RAPPORT FINAL 2022

Commission canadienne sur l'expression démocratique

Comment rendre les plateformes en ligne plus transparentes et plus responsables envers les utilisateurs rices canadiens

MAI 2022

DEMOCRATIC EXPRESSION DÉMOCRATIQUE

PUBLIC POLICY FORUM
FORUM DES POLITIQUES PUBLIQUES
PPF

PUBLIC POLICY FORUM
FORUM DES POLITIQUES PUBLIQUES

Le Forum des politiques publiques travaille avec tous les niveaux du gouvernement et de la fonction publique, le secteur privé, les syndicats, les établissements d'enseignement postsecondaire, les ONG et les groupes autochtones afin d'améliorer les retombées des politiques pour les Canadiens. En tant qu'organisation non partisane, basée sur ses membres, nous travaillons "de l'inclusion à la conclusion ", en organisant des discussions sur des questions politiques fondamentales et en identifiant de nouvelles options et des voies à suivre. Depuis plus de 30 ans, le FPP fait tomber les barrières entre les secteurs, contribuant ainsi à des changements significatifs pour bâtir un meilleur Canada.

1400 - 130 rue Albert

Ottawa, ON, Canada, K1P 5G4

Tél : 613.238.7858

www.ppforum.ca

ISBN: 978-1-77452-115-1

TABLE DES MATIÈRES

À PROPOS DE L'INITIATIVE

DEMOCRATIC EXPRESSION
DÉMOCRATIQUE

La Commission canadienne de l'expression démocratique est une initiative de trois ans dirigée par le Forum des politiques publiques, qui vise à permettre un examen concerté et rigoureux de l'état de la démocratie canadienne et des mesures qui pourraient la renforcer. Une petite commission délibérante est au cœur de cette initiative. Elle s'appuiera sur des travaux de recherche antérieurs originaux, sur les avis de différents experts et les délibérations d'une assemblée citoyenne représentative afin de déterminer ce qu'il faut faire pour contrer les préjudices en ligne et favoriser le bien commun. La Commission est chargée de proposer chaque année des avis et des options de politiques qui soutiennent la démocratie et la cohésion sociale du Canada. Elle sera soutenue par des assemblées citoyennes nationales et par un programme de recherche indépendant.

Cette initiative découle de précédentes observations sur la relation entre les technologies numériques et la démocratie canadienne. Cette relation était au cœur du rapport novateur *Le miroir éclaté* et des recherches multidisciplinaires subséquentes du Forum des politiques publiques (FPP) présentées dans le rapport *La démocratie divisée* (en collaboration avec l'Université de la Colombie-Britannique), ainsi que du Digital Democracy Project, un partenariat avec l'Université McGill.

L'initiative est réalisée en partenariat avec MASS LBP et le Centre for Media, Technology and Democracy à l'École de politiques publiques Max Bell de l'Université McGill, responsables respectivement des assemblées citoyennes nationales et du programme de recherche.

Afin d'en savoir plus sur cette initiative et les manières de vous impliquer, veuillez vous rendre au ppforum.ca/fr/project/expression-democratique. Cettte initiative restera effective d'Avril 2020 à Mars 2023.

Ce projet a été rendu possible en partie grâce au gouvernement du Canada.
Le FPP tient également à remercier la Fondation McConnell pour son soutien.

Canada

La Fondation McConnell Foundation

EDWARD GREENSPON

AVANT-PROPOS

Les mois qui ont précédé ce deuxième rapport de la Commission canadienne de l'expression démocratique ont été marqués par un mouvement domestique de protestation alimenté par Internet et par l'invasion de l'Ukraine par le principal intrus, en ligne et hors ligne, dans les affaires démocratiques des autres nations. Dans les deux cas, Internet et sa ramification la plus influente, les médias sociaux, ont joué leurs rôles dans le partage, la sélection, le classement et l'amplification de l'information, de mésinformation et de désinformation.

Le fait qu'Internet possède une capacité sans précédent de distribuer les véritables biens sociaux que sont les nouvelles et les opinions mérite d'être célébré quotidiennement. Comme l'imprimerie avant elle, cette technologie de communication est dotée de puissantes forces démocratisantes. Elle donne la parole aux personnes marginalisées, élargit l'accès à la connaissance et permet aux relations humaines de transcender les limites physiques.

Mais il convient de ne pas ignorer son côté sombre. Les déformations intentionnelles de la vérité et le ciblage de groupes et d'individus par des flots constants de haine, de harcèlement et d'humiliation minent la cohésion et le bien commun qui sous-tendent les sociétés bien organisées. L'essence même de l'expression démocratique est pervertie, car les personnes victimes de violence en ligne sont chassées de la place publique. L'imprimerie a également connu ses excès, mais ceux d'Internet sont sans commune mesure.

Le Forum des politiques publiques travaille depuis plus de cinq ans sur des questions de politique du système d'information et a publié les rapports tels que *Le Miroir éclaté, La Démocratie divisée, Ce que les Roughriders de la Saskatchewan peuvent enseigner au journalisme canadien [en anglais seulement], Diminuer un tort et Le miroir éclaté, cinq ans plus tard*. Chacun de ces rapports traite des répercussions des nouvelles technologies de l'information et de la communication sur la santé de notre démocratie, et des mesures qui peuvent être prises pour remédier aux conséquences de l'état affaibli du journalisme sur l'état pollué du discours en ligne sans mettre en danger la liberté d'expression.

Si le médium est le message, comme l'affirmait Marshall McLuhan, quel est le message contenu dans nos flux contemporains de communications? Quel est l'effet collectif de leur vitesse, de leur volume, de leur portée et de leur caractère continu? Ces qualités conduisent-elles à privilégier le jugement rapide à la réflexion, la condamnation à l'empathie, la communauté virtuelle à la communauté physique, l'expérience à l'expertise, l'émotion à la raison?

Fondamentalement, comment faire en sorte que ceux/celles qui programmant les décisions éclairs d'Internet à l'aide d'algorithmes assument la responsabilité de ce qu'ils/elles font, et choisissent d'en éliminer les effets pervers? Bien qu'il puisse ressembler à un espace ouvert, Internet est depuis longtemps colonisé par les intérêts de très grandes entreprises qui exercent une domination sur ce qui circule et est mis en valeur sur de vastes étendues du terrain informationnel. Elles opèrent des choix qui ont de graves répercussions sur les sociétés.

Le premier rapport de la Commission canadienne de l'expression démocratique, *Diminuer un tort*, publié en 2021, portait sur le contenu d'Internet, plus particulièrement sur les défis que posent la haine en ligne et les préjudices qui en découlent. Il proposait un programme en six étapes, commençant par l'obligation pour les entreprises propriétaires de plateformes de veiller à la sécurité des utilisateurs.rices d'Internet, tout comme le ferait un.e propriétaire pour les locataires d'un complexe immobilier. Mais il ne s'agissait que d'un début – les commissaires ont estimé que le prochain cycle devrait aller plus loin dans la lutte contre les préjugés structurels qui favorisent certains types d'informations indépendamment de leur vérité ou de leur utilité. Si, plus que des actes aléatoires de personnes mal intentionnées, ces abus étaient d'une certaine façon la résultante de choix systémiques, que pourrait-on et devrait-on faire à ce sujet?

Tel est le point de départ de ce deuxième rapport de la Commission. Il va au-delà du contenu que nous pouvons tous voir pour faire enquête sur la manière dont il a pris de l'ampleur, et comment la haine ou la désinformation d'une personne se traduit par le cri de ralliement d'une foule ou le trouble de l'ordre social. Comme le verront les lecteurs.rices du présent rapport, ces résultats sont le produit de deux facteurs liés : les entrées de milliards de données et les systèmes algorithmiques en boîte fermée qui gèrent, agrègent et distribuent ces données pour maximiser l'engagement de l'audience et les revenus publicitaires. Ce rapport examine ce qu'il faut faire pour assurer un meilleur équilibre des pouvoirs sur ces systèmes de contrôle.

Je tiens à remercier les neuf commissaires qui se sont attelés à cette tâche colossale de découverte et de délibérations avec une courtoisie qui devrait servir de modèle à l'ère numérique. Je remercie également le rédacteur principal Chris Waddell, nos partenaires de recherche au Centre for Media, Technology and Democracy de l'Université McGill, ainsi que les membres de l'Assemblée citoyenne sur l'expression démocratique parallèle et ses architectes au MASS LBP, sans oublier mes collègues du Forum des politiques publiques.

Edward Greenspon
Président-directeur général
Forum des politiques publiques

RÉSUMÉ

Après six mois d'étude et de délibérations, la Commission canadienne de l'expression démocratique a établi une série de principes et de recommandations qui sous-tendent un plan d'action pratique pour le public, les gouvernements et les plateformes de médias sociaux afin de protéger l'expression démocratique au Canada et de contrer les préjudices créés par le contenu publié, partagé et amplifié par les plateformes de médias sociaux. Nous reconnaissons la complexité des enjeux en question dans une société libre, démocratique et fondée sur les droits, et proposons ces recommandations comme voie à suivre. Nous encourageons le débat qui pourrait les affiner davantage et conduire à leur mise en œuvre dans les mois à venir par les gouvernements et les organismes de réglementation.

Principes

1. La liberté d'expression est fondamentale pour une société démocratique. Internet permet à un plus grand nombre de personnes de participer à des discussions et des débats publics.

2. La montée de la haine, de la désinformation, du contenu politiquement polarisant, des théories du complot, de l'intimidation et d'autres communications nuisibles en ligne mine ces acquis et ont une incidence corrosive sur l'expression démocratique au Canada, tant en ligne que hors ligne.

3. Le statu quo qui consiste à laisser la modération des contenus à la seule discrétion des plateformes n'a pas réussi à endiguer la propagation de ces préjudices. Les entreprises numériques peuvent se trouver en conflit entre leurs intérêts privés et le bien public.

4. Il est erroné de considérer que les plateformes sont des diffuseurs d'information neutres. Les plateformes distribuent du contenu pour servir leurs intérêts commerciaux et doivent donc assumer une plus grande responsabilité pour les préjudices qu'elles amplifient et propagent tout en gardant à l'esprit que la liberté d'expression est le rempart d'une société démocratique.

5. Les organismes publics doivent jouer un rôle plus actif dans la promotion de l'expression démocratique et la protection des Canadiens et Canadiennes contre les préjudices en ligne.

