonne foi, le signalement des contenus et les mécanismes de plaintes accessibles peuvent être ce qui différencie les lois qui violent les droits de celles qui les protègent. L'enjeu est que les solutions techniques requièrent une certaine quantité d'expérimentations. Qui devrait avoir le contrôle de ces expérimentations? Il faut envisager les types de règlements qui pourraient être utiles : fondés sur la finalité (commandes générales, ouverts quant à la façon dont une plateforme atteint les objectifs, utiles lors de l'asymétrie d'information), fondés sur des moyens (mandats de spécifications techniques, utiles lorsque les connaissances sont égales) et méta (autoréglementation imposée, relativement interventionnistes et utiles lorsque les cibles sont diverses, que les problèmes sont complexes et que l'asymétrie d'information est prononcée) [17].

[12] Mackenzie Common, *Rule of law and human rights issues in social media content moderation* (2020), thèse de doctorat,London School of Economics and Political Science, chapitre 7.

[13] Marcelo Thompson, *Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries* (2016) 18(4) Vanderbilt Journal of Entertainment & Technology Law.

[14] *Supra* note 6, Article 25.

[15] UK *Draft Online Safety Bi/12021, supra* note 6 et le rapport de cette commission : *Harm Reduction: A Six-Step Program to Protect Democratic Expression Online*, Forum des politiques publiques (janvier 2021).

[16] Emily B. Laidlaw et Hilary Young, *Internet Intermediary Liability in Defamation* 56(1) OHLJ (2018) 112.

[17] Cary Coglianese et Evan Mendelson, *Meta-Regulation and Self-Regulation in Robert Baldwin, Martin Cave and Martin Lodge,* ed, *The Oxford Handbook of Regulation* (Oxford University Press, 2010).