6. Toute politique adoptée doit privilégier les individus, réduire les préjudices en ligne et prévenir les risques d'une trop grande censure du contenu par ses propositions de solutions, en particulier pour les Autochtones et les autres groupes en quête d'équité. Cela exige une approche équilibrée et à plusieurs volets.

7. La protection de la vie privée est fondamentale pour les droits de la personne et l'expression démocratique. Les recours visant à remédier aux préjudices en ligne et à protéger l'expression démocratique doivent être axés sur des approches fondées sur les droits, tant pour protéger les citoyen.ne.s contre d'éventuelles atteintes à la vie privée que pour donner aux individus un plus grand contrôle sur leurs données et leur expression démocratique.

8. Les mineur.e.s (moins de 18 ans) sont particulièrement vulnérables aux préjudices en ligne et les plateformes auxquelles ils/elles accèdent ont donc une obligation particulière de mettre en place des garanties appropriées.

9. De nombreuses démocraties qui partagent ses vues font face à des défis similaires en matière d'expression démocratique au 21e siècle et, à ce titre, le Canada devrait chercher à agir de manière multilatérale et de concert avec d'autres nations aux vues similaires, dans la mesure du possible et là où cela est le plus logique.

Ces principes ont amené la Commission à adopter un ensemble de recommandations interdépendantes autour de trois thèmes fondamentaux de l'expression démocratique : la transparence, la responsabilité et l'autonomisation.

Recommandations

THEME 1 : TRANSPARENCE

1.1. Mandat et pouvoir de contrainte : mettre sur pied et habiliter un organisme de réglementation pour imposer et permettre l'accès, à des fins de recherche et de surveillance, aux données contenues dans les plateformes de médias sociaux.

L'organisme de réglementation veillera à l'application des exigences obligatoires en matière d'accès et de partage des données de la plateforme définies dans la législation pour chacun des trois niveaux suivants : le grand public, les chercheurs.euses et les journalistes accrédités, et les recherches plus spécialisées et

détaillées dans l'intérêt public qui, sans garanties supplémentaires importantes, pourraient avoir des répercussions sur la vie privée.

1.2. Mettre en œuvre un accès hiérarchisé aux données : imposer des niveaux distincts d'accès aux données avec des garanties pour le public, les chercheurs.euses, les journalistes et les groupes de la société civile[1].

Instaurer des niveaux hiérarchisés de droits d'accès aux données pour les plateformes afin d'accorder au public un accès de niveau inférieur (niveau 1); d'accorder aux chercheurs.euses, aux acteurs.rices de la société civile et aux journalistes un accès de niveau intermédiaire (niveau 2); et d'accorder à un nombre restreint de candidat.e.s menant des recherches spécialisées d'intérêt public un accès nécessitant des garanties détaillées plus importantes afin d'équilibrer la protection de la vie privée avec la nécessité d'une plus grande transparence et d'une plus grande responsabilité des plateformes (niveau 3).

1.3. Imposer une transparence universelle sur la publicité numérique.

Instaurer une obligation pour les plateformes de divulguer régulièrement et d'archiver, sous un format normalisé, des informations précises sur chaque publicité numérique et contenu payant publié sur leurs plateformes. La divulgation et l'archivage doivent être universels, ce qui signifie que les plateformes doivent présenter les données sous un format normalisé lisible par machine, avec des normes minimales communes de divulgation. Toutes ces données doivent être conservées dans une archive unique et centrale dont le contenu doit être accessible aux trois niveaux d'utilisateurs énumérés dans les recommandations précédentes.

1.4. Instaurer des protections renforcées en faveur des dénonciateurs.

Au regard des risques économiques, professionnels ou personnels auxquels les dénonciateurs peuvent être exposés, toute recommandation visant à protéger les personnes qui signalent et dénoncent les malversations internes des entreprises devrait offrir une garantie contre les représailles juridiques, économiques et réputationnelles de la part de leurs employeurs. Le gouvernement fédéral pourrait s'inspirer d'autres secteurs pour renforcer la protection des dénonciateurs privés.

THEME 2 : RESPONSABILISATION

2.1. Accroître les capacités des organismes publics : veiller à ce que les organismes de réglementations existants soient correctement habilités et outillés pour travailler dans le monde numérique du 21e siècle de manière efficace et efficiente. De plus, mettre en place un nouvel organisme fédéral de réglementation indépendant (comme indiqué ci-dessus et proposé dans le premier rapport de la Commission) doté de pouvoirs et de responsabilités en matière d'enquête, d'audit et de contrainte pour faire en sorte qu'une nouvelle obligation législative d'agir de

manière responsable soit imposée aux plateformes. Au fil du temps, le nouvel organisme sera également chargé d'examiner systématiquement les politiques et les réglementations et de formuler des propositions de réforme si nécessaire.

Ce nouvel organisme de réglementation, dont le mandat principal est de superviser et de faire respecter l'obligation d'agir de manière responsable, se focaliserait sur les systèmes et les opérations des plateformes à l'intérieur de la « boîte fermée » afin de promouvoir et d'assurer la transparence et la responsabilisation, d'enquêter sur les préjudices perçus, d'évaluer la responsabilité de la plateforme, et de déterminer et d'appliquer des solutions lorsque la responsabilité de la plateforme est établie. L'organisme de réglementation doit être officiellement indépendant du gouvernement, des médias grand public et des plateformes. Il est crucial de doter l'organisme de ressources adéquates et de le concevoir correctement, après des consultations publiques pour étoffer son champ d'action et ses attributions. L'organisme de réglementation doit fonctionner de manière transparente et responsable, et rendre compte au Parlement à intervalles réguliers, conformément à la loi.

2.2. Imposer des obligations à plusieurs niveaux pour différents types de plateformes et/ou pour les services susceptibles d'être consultés par des mineur.e.s et des adultes.

Toutes les plateformes, quelle que soit leur taille, sont tenues d'agir de manière responsable. Toutefois, les obligations imposées aux plateformes individuelles peuvent différer selon le type et la taille de celles-ci et en fonction de leur capacité à se conformer aux exigences de la législation. Il y aurait également une différenciation entre les obligations imposées aux plateformes en fonction de leur utilisation par les mineur.e.s (moins de 18 ans), et les adultes.

2.3. Légiférer sur les exceptions et les protections de responsabilité des intermédiaires en matière de responsabilité des plateformes.

En précisant les cas où les plateformes peuvent être tenues légalement responsables des conséquences néfastes générées par leurs systèmes de recommandation algorithmique et leurs outils d'amplification, on les encouragerait à mieux modérer le contenu généré par les utilisateurs.rices. Il faut autoriser, avec discernement, les utilisateurs.rices à exprimer librement leurs opinions en ligne (dans les limites prévues par la loi canadienne). Dans le même temps, le fait de rendre les plateformes entièrement responsables des préjudices découlant de l'expression des utilisateurs.rices peut entraîner une suppression excessive de contenu et la censure. Néanmoins, la mesure dans laquelle le contenu problématique est amplifié et l'incidence des systèmes de recommandation sur l'opinion publique doivent être prises en considération dans l'examen du rôle des plateformes dans les sociétés démocratiques.

2.4. Habiliter les organismes de réglementation à développer et mettre en œuvre un cadre de responsabilité algorithmique fondé sur les droits qui comprend des

évaluations de l'incidence algorithmique (EIA), des évaluations de l'incidence sur les droits de la personne (EIDP) et des audits algorithmiques.

Il faut donner aux organismes de réglementation compétents le pouvoir d'élaborer et de mettre en œuvre un cadre de responsabilité algorithmique solide, axé sur des approches de la gouvernance algorithmique fondée sur les droits. Le fait de placer les droits au centre des cadres de responsabilité des systèmes automatisés de prise de décision est conforme aux normes internationales visant à traiter les risques accrus pour la sécurité et les libertés fondamentales, tels que le droit à la non-discrimination[2].

2.5. Élaborer un code de pratique sur la désinformation.

En collaboration avec les principales plateformes en ligne, le Canada doit élaborer un code de pratique sur la désinformation établissant des engagements et des exigences. L'objectif général du Code est de promouvoir l'élaboration de politiques et de procédures relatives aux plateformes pour lutter contre la désinformation, notamment en démonétisant les contenus problématiques, en améliorant la transparence des publicités politiques et thématiques, en donnant aux utilisateurs.rices les moyens de mieux contrôler leurs activités en ligne et en permettant un accès aux données respectueux de la vie privée pour les activités de vérification des faits et de recherche.

THEME 3 : AUTONOMISATION

3.1. Soutenir le développement des connaissances, des relations et des protocoles autochtones et la gouvernance des données des Autochtones pour les collectivités autochtones.

Soutenir une participation significative des Autochtones et veiller à intégrer les relations et protocoles autochtones dans l'élaboration des politiques, outils et mécanismes technologiques et sociaux. Le gouvernement fédéral doit collaborer avec les Autochtones, les collectivités et les organisations pour s'assurer que les droits de gouvernance des données des Autochtones sont respectés et que ceux-ci possèdent les moyens de mener à bien les programmes qu'ils ont eux-mêmes définis. Le soutien supplémentaire devrait inclure le financement, la création de nouvelles propositions législatives, des programmes de littératie autour de la propriété des données et de l'autodétermination, et d'autres besoins recensés en partenariat avec les peuples et collectivités autochtones.

3.2. Renforcer considérablement l'éducation civique en matière de respect des droits, de littératie numérique et d'accès à l'information de qualité pour soutenir les groupes en quête d'équité et les programmes pilotés par les collectivités.

Les initiatives d'éducation publique et de littératie numérique doivent permettre au public de comprendre ses droits et libertés, le fonctionnement des médias numériques, l'incidence qu'ils peuvent avoir sur l'opinion publique et la manière dont les préjugés structurels y opèrent et renforcent les inégalités dans la vie réelle. Il

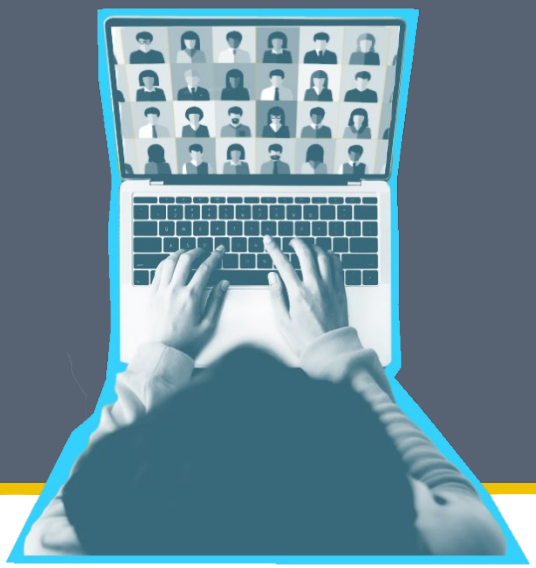
s'agit notamment de doter les citoyen.ne.s de compétences leur permettant de reconnaître les préjugés et d'évaluer la fiabilité de l'information, de savoir comment rechercher, naviguer, synthétiser et évaluer le contenu en ligne, et de savoir comment participer utilement aux communautés en ligne. Les groupes sous-représentés devraient être soutenus par des politiques et des programmes ciblés qui renforcent l'équité, y compris le financement de la production numérique des cultures et des connaissances autochtones. Les programmes doivent être proposés dans plusieurs langues, y compris les langues autochtones.

3.3. Rendre obligatoires l'interopérabilité et la mobilité des données.

Les systèmes d'information doivent pouvoir interagir et échanger régulièrement des informations entre eux, ce qui permettrait à d'autres acteurs tels que les jeunes entreprises et les coopératives de plateformes de se connecter aux services existants. Le Canada devrait assurer l'interopérabilité des services numériques afin de donner aux gens un plus grand choix et un meilleur contrôle sur leurs interactions en ligne. De plus, le Canada doit introduire le droit à la portabilité des données – donnant aux gens le droit de voir leurs données personnelles transmises directement d'une plateforme à une autre, sans entrave.

3.4. Moderniser la législation canadienne sur la protection de la vie privée.

Le Canada doit mettre à jour sa législation sur la protection de la vie privée afin d'adopter un cadre fondé sur les droits pour les développements technologiques actuels et futurs. Il faudrait conférer au commissaire à la protection de la vie privée du Canada une plus grande autorité pour moderniser le cadre législatif actuel du Canada en matière de protection de la vie privée et décider de la manière dont les entreprises de plateformes privées peuvent recueillir, traiter et cibler les données personnelles.



PRÉAMBULE DE LA COMMISSION

Il y a un an, le premier rapport de la Commission notait déjà : « Nous saluons la capacité inouïe d'Internet et des médias sociaux en particulier de réduire les obstacles à la participation au domaine public. Ils ont renforcé notre démocratie en donnant aux individus de nouvelles façons de se faire entendre, de s'organiser politiquement, d'interpeller les représentants élus et de rendre les pouvoirs responsables.

Aujourd'hui, n'importe qui a le pouvoir d'élire domicile et de s'exprimer sur Internet. Plus de personnes que jamais peuvent bénéficier d'un meilleur accès aux connaissances, à l'action communautaire et collective. Mais il y a aussi un côté sombre à cela. Autant l'espace public est devenu plus ouvert et accessible, autant il est devenu, à bien des égards, moins sécuritaire et moins fiable. Cela représente l'un des paradoxes et l'un des défis centraux de notre époque – et du présent rapport[3]. »

Un an après, tout cela reste vrai. Pourtant, il est également vrai que les marées montantes de la haine, de la désinformation, des théories du complot, de la misogynie, de l'intimidation et d'autres communications préjudiciables en ligne se sont transformées en déluge. Ce tsunami de préjudices sociaux et démocratiques contribue à chasser les femmes, les minorités, les peuples autochtones et d'autres personnes de la sphère publique numérique.

Le harcèlement en ligne affecte et façonne nos expériences hors ligne avec des effets néfastes pour l'expression démocratique. Il pervertit la politique au quotidien et peut détériorer les relations dans les familles, sur les lieux de travail, dans les écoles et dans les collectivités.

La désinformation mine le débat public en nous privant d'une compréhension commune des faits. Enfermer les citoyens dans des silos d'information compromet notre capacité de prendre des décisions collectives. Cela est particulièrement grave dans un pays diversifié comme le Canada où l'accommodement et la cohésion sociale sont des valeurs nécessaires.

Nous ne pouvons pas laisser les personnes qui cherchent à entraver l'expression démocratique au Canada détourner cette grande occasion d'enrichissement démocratisant. La liste des préjudices est longue : misogynie, racisme, antisémitisme, islamophobie, suprématie blanche, homophobie, désinformation, faits alternatifs, intimidation, critiques de consommation falsifiées, fraude contre les aînés, encouragement au suicide, théories du complot, attaques contre l'intégrité électorale, incitation à la violence, et ainsi de suite. Nous en sommes au point où les cibles du harcèlement sentent parfois que la menace à leur santé et leur sécurité les oblige à se retirer de l'espace public numérique – le contraire même de l'expression démocratique.

Les plateformes en ligne n'ont pas fait preuve d'une diligence suffisante pour contrer ces méfaits. En effet, leurs systèmes sont à bien des égards complices. Les discours néfastes et haineux ne sont pas tant des anomalies que les produits logiques des structures, de l'architecture, des politiques et des pratiques des médias sociaux.

Comme l'an dernier, la Commission a travaillé parallèlement avec la deuxième Assemblée citoyenne sur l'expression démocratique organisée par le FPP, composée de 42 Canadiens et Canadiennes venus des 10 provinces et des trois territoires qui ont formulé leurs recommandations lors d'une série de réunions en ligne et en présentiel à l'automne 2021. Leur rapport de janvier 2022 doit être lu conjointement avec le présent rapport[4]. Il a été remarquablement rassurant d'observer le processus de l'Assemblée citoyenne. Alors que l'on s'attendait à ce que le débat et la discussion en ligne sur ces enjeux soient clivants et toxiques, il est remarquable de constater à quel point la discussion devient courtoise lorsqu'on réunit 42 Canadiens et Canadiennes de tous les horizons et de toutes les sensibilités idéologiques. Bien que tous/toutes se soient engagés dans le processus en possédant leurs propres expériences, idées subjectives et points de vue sur le problème et le rôle du gouvernement dans la solution, ils/elles sont repartis étonnamment unis. Les commissaires étaient très conscients de cette réalité lors des délibérations de cette année. Les citoyen.ne.s veulent de l'action et sont beaucoup plus unis que le discours en ligne et dans les médias pourrait nous le faire croire. Nous avons rédigé nos recommandations dans ce rapport en gardant à l'esprit les dernières recommandations de l'Assemblée citoyenne.

Cela étant, il est de la responsabilité des gouvernements de protéger ses citoyens et citoyennes contre les préjudices sociaux, de défendre les personnes ciblées et d'affirmer le plus grand intérêt public par la gouvernance appropriée des plateformes, des moteurs de recherche et d'autres fournisseurs directs ou accessoires de contenu. Les recommandations de ce rapport proposent aux gouvernements comment trouver un équilibre dans ce domaine.

Nous savons qu'il y a beaucoup de contenu illicite en ligne : propagande haineuse, harcèlement, menaces, qui doit être combattu. L'application des lois existantes relève de la responsabilité des gouvernements. À long terme, l'incapacité à faire appliquer les réglementations et les lois actuelles menace l'État de droit. Le

présent rapport recommande des mesures nouvelles et supplémentaires pour limiter les préjudices en ligne, et ne doit pas être lu comme un rejet des efforts visant à faire respecter notre régime juridique existant.

Cependant, il y a beaucoup de choses en ligne qui sont « légales, mais abominables » et qui sapent et nuisent à l'expression démocratique comme nous l'avons souligné. Mais il est important de comprendre que les préjudices causés à l'expression démocratique en ligne ont également un effet direct sur le monde « hors ligne », notamment sur la façon dont la politique se déroule dans l'isoloir et sur la façon dont les individus interagissent sur le lieu de travail, dans les écoles et en public. Dans des contextes mondiaux particuliers, les incitations à la violence et le harcèlement en ligne ont des répercussions directes sur des événements hors ligne qui, à leur tour, ont d'énormes implications pour la démocratie, notamment le rôle des médias sociaux dans les blocages de la frontière entre le Canada et les États-Unis et l'occupation du centre-ville d'Ottawa par des manifestant.e.s en février 2022, ainsi que l'attentat du 6 janvier 2021 contre le Capitole aux États-Unis et le génocide au Myanmar.

Dans ce monde d'expression « légale, mais abominable », les utilisateurs.rices sont à la fois victimes et auteur.e.s. Des individus et des organisations publient des contenus misogynes et intimidants, qui ne constituent que deux exemples des nombreux préjudices mentionnés ci-dessus. D'autres utilisateurs.rices partagent ces messages préjudiciables, amplifiant les préjudices créés et les diffusant à un public plus large. Les utilisateurs.rices doivent veiller à ne pas publier de contenu préjudiciable, tandis que les plateformes doivent se préoccuper de la manière dont ce contenu est amplifié et partagé, ainsi que de son retrait lorsqu'il fait l'objet d'une plainte de la part d'un.e utilisateur.rice ou de personnes heurtées par ce contenu, ou lorsqu'il représente une menace imminente pour une personne.

Plus généralement, ces devoirs trouvent leur fondement dans ce que nous sommes en tant que société. Grâce à notre Charte des droits et libertés, les Canadiens et Canadiennes sont fiers de vivre dans une société fondée sur les droits, dans un État de droit basé sur le respect et la protection des droits de la personne. Cela inclut les droits individuels, mais aussi les droits des groupes et communautés marginalisés dans une nation multiculturelle. La montée de la désinformation et de la mésinformation en ligne pose de nouveaux défis à notre société, nécessitant une réponse multiforme de nos gouvernements et institutions, comme le propose le récent deuxième rapport de l'Assemblée citoyenne.

Que signifiera et à quoi ressemblera l'expression démocratique à l'avenir? Ce qui se limitait naguère à la parole est devenu multimédia et bénéficie d'une portée et d'une incidence mondiales instantanées grâce aux plateformes de médias sociaux. Cela inclut les publications d'acteurs.rices anonymes et de robots amplifiant les messages, conçus pour créer l'illusion d'un consensus autour de mensonges et de théories du complot. Les menaces à l'expression démocratique peuvent émerger même du contenu des jeux vidéo et des nouvelles technologies telles que la réalité augmentée et la place que le métavers peut jouer dans l'avenir de nous tous/toutes.

Les entreprises propriétaires de plateformes doivent s'engager à protéger, promouvoir et améliorer les droits de la personne, l'égalité et les responsabilités qui en découlent. Cela vaut tout particulièrement pour les enfants et leurs droits. Les enfants, les adolescent.e.s et les jeunes passent autant de temps, voire plus, sur les plateformes de médias sociaux que les adultes. L'incidence de ce qu'ils/elles publient, voient, entendent, lisent et partagent façonne le développement de leur cerveau et de leur identité d'une manière différente de celle des adultes. Le devoir des plateformes de médias sociaux d'agir de manière responsable doit particulièrement veiller, dans l'esprit et dans l'action, à ce que les activités des enfants sur les plateformes reçoivent une attention et une protection particulières. Les organismes de réglementation ont ici le devoir d'élaborer et d'appliquer les meilleures pratiques concernant les enfants et les médias dans le respect des défis distincts qui émergent des différents contenus et interactions. Le principe de minimisation des données doit être strictement appliqué lorsqu'il s'agit d'enfants.

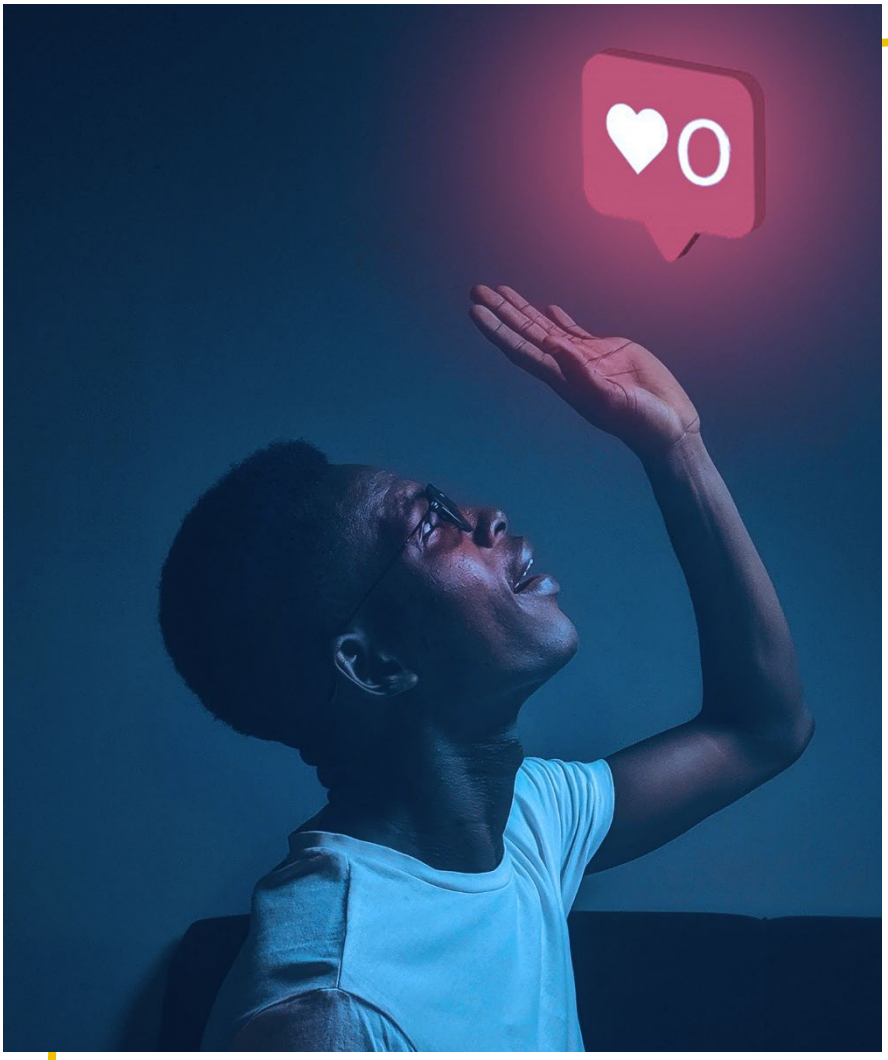
Enfin, le droit à la vie privée ne doit pas être compromis. De par leur nature, les menaces et les limites à la vie privée restreignent et risquent de compromettre directement l'égalité des individus et des groupes à exercer leurs droits à la participation et à l'expression démocratiques. Cela porte atteinte à la démocratie.

> **Les citoyen.ne.s ne peuvent pas participer à une démocratie sans un droit à la vie privée et la possibilité d'exercer un certain contrôle sur ce que les autres savent d'eux/elles.**

En ce qui concerne les plateformes de médias sociaux, leur collecte systématique de données enfreint le droit à la vie privée. Un consensus émerge dans le monde entier sur le fait que la collecte systématique de données peut également interférer avec d'autres droits de la personne, étant donné que la collecte gratuite de données et le profilage peuvent porter atteinte au droit à la liberté d'opinion[5]. La sensibilisation du public à la surveillance en ligne peut également conduire à l'autocensure, présentant un « effet dissuasif » de la collecte de données sur la participation et l'engagement du public[6]. Dans son tout premier rapport sur la désinformation, le Rapporteuse spéciale des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression estime que les garanties à la liberté d'expression et les garanties à la vie privée sont complémentaires. Les efforts du Canada pour protéger et promouvoir l'expression démocratique doivent être considérés comme un complément à sa modernisation de la législation sur la protection des données. Sans efforts conjoints et coordonnés, les gouvernements et les individus seront toujours en train de courir après le temps perdu – appliquant de petits pansements plutôt que s'attaquant à la cause des blessures.

Nous pensons que ces menaces à l'expression démocratique peuvent être contrées par la mise en place et l'application sur les plateformes de médias sociaux d'une obligation d'agir de manière responsable en vertu de trois thèmes interconnectés dans la définition de la relation entre les utilisateurs.rices de médias sociaux et les plateformes : la transparence, la responsabilisation et l'autonomisation.

L'objectif de nos recommandations est de parvenir à un équilibre plus équitable du pouvoir entre les utilisateurs.rices des médias sociaux et les plateformes qu'ils/elles utilisent, qui soit bénéfique aux deux.



Rick Anderson

Wendy Chun

Nathalie Des Rosiers

Amira Elghawaby

Merelda Fiddler-Potter

Philip N. Howard

Vivek Krishnamurthy

Beverley McLachlin

Taylor Owen

CHAPITRE UN : DÉFINITION DU PROBLÈME

Les médias sociaux ont changé une grande partie de nos vies au cours des deux dernières décennies.

Les Canadiens et Canadiennes utilisent couramment les médias sociaux pour rester en contact avec leur famille et leurs vieux ami.e.s, proches ou lointains, partageant les joies et les peines de leur vie, leurs photos et leurs vidéos, leurs espoirs et leurs rêves. Ils ont permis aux individus de se réunir en groupes et de nouer de nouvelles amitiés autour de leurs intérêts communs. Ils sont devenus le moyen par lequel beaucoup obtiennent leurs nouvelles et leurs informations, puis les partagent avec leurs ami.e.s et leurs connaissances. Les médias sociaux sont devenus une partie de la vie quotidienne que beaucoup attendent avec impatience de consulter régulièrement, que ce soit en publiant du contenu pour informer et impressionner leurs ami.e.s ou simplement pour tuer le temps en faisant défiler les publications des autres à la recherche de choses différentes, inattendues ou drôles qui attirent leur attention.

Plus le nombre d'utilisateurs.rices augmente sur les plateformes de médias sociaux, plus leur incidence collective augmente. Les entreprises de plateforme ont une grande influence sur le façonnement et la distribution des nouvelles et des informations à portée mondiale, pouvant, à n'importe quel moment, délivrer le message de toute personne, à tout le monde, ou à un micro-public délibérément sélectionné. La capacité des utilisateurs.rices à être présents en permanence sur les plateformes peut générer à celles-ci des revenus publicitaires et des profits massifs.

Comme l'indique le premier rapport de la Commission, publié en janvier 2021, les plateformes ne sont pas des diffuseurs neutres d'informations. Elles sélectionnent le contenu pour servir leurs intérêts commerciaux et ont une part de responsabilité dans les préjudices que le contenu peut amplifier et propager.

Plus précisément, nous sommes préoccupés par les préjudices causés à l'expression démocratique.

Il s'agit notamment de mésinformation et de désinformation, de mensonges, de menaces, de calomnies, d'intimidations, de pressions et d'humiliations, dirigés contre des politicien.ne.s, des fonctionnaires, des

organisations et des groupes d'intérêt, des journalistes, des communautés ethniques et des membres du public.

Nombre de ces préjudices ne sont pas nouveaux, mais l'ampleur des plateformes de médias sociaux et leur capacité à amplifier les messages augmentent l'ampleur des préjudices et les risques qu'ils représentent pour l'expression démocratique.

Il existe des recours juridiques pour certains de ces préjudices qui impliquent des violations de la vie privée et la possibilité de réclamations en responsabilité civile pour diffamation. D'autres préjudices enfreignent le Code criminel ou la législation sur les droits de la personne, qu'il s'agisse d'incitation à la violence, de menaces de mort ou d'agressions racistes visant les communautés minoritaires. Tous ces phénomènes sont devenus de plus en plus courants et fréquents ces dernières années.

Des poursuites judiciaires peuvent et doivent être engagées contre les contrevenants à la loi. Beaucoup peut et doit être fait avec les outils juridiques actuels. Cependant, de nombreux préjudices ne sont pas illicites, ce qui rend une réponse légale difficile, voire impossible. Par exemple, la radicalisation est une conséquence des atteintes à l'expression démocratique causées par le partage de théories du complot sur les médias sociaux qui amplifient le message et peuvent ainsi créer un faux sentiment de consensus qui attire une communauté de partisans et de soutiens. Une telle activité peut être « légale, mais abominable ». Elle mine l'expression démocratique et menace la démocratie des manières suivantes :

Préjudices	Exemples
Une plus grande toxicité en politique et une difficulté à convaincre les individus de se présenter aux charges publiques	Publications misogynes, calomnieuses et racistes qui menacent les politicien.ne.s, les journalistes, les fonctionnaires
Une montée des discours de haine, des menaces à la stabilité sociale et des attaques visant les communautés minoritaires	Des publications qui rendent les collectivités en quête d'équité responsables des crises de santé publique
Les pressions sur notre système démocratique et les tentatives de saper la légitimité des institutions	La remise en question des résultats des élections sans preuve
Publicité mensongère et trompeuse	Mensonges et déformations des politiques du gouvernement et des partis politiques et des déclarations des politicien.ne.s
Mésinformation et désinformation en matière d'élections	Tentatives de suppression du vote par la désinformation sur les lieux de vote, les heures, etc.

Désinformation et mésinformation en matière de santé	Faire circuler des mensonges sur les vaccins, les immunisations et d'autres mesures de santé tout en promouvant des « remèdes » pour des gains financiers
Tentatives de blocage de l'accès aux événements et institutions publics	Encourager les individus à bloquer les établissements de soins de santé ou à empêcher les événements politiques publics
Théories du complot	Allégations sur les sources de la maladie, les motivations derrière des politiques gouvernementales précises
Grossièreté croissante et manque de courtoisie dans le dialogue public	Partisanerie extrême et mise en cause des motivations des adversaires, ce qui empêche la discussion sur les politiques et la recherche d'un consensus

Réguler le rôle des plateformes de médias sociaux est sans aucun doute complexe étant donné l'ampleur et la nature des différents préjudices qu'elles causent à l'expression démocratique, aux droits de la personne et au bien public. Une grande partie du débat mondial sur les activités des plateformes de médias sociaux, les préjudices qu'elles peuvent causer et les appels à la régulation et à la surveillance s'est concentrée sur les résultats – ce que les utilisateurs.rices voient.

La Commission est convaincue que le moment est venu de se pencher sur les systèmes algorithmiques qui amplifient le contenu en plus de traiter les résultats.

Notre attention se porte sur les systèmes mis au point et déployés par les plateformes de médias sociaux et sur les incitations dans ces systèmes qui peuvent causer des préjudices et les amplifier. Ces « systèmes à boîte fermée » comprennent au mieux un monde très opaque pour les gouvernements, les organismes de réglementation, les utilisateurs.rices de médias sociaux et le public.

Ce système peut être conceptualisé comme suit : les entrées, la boîte fermée et les résultats.

- **Les entrées** – les données matérielles et personnelles que les utilisateurs.rices et les annonceurs publient et fournissent aux plateformes de médias sociaux, ainsi qu'un large éventail de données en ligne et hors ligne, ainsi que des variables déduites sur nos vies, nos croyances et nos préférences.

- **Les « systèmes à boîte fermée »** – les processus automatisés conçus et déployés par les entreprises de plateformes pour gérer, agréger et distribuer le contenu et les données collectées ; et

- **Les résultats** – le contenu que les utilisateurs voient – ou ne voient pas – affiché sur leurs pages et sites.

Au Canada, le gouvernement fédéral a déposé plusieurs projets de loi, dont aucun n'a été adopté avant la dissolution du Parlement en août 2021 en vue des élections de septembre. Ces propositions législatives ont largement porté sur la tentative de minimiser les préjudices qui découlent des « résultats ».

De même, le premier rapport de la Commission publié en 2021 traitait essentiellement de ceux-ci. Plus précisément, il a exposé un programme intégré en six étapes pratiques qui excluait une politique de démantèlement énergique du contenu préjudiciable en faveur d'une approche axée sur le/la citoyen.ne qui attribue la responsabilité du contenu haineux et préjudiciable aux utilisateurs.rices qui le publient et aux plateformes qui amplifient leurs messages.

Les entrées peuvent être limitées par les dispositions du Code criminel sur les discours haineux. (Il convient de noter que les politiques des plateformes grand public limitent ce que les individus peuvent publier sur les plateformes dans une mesure bien plus importante que celle autorisée par la loi, en raison des droits à la liberté d'expression). La publicité fausse et trompeuse peut être prise en charge par le Bureau de la concurrence. La législation fédérale et provinciale, si elle est appliquée, peut protéger le droit à la vie privée des citoyen.ne.s et restreindre ce que les utilisateurs.rices de médias sociaux peuvent faire et publier. À des degrés divers, ces restrictions existent également sur les « résultats ».

Les systèmes algorithmiques opaques sont ceux qui sont le moins soumis à la surveillance et aux contraintes externes. C'est pourquoi nous pensons qu'il serait judicieux pour les gouvernements de maintenant chercher à comprendre comment les plateformes de médias sociaux gèrent ces systèmes – et de s'assurer de l'aide des organismes de réglementation, des chercheurs.euses, des utilisateurs.rices, ainsi que des personnes concernées par le contenu que les plateformes distribuent. Il s'agit d'une condition préalable essentielle aux gouvernements et aux organismes de réglementation pour rendre les plateformes responsables de l'élimination des préjudices à l'expression démocratique et de l'instauration de mesures visant à empêcher ces préjudices de se produire.

Exiger la transparence sur la façon dont les plateformes programment et gèrent les rouages de leurs systèmes algorithmiques est le premier des trois principes que nous estimons primordiaux pour protéger contre les préjudices à l'expression démocratique.

Mais la transparence est un moyen d'atteindre une fin, pas la fin elle-même. Grâce à la transparence, les gouvernements, les organismes de réglementation, les chercheurs.euses, les utilisateurs.rices de médias sociaux et les personnes touchées par le contenu des plateformes de médias sociaux peuvent évaluer la responsabilité des plateformes dans la diffusion de matériel nuisible qui menace l'expression démocratique.

Pour réduire les préjudices et permettre à l'expression démocratique de s'épanouir, nous pensons que la transparence et la responsabilisation doivent s'accompagner d'un troisième principe : l'autonomisation. Le fait de savoir comment les utilisateurs.rices sont ciblés, comment leur expression est rendue visible,

amplifiée ou réduite au silence, et comment leurs renseignements personnels sont utilisés sans leur consentement éclairé ou à leur insu va à l'encontre de leurs droits fondamentaux et des principes fondamentaux de l'expression démocratique. Il en résulte un déséquilibre de pouvoir dans lequel les utilisateurs.rices et les personnes touchées par le contenu des plateformes ne disposent que de peu ou pas de recours ou de mécanismes permettant de tenir les entreprises responsables des préjudices potentiels. Au pire, les utilisateurs.rices faisant face à ce spectre accablant de collecte insidieuse n'exerceront tout simplement pas leur droit d'expression démocratique. L'autonomisation permet de transférer aux utilisateurs.rices et au public un pouvoir et un contrôle accrus sur leurs interactions en ligne et hors ligne.

Ce rapport et nos recommandations portent sur la manière dont l'action gouvernementale et réglementaire sur ces trois thèmes – transparence, responsabilisation et autonomisation – constitue la clé pour prévenir les préjudices à l'expression démocratique résultant des activités actuellement incontrôlées des plateformes de médias sociaux.

VALEURS ET PRINCIPES

Le premier rapport de la Commission en 2021, intitulé *Diminuer un tort*, a recensé un ensemble de principes qui ont guidé ses délibérations et ses recommandations, et ceux-ci sont mentionnés dans le résumé du présent rapport.

Nous restons attachés à ces principes et en avons ajouté d'autres. Les valeurs fondamentales de notre société sont au cœur de toutes les réponses visant à remédier aux atteintes à l'expression démocratique. Internet façonne maintenant presque tout dans la vie des Canadiens et Canadiennes – notre façon de travailler, de dépenser et d'épargner, de rencontrer des personnes, de nous divertir, d'utiliser notre temps libre, d'interagir avec les gouvernements et autres institutions et de communiquer.

Mais nous pensons que cela n'a pas changé et ne devrait pas changer les valeurs et principes sous-jacents de notre société – l'importance de la vie privée; le respect des autres et de leurs points de vue; la protection des personnes vulnérables et des jeunes; la reconnaissance que nous sommes une société diverse, multiculturelle et multiraciale dans laquelle tous possèdent les mêmes droits qui doivent être protégés; la garantie de la liberté d'expression dans les limites fixées par les lois et les décisions judiciaires du Canada; et la promotion d'une économie ouverte et compétitive qui profite à tous/toutes. Ces valeurs et principes constituent le fondement de la société canadienne et restent des pierres angulaires importantes de notre démocratie. Elles font partie intégrante de nos délibérations et de nos recommandations.

Il y a des mesures qui peuvent être mises en œuvre au Canada pour protéger le droit à la vie privée et les libertés tout en contrant les préjudices et les menaces à l'expression démocratique, en restant fidèle aux principes que la Commission a énoncés il y a un an et en respectant les recommandations de notre rapport original. Mais ce que nous proposons maintenant sera plus efficace si les actions du Canada sont coordonnées avec le consensus international croissant qui s'est formé sur les mesures que les démocraties respectueuses des droits peuvent prendre conjointement dans l'intérêt de l'expression démocratique.

Toutes nos nations font face à des menaces similaires au 21e siècle et le Canada devrait adopter des réponses communes de concert avec d'autres démocraties, en travaillant ensemble par le biais d'initiatives multilatérales et multipartites telles que la Freedom Online Coalition, à moins qu'il y ait une raison et une justification claires pour adopter une autre approche.

Notes sur la liberté d'expression dans le contexte canadien relativement à la régulation des plateformes de médias sociaux et d'Internet

La très honorable Beverley McLachlin, PC, CC

La constitution canadienne garantit la liberté d'expression. L'alinéa 2(b) de la Charte des droits et libertés prévoit :
2. Chacun a les libertés fondamentales suivantes :
b. liberté de pensée, de croyance, d'opinion et d'expression, y compris la liberté de la presse et des autres moyens de communication.

Objectif

La protection de la liberté d'expression repose sur des valeurs et des principes fondamentaux – la valeur de la recherche et de la quête de la vérité, la participation à la prise de décision sociale et politique et la possibilité pour l'individu de s'épanouir par l'expression : *Irwin Toy Ltd. c. Québec (Procureur général)*, [1989] 1 RCS 927 et 976.

Interprétation

Les tribunaux ont interprété l'alinéa 2(b) de manière large pour qu'il s'applique à tout ce dont le contenu expressif n'est pas supprimé par la méthode ou le lieu de l'expression – c'est-à-dire l'expression qui prend la forme de violence ou de menaces de violence : *Société Radio-Canada c. Canada (Procureur général),* 2011 CSC 2.

Il n'y a pas de protection contre la violence physique, ni contre les menaces de violence *: Irwin Toy, précité; Suresh c. Canada (Ministre de la Citoyenneté et de l'Immigration),* [2002] 1 RCS 3) 107-108. À d'autres égards, la forme ou le moyen utilisé pour transmettre un message est considéré comme faisant partie intégrante du message et protégé par l'alinéa 2(b) : *Weisfeld* (F.C.A.) Autrement, les discours nuisibles sont protégés – les discours haineux, la pornographie infantile et la désinformation bénéficient de la protection en vertu de l'alinéa 2(b).

La référence dans la garantie aux « autres moyens d'expression » indique clairement qu'elle s'applique à Internet. La garantie constitutionnelle de la liberté d'expression offre une protection présumée aux messages en ligne de tous types (à l'exception peut-être des menaces de violence). Le contenu de l'expression ne supprime pas la protection conférée par l'alinéa 2(b); il couvre même l'expression odieuse et haineuse.

Restrictions en vertu de l'article 1 de la Charte

La garantie de la liberté d'expression prévue par la Charte n'est pas absolue. L'État peut imposer des limites à la liberté d'expression en vertu de l'article 1 de la Charte, qui prévoit que les droits garantis ne « peuvent être restreints que par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique ». Dans une société démocratique, les droits – y compris la liberté d'expression – doivent parfois être restreints pour éviter de nuire à autrui. La plupart des garanties modernes des droits suivent ce modèle et reconnaissent expressément que la liberté d'expression peut être restreinte lorsque les valeurs et les préoccupations sont en conflit.

Les restrictions à l'expression peuvent être imposées par des lois ou découler de la définition de délits hérités de la common law, telle que la diffamation. Les restrictions à la liberté d'expression imposées par les gouvernements varient. Le Parlement a adopté des lois faisant de certains types de discours des délits – par exemple, des délits contre les discours de haine, la pornographie et la sédition. Le Parlement et les assemblées législatives peuvent autoriser des organismes établis par décret à prendre des mesures contre les discours nuisibles; les exemples incluent les lois fédérales et provinciales sur les droits de la personne et les contraintes imposées aux médias par le CRTC. Les règlements municipaux sur le bruit et les manifestations sont encore d'autres exemples de restrictions à l'expression imposées par la loi. Enfin, les individus peuvent engager des poursuites au civil pour limiter ou réparer des préjudices reconnus par la loi, tels que la diffamation ou la violation des règlements locaux en matière de bruit. Les individus peuvent obtenir des injonctions du tribunal pour interdire les discours illicites.

En fin de compte, ce sont des tribunaux indépendants – et non le gouvernement – qui décident des restrictions de la liberté d'expression. Si elles sont contestées, il faut prouver devant un tribunal que les lois restreignant l'expression adoptées par le Parlement, les assemblées législatives et les municipalités sont raisonnables et justifiées dans une société libre et démocratique. Les mesures prises et les règlements établis par les gouvernements et les organismes gouvernementaux sont soumis au même examen judiciaire. Au Canada, la censure d'un discours a généralement nécessité une ordonnance ou une injonction du tribunal. Ces protections garantissent que les restrictions à la liberté d'expression ne dépassent pas le cadre de ce qui est raisonnable et justifié dans une société libre et démocratique.

Nous pensons également que nous avons beaucoup à apprendre de la culture et des traditions des Autochtones du Canada. Willie Ermine, professeure adjointe à l'Université des Premières nations du Canada à Regina et originaire de la Première Nation de Sturgeon Lake située dans le centre-nord de la Saskatchewan, écrit sur la nécessité de créer des « espaces éthiques », qu'elle décrit comme un terrain neutre – où l'on peut sortir de ses propres règles et espaces – libéré de nos obligations et de nos cages mentales, c'est un espace éthique où le contact entre humains peut se produire[7].

Il s'agit d'insuffler à nos communications des valeurs humaines, des enjeux de cœur et d'âme, des valeurs démocratiques et supérieures aux commentaires extrêmes que l'on déverse trop souvent sur les médias sociaux. Dès lors, l'engagement de tous les acteurs de ce processus de communication agissant dans un esprit commun et insufflant des espaces éthiques et de l'humanité à la technologie, est nécessaire – qu'il s'agisse des utilisateurs.rices ou des développeurs.euses de logiciels et des programmeurs.euses qui conçoivent les algorithmes pour générer des réponses précises et les plateformes qui les utilisent.

Les membres de l'Assemblée citoyenne sur l'expression démocratique sont parvenus à une conclusion similaire, soulignant que « la pratique éthique vise à ne pas causer de dommages aux individus ou au public. Les dommages peuvent être physiques, émotionnels, mentaux, politiques ou financiers. La pratique éthique est à la base de valeurs telles que la responsabilisation et la transparence et comprend le devoir d'agir de manière responsable dans tous les environnements en ligne[8]. »

Cela commence, comme la Commission l'a noté dans son premier rapport, par un code de conduite des plateformes qui traite équitablement tous les utilisateurs.rices dans leurs interactions avec les plateformes. Cela comprend l'incidence sur les utilisateurs.rices de ce qu'ils/elles voient et font et la façon dont les plateformes façonnent et affectent les relations que les utilisateurs.rices entretiennent entre eux/elles, avec d'autres communautés et avec la société canadienne dans son ensemble.

LE DÉSÉQUILIBRE DE POUVOIR

Comment les individus, les communautés et les gouvernements peuvent-ils délimiter et faire respecter cette responsabilité face à un tel déséquilibre de pouvoir?

À ce sujet, le rapport de l'Assemblée citoyenne souligne : « Jusqu'à présent, les plateformes de médias sociaux ont été laissées sans surveillance. La profitabilité a pris le dessus sur le respect de la vie privée et la propriété des données. La protection inadéquate des données et le manque de reconnaissance de nos droits à la vie privée nous ont déresponsabilisés. Il est grand temps d'opter pour une approche proactive pour le bien du public[9]. »

Cela nous amène au cœur de notre mandat – les systèmes opaques et de plus en plus automatisés par lesquels les fournisseurs de plateformes façonnent le discours public sans recours pour les préjudices potentiels ou sans les protections adéquates pour atténuer les risques potentiels.

Comme nous l'ont noté les expert.e.s, cette réalité fait écho aux déséquilibres de pouvoir « incroyables » entre les plateformes numériques, d'une part, et les utilisateurs.rices et les chercheurs.euses et journalistes indépendants orientés vers l'intérêt public, d'autre part.

Les plateformes sont responsables de l'établissement de politiques relatives à ce qu'elles autorisent sur leurs sites. Ces normes sont ensuite appliquées par le truchement de la programmation pour repérer la haine, la désinformation, les théories de complot et autres communications et images écrites et vidéo préjudiciables qui peuvent faire l'objet d'un retrait et de sanctions à l'encontre des auteur.e.s.

Bon nombre des contrôles exercés par les plateformes sur les utilisateurs.rices, les contenus et les annonceurs résident dans des systèmes actuellement opaques, y compris des algorithmes constamment ajustés et utilisés pour catégoriser les utilisateurs.rices et faire correspondre les contenus et les publicités aux préférences perçues des utilisateurs.rices. Comme les expert.e.s l'ont fait savoir à maintes reprises à la Commission, les utilisateurs.rices n'ont aucune idée de ce que les plateformes savent d'eux/elles et de la façon dont elles déterminent ces préférences. Ils/elles disposent de peu de moyens de façonner ou de modifier ces renseignements et leurs recours pour faire retirer un contenu haineux ou offensant sont limités.

Des expert.e.s nous ont également confié que les utilisateurs.rices et les chercheurs.euses ne savent pas quels préjugés sociétaux ou culturels sont inhérents aux algorithmes, ni comment ou si les plateformes compensent cela. Ils/elles ne savent pas non plus si les plateformes ont conscience de leurs propres préjugés algorithmiques qui peuvent fausser les résultats fournis à des groupes précis de la société, sur la

base de critères démographiques tels que la religion, le revenu, l'origine raciale ou ethnique, le sexe, l'éducation ou le statut de minorité dans un milieu majoritaire. Ils/elles ont témoigné que les systèmes automatisés conçus pour protéger les groupes marginalisés n'y parviennent pas et censurent davantage leurs tentatives de lutter contre la discrimination en ligne.

Sur la base de ces témoignages, nous proposons trois moyens d'établir une répartition plus équilibrée du pouvoir entre les utilisateurs.rices, les personnes touchées par un système algorithmique et les plateformes.

Premièrement, exiger une plus grande transparence concernant les systèmes automatisés autrement fermés afin que les utilisateurs.rices, les personnes touchées par un système algorithmique, les chercheurs.euses, les organismes de réglementation et les gouvernements aient une plus grande capacité à évaluer et à vérifier la façon dont les algorithmes sont utilisés. Cela pourrait se faire sous plusieurs formes éprouvées au niveau international, telles que des registres de transparence, l'audibilité des plateformes et des systèmes algorithmiques, et un accès protégé aux publics, aux groupes de la société civile et aux parties indépendantes qui évaluent ces systèmes.

Deuxièmement, mettre à profit cette transparence accrue créée par l'ouverture des systèmes pour déterminer et évaluer si le contenu promu par les plateformes contribue à nuire à l'expression démocratique et si et comment les plateformes doivent être tenues responsables. Poser des questions, juger et appliquer des sanctions à l'encontre des plateformes qui hébergent et amplifient des contenus contribuant à nuire à l'expression démocratique.

Troisièmement et plus important encore, donner aux utilisateurs.rices plus de pouvoir pour déterminer, gérer et contrôler les renseignements les concernant qui sont recueillis et utilisés par les plateformes.

Les recommandations de notre rapport sont axées sur la manière de concrétiser ces trois objectifs.

DÉVELOPPEMENTS RÉCENTS

Tout au long de l'année qui s'est écoulée depuis le premier rapport de la Commission, l'ampleur de l'examen international et des propositions de solutions législatives pour lutter contre les préjudices en ligne et les menaces à l'expression démocratique a connu une croissance considérable, ainsi que la vaste couverture médiatique qui s'y rapporte. Ce débat de société et de politique publique évolue rapidement.

Comme l'a souligné l'Aspen Institute aux États-Unis dans le rapport final de novembre 2021 de sa Commission sur le désordre de l'information[10], en décrivant la situation aux États-Unis : « La dernière décennie a été marquée par un énorme changement dans le tissu de la vie sociale, culturelle et politique des États-Unis. Alors que nous approchons de la fin de la deuxième année de la pandémie de COVID-19, les coutures se déchirent et les menaces qui pèsent sur les collectivités et les moyens de subsistance sont passées des salons de discussion sur Internet aux unités de soins intensifs. Nous voyons comment notre écosystème de l'information laisse tomber le public, et comment l'absence ou la perte de confiance dans les entités gouvernementales, les institutions communautaires et le journalisme, combinée à un nombre croissant de mauvais acteurs.ices et d'entrepreneur.e.s de conflits qui exploitent ces faiblesses, a conduit à des préjudices réels, parfois avec des conséquences fatales. Le discours public est profondément polarisé et acrimonieux; nous nous méfions les uns des autres et des institutions puissantes (parfois à juste titre). Beaucoup sont devenus inutilement sceptiques à l'égard de la recherche scientifique et rejettent les faits étayés. De plus, parmi les confinements obligatoires et les changements abrupts vers le tout en ligne, l'année dernière a montré à quel point il est essentiel pour nous de nous connecter les uns aux autres dans un véritable dialogue et un discours significatif. Notre incapacité croissante à combler ces écarts et à établir des liens vitaux dans nos vies a un effet corrosif[11]. »

Le Canada n'est pas les États-Unis, mais les deux pays présentent des similitudes.

Notre culture et nos institutions politiques, notre héritage linguistique, nos modèles d'immigration, notre diversité multiculturelle, notre structure sociale et juridique et nos environnements médiatiques sont différents de ceux des États-Unis. À bien des égards, ils sont très différents.

Nous pensons que le Canada commettrait une erreur en adoptant simplement l'analyse sociétale ou les solutions proposées et débattues aux États-Unis.

Les plateformes de médias sociaux n'étaient pas seulement essentielles pour les politicien.ne.s qui tentaient de toucher les électeurs.rices. De nombreux Canadiens et Canadiennes ont utilisé positivement les médias sociaux pendant l'élection pour discuter et débattre des politiques des partis et des candidat.e.s qu'ils/elles devraient soutenir, pour partager des vidéos et des blagues et pour commenter en continu pendant les débats télévisés.

Mais pour certains, les plateformes de médias sociaux sont aussi devenues le canal de diffusion de la désinformation et des théories du complot, comme celles qui prétendent que la COVID-19 n'existe pas et qui mentent sur les risques et les effets secondaires des vaccins. Le partage de ces informations sur les plateformes de médias sociaux pendant la pandémie de COVID-19 a alimenté la formation de groupes anti-vaccination, dont certains ont harcelé et menacé des travailleurs.euses de la santé et tenté de bloquer l'accès du public, des employé.e.s et des patient.e.s aux établissements de soins de santé et aux hôpitaux.

Et comme l'année dernière au Canada l'a démontré, même si elles ne sont pas aussi répandues, bon nombre de ces pressions sous-jacentes sur la société, le discours civilisé et le désaccord recensés par l'Aspen Institute se retrouvent ici aussi.

Les réactions sont également similaires, comme l'occupation extrêmement bien organisée et financée du centre-ville d'Ottawa pendant plus de trois semaines en février 2022, par un mélange de suprémacistes blancs, de théoriciens du complot anti-vaccination, de personnes s'opposant à toutes les mesures de lutte contre les pandémies et d'extrémistes prônant le renversement du gouvernement fédéral, en utilisant des camions comme armes. Un exemple similaire a été la série de blocages à l'aide de camions à la frontière entre le Canada et les États-Unis au cours du même mois en Ontario, au Manitoba, en Alberta et en Colombie-Britannique.

Lors de tous ces événements, comme lors de la campagne électorale fédérale de 2021, de nombreux slogans, images et chants importants des manifestant.e.s ont imité ceux de groupes similaires aux États-Unis impliqués dans la prise d'assaut du Capitole le 6 janvier 2021. Une part importante du financement des manifestations provenait également des États-Unis, mais les manifestations étaient dirigées par des Canadiens et Canadiennes, et soutenues par des millions de dollars de financement canadien, dont une grande partie en petits montants provenant de donateurs.rices individuels.

Les Canadiens et Canadiennes ne doivent pas minimiser l'importance de ces confrontations qui, à ce jour, sortent de l'ordinaire. Notre analyse et nos recommandations sont ancrées dans nos normes et notre histoire juridiques, culturelles et sociales, ainsi que dans les valeurs et les principes de nos citoyen.ne.s.

Sur le front de la politique publique, l'année dernière a également vu un nombre croissant de propositions législatives et réglementaires qui, comme ce rapport, se concentrent sur la transparence, la responsabilisation et l'autonomisation des utilisateurs.rices.

Dans l'Union européenne, la loi sur les services numériques (DSA) est sur le point d'être adoptée et la loi sur les marchés numériques (DMA) pourrait l'être au printemps 2022. Ensemble, ces deux textes visent à « créer un espace numérique plus sûr dans lequel les droits fondamentaux de tous les utilisateurs de services numériques sont protégés; et à établir des conditions de concurrence équitables pour favoriser l'innovation, la croissance et la compétitivité, tant au sein du marché unique européen qu'à l'échelle mondiale[12]. »

Par exemple, la DSA prévoit l'obligation pour les plateformes de rendre leurs données accessibles aux chercheurs.euses et de divulguer tous les paramètres de publicité et de ciblage en ligne.

La législation proposée aux États-Unis met l'accent sur la responsabilité algorithmique, y compris des régulations qui exigeraient de certaines entités utilisant des renseignements personnels qu'elles procèdent à des évaluations d'incidence et qu'elles « traitent raisonnablement et en temps opportun » tout préjugé ou enjeu de sécurité décelé.

Promouvant l'autonomisation des utilisateurs.rices, le Règlement général sur la protection des données (RGPD) de l'UE donne aux Européen.ne.s huit droits d'utilisateur : le droit à l'information, le droit d'accès, le droit de rectification, le droit à l'effacement, le droit à la restriction du traitement, le droit à la portabilité des données, le droit d'opposition et le droit d'éviter la prise de décision automatisée. Les autorités nationales chargées de la protection des données dans les 27 États membres de l'UE font respecter ces droits à la protection des données pour protéger à la fois les intérêts individuels et l'intérêt public en veillant au respect des lois sur la protection de la vie privée.

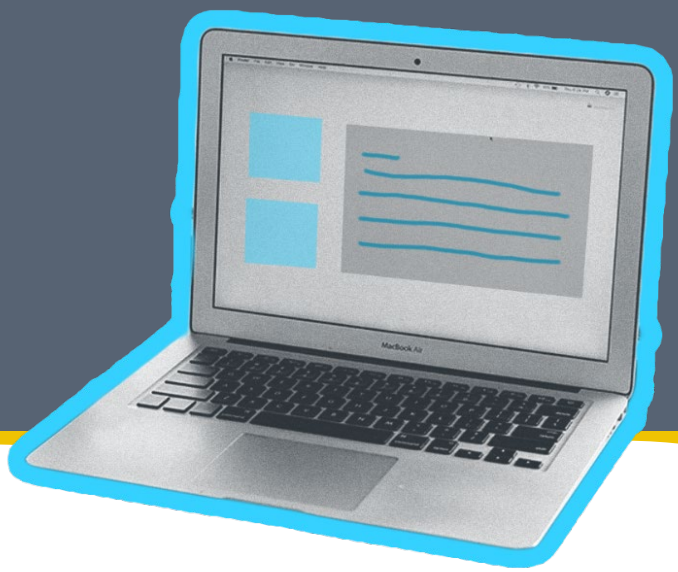
Au Canada, le gouvernement fédéral a répondu par plusieurs projets de loi, dont aucun n'a été adopté avant la dissolution du Parlement en août 2021 en vue des élections de septembre.

En novembre 2020, le gouvernement fédéral a introduit deux projets de loi traitant de certains aspects des activités des plateformes et de leur incidence sur l'expression démocratique : le projet de loi C-10 – Loi modifiant la Loi sur la radiodiffusion et apportant des modifications connexes et corrélatives à d'autres lois, et le projet de loi C-11 – Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois. Un troisième projet de loi a suivi en juin 2021 : C-36 - Loi modifiant le

Code criminel et la Loi canadienne sur les droits de la personne et apportant des modifications connexes à une autre loi (propagande haineuse, crimes haineux et discours haineux). De plus, le gouvernement fédéral a publié en juillet 2021 un document technique soulignant une approche pour lutter contre le contenu préjudiciable en ligne et a sollicité la rétroaction du public sur les propositions par le truchement d'un processus de consultation[13].

Seul le projet de loi C-10 a fait l'objet d'un examen parlementaire approfondi, mais cela n'a pas empêché une réaction largement négative à l'ensemble des propositions du gouvernement, même si la pandémie de COVID-19 et une campagne nationale de vaccination de masse ont fait les gros titres à la fin du printemps et pendant l'été. Une grande partie de la critique a porté sur les menaces perçues que la législation fait peser sur la liberté de parole et d'expression ainsi que sur la vie privée des individus.

En février 2022, le gouvernement fédéral a répondu à sa consultation sur les préjudices en ligne en publiant un rapport intitulé « Ce que nous avons entendu », qui souligne la rétroaction au processus de consultation et annonce la création d'un groupe d'expert.e.s chargé de donner des avis sur la manière d'ajuster les propositions pour répondre aux préoccupations.



CHAPITRE DEUX : CONTRER LES MENACES CONTRE L'EXPRESSION DÉMOCRATIQUE

RECOMMANDATIONS

Nous avons regroupé nos recommandations sous trois thèmes interdépendants : la transparence, la responsabilisation et l'autonomisation. Les trois œuvrent ensemble pour fournir aux utilisateurs.rices, aux annonceurs, aux gouvernements, aux organismes de réglementaion et au public le matériel nécessaire pour comprendre et contrer la façon dont les médias sociaux sont utilisés, et pour aider à déterminer comment les plateformes façonnent les contours de l'expression démocratique qui peut finir par entraîner des préjudices en ligne.

Chaque thème commence par sa définition et par quelques renseignements généraux supplémentaires, suivis de recommandations individuelles liées à ce thème. Chaque recommandation est accompagnée d'une brève explication de sa raison d'être et de détails sur les cas où des recommandations similaires sont proposées ou mises en œuvre par les gouvernements et leurs organismes de réglementation dans d'autres pays.

THÈME 1 : LA TRANSPARENCE

Définition

La transparence désigne un éventail de mécanismes de divulgation par lesquels les plateformes fournissent de l'information sur leurs opérations, y compris les systèmes de prise de décision automatisés. En général, cette information n'est pas publique, ce qui ne facilite pas l'identification et l'atténuation des incidences

discriminatoires pour les personnes extérieures aux plateformes. L'objectif d'une véritable transparence – une transparence qui sert ceux/celles qui sont le plus touchés par l'opacité des plateformes – est de démontrer la conformité avec les exigences légales et/ou réglementaires et de renforcer les mécanismes de responsabilisation, y compris la capacité des individus et des organismes de réglementation à contester les décisions cachées ou automatisées. En ce sens, une véritable transparence peut partiellement servir les efforts visant à identifier les résultats et les préjudices injustes, à tenir les acteurs puissants publiquement responsables et à améliorer la gouvernance globale. La transparence peut également fournir aux utilisateurs.rices les outils nécessaires pour prendre des décisions éclairées sur leur comportement, tant en ligne que hors ligne.

Contexte

Les plateformes numériques utilisent des données personnelles et des outils et algorithmes automatisés qui ont une incidence sur la sphère publique. Nous avons entendu des expert.e.s témoigner que les données personnelles des utilisateurs.rices collectées par les plateformes peuvent être utilisées pour cibler d'autres utilisateurs.rices et pour permettre et amplifier des contenus clivants et nuisibles, ce qui cause des préjudices dans le monde réel. Pourtant, ces processus de plateforme restent cachés au public et aux acteurs indépendants qui s'efforcent de réduire les schémas discriminatoires. La prise de décision opaque concernant le public entrave directement les valeurs démocratiques et les droits, notamment ceux à la vie privée, à l'équité et à l'application régulière de la loi. Bien que de nombreuses plateformes rendent compte de leurs activités concernant des contenus précis, ces rapports sont entièrement autorégulés, souvent incomplets et ne peuvent être vérifiés de manière indépendante. Les plateformes manifestent également une grande réticence à publier des informations sur le type de données qu'elles collectent ou à autoriser des experts indépendants à évaluer le rendement de leurs algorithmes. En partie en invoquant légitimement des préoccupations concernant la vie privée, la propriété intellectuelle, les secrets commerciaux et la possibilité d'une utilisation malveillante de tout ce qu'elles rendent public. Les chercheurs.euses et les journalistes travaillant dans l'intérêt du public se voient régulièrement refuser l'accès aux contenus publics sur les plateformes. Le manque de transparence fait en sorte qu'il est presque impossible pour les gouvernements et les organismes de réglementation de vérifier si les entreprises respectent la loi.

Des propositions législatives émanant d'Europe, des États-Unis et d'ailleurs ont tenté de renforcer ou d'imposer la transparence par le biais de rapports réguliers, de notifications aux utilisateurs.rices, d'accès aux données pour l'intérêt public et d'audits des pratiques des plateformes destinés au public[14]. Mais les mesures de transparence doivent également garantir la protection de la vie privée des individus. Cela inclut la confidentialité de ceux/celles dont les données sont collectées et partagées avec des tiers. Cette confidentialité est essentielle car ces données doivent être suffisamment contextuelles et granulaires pour permettre d'identifier des tendances plus larges et des schémas de discrimination[15], tout en protégeant la vie privée des utilisateurs et en empêchant les gouvernements, les entreprises et les chercheurs.euses d'aller

trop loin. De nombreux expert.e.s et praticien.ne.s reconnaissent qu'une plus grande transparence, en soi, est un mécanisme de responsabilisation insuffisant étant donné que les données globales autodéclarées offrent rarement un véritable aperçu des pratiques en matière de contenu. Ce n'est pas parce que les données sont rendues transparentes que leur collecte ne peut pas causer de tort. C'est pourquoi nous soutenons également les efforts du gouvernement pour moderniser notre régime de protection des données afin de garantir une bien meilleure protection des données des utilisateurs.rices au Canada.

Bien que la transparence ne soit qu'une solution partielle, elle reste un mécanisme clé pour améliorer la compréhension du public sur les processus de conception ainsi que les processus techniques et financiers qui régissent les plateformes de médias sociaux d'aujourd'hui.[16] Nos recommandations dans ce domaine sont destinées à renforcer les efforts visant à obliger les entreprises à rendre des comptes pour les dommages causés à la société et à doter le public, les chercheurs.euses, les journalistes et les décideurs.euses politiques d'outils permettant de mettre en évidence puis de traiter les inégalités structurelles et leur amplification en ligne.

Recommandations

1.1. Mandat et pouvoir de contrainte : Mettre sur pied et habiliter un organisme de réglementation pour imposer et permettre l'accès, à des fins de recherche et de surveillance, aux données contenues dans les plateformes de médias sociaux.

L'organisme de réglementation veillera à l'application des exigences obligatoires en matière d'accès et de partage des données de la plateforme définies dans la législation pour chacun des trois niveaux suivants : le grand public, les chercheurs.euses et journalistes accrédités, et les recherches plus spécialisées et détaillées dans l'intérêt public qui, sans garanties supplémentaires importantes, pourraient avoir des répercussions sur la vie privée.

Confier à une entité de régulation la tâche d'administrer la diffusion des données de la plateforme permettrait de garantir une voie d'accès aux données protégée par la confidentialité et sécurisée. L'entité, qui fonctionnerait peut-être sous les auspices du Tri-Conseil[17], garantirait que seuls les chercheurs.euses et les journalistes qualifiés ayant un intérêt public aient accès à des niveaux de données plus élevés, préservant ainsi la vie privée et la sécurité des individus. L'entité devra tenir compte de la vie privée des utilisateurs.rices dans toutes les décisions d'octroi d'accès et prendre les mesures appropriées pour empêcher la divulgation de données sensibles. Ses tâches consisteraient à administrer les données aux chercheurs.euses, à approuver les demandes et à créer un conseil consultatif (composé de représentant.e.s de l'industrie et du milieu universitaire). L'entité disposerait également de pouvoirs de police pour garantir la coopération des plateformes et des chercheurs.euses. Le fait de n'autoriser qu'un accès moyen à élevé à des

chercheurs.euses, journalistes et universitaires approuvés permet de préserver la sécurité et la confidentialité des données.

Précédents

Avec la proposition de loi sur les services numériques de l'Union européenne, les autorités nationales (« coordonnateurs de services numériques ») seraient en mesure d'ordonner aux plateformes de fournir un accès aux données à des chercheurs agréés (article 31). Aux États-Unis, la proposition de loi sur la transparence et la responsabilisation des plateformes[18], laisse entrevoir la création d'une « Division de la transparence et de la responsabilisation des plateformes » au sein de la Commission fédérale du commerce. La principale attribution de la division serait de développer et d'établir des normes, des critères et un processus d'approbation recommandés pour les chercheurs.euses, les projets de recherche et les plateformes.

1.2. Mettre en œuvre un accès hiérarchisé aux données : imposer des niveaux distincts d'accès aux données avec des garanties pour le public, les chercheurs.euses, les journalistes et les groupes de la société civile.[19]

Instaurer des niveaux hiérarchisés de droits d'accès aux données pour les plateformes afin d'accorder au public un accès de niveau inférieur (niveau 1); d'accorder aux chercheurs.euses, aux acteurs.rices de la société civile et aux journalistes un accès de niveau intermédiaire (niveau 2); et d'accorder à un nombre restreint de candidat.e.s spécialisés menant des recherches spécialisées d'intérêt public un accès nécessitant des garanties détaillées plus importantes afin d'équilibrer la protection de la vie privée avec la nécessité d'une plus grande transparence et responsabilisation des plateformes (niveau 3).

En obligeant les plateformes numériques à mieux informer les utilisateurs.rices sur leur mode de fonctionnement, les individus pourront faire des choix plus éclairés sur la façon dont ils utilisent les médias sociaux.

Le niveau 1 prévoit que l'utilisateur.rice individuel du grand public puisse obtenir les données démographiques de base et les données connexes le/la concernant que les plateformes utilisent pour déterminer le contenu partagé et la publicité qui sont promus par la plateforme auprès de cet/cette utilisateur.rice. Ces données doivent lui être fournies par la plateforme sur la base d'une demande de cet/cette utilisateur.rice à une plateforme précise. De plus, le niveau 1 doit assurer la transparence publique du contenu public à forte visibilité et/ou à fort engagement – c'est-à-dire les publications publiques des comptes ayant un nombre très élevé d'abonné.e.s et les publications publiques qui reçoivent des niveaux élevés de vues (impressions) et/ou d'engagement.

Le niveau 2 d'accès aux données doit être lié à des objectifs précis de recherche et de journalisme (p. ex. la réalisation d'évaluations indépendantes des risques, l'évaluation de l'incidence des plateformes dans des domaines d'action particuliers, la façon dont les préjudices en ligne sont propagés, etc.) L'accent devra être mis sur l'obligation de fournir des données qui éclairent et favorisent la prévention des préjudices à long terme et sur la fourniture de données permettant de cerner les structures et les schémas plus larges des préjudices, notamment la discrimination et l'inégalité. Les détenteurs.rices du niveau 2 devront se conformer à des exigences précises et détaillées en matière d'éthique, de sécurité et de confidentialité. Le niveau d'accès 2 devra être contrôlé par un organisme, peut-être sous les auspices des trois Conseils.

Les demandeurs.euses de niveau 3 doivent satisfaire à des exigences plus strictes en matière d'accès aux données et à des dispositions plus détaillées en matière d'utilisation éthique et de respect de la vie privée, en fonction de la nature des données utilisées et du but dans lequel elles sont obtenues.

Cette recommandation permet aux chercheurs.euses, journalistes et acteurs de la société civile travaillant dans l'intérêt public de déceler les préjudices potentiels avant qu'ils ne se produisent et de tenir les plateformes responsables des préjudices sociétaux. Il est nécessaire de s'assurer que des chercheur.euse.s indépendants ont accès aux données des plateformes afin d'examiner comment les préjudices sont amplifiés par la publication croisée du même contenu sur différentes plateformes et d'établir un système de réponse aux risques en ligne.

En fournissant différents niveaux d'accès aux données, on s'assure que les destinataires disposent des outils et des compétences nécessaires pour comprendre les données fournies. Les données sur les tendances problématiques en ligne permettraient de remédier en partie aux difficultés rencontrées par les parties intéressées pour comprendre réellement comment différents groupes sont lésés de manière disproportionnée en ligne.

Précédents

L'Union européenne a annoncé une version révisée du « Code de bonnes pratiques contre la désinformation » comprenant un « cadre solide pour l'accès aux données par les chercheurs[20]». L'article 31 de la proposition de loi sur les services numériques (DSA) exige que les très grandes plateformes (dont la base d'utilisateurs.rices actifs représente plus de 10 % de la population européenne) fournissent un accès aux données à un.e coordonnateur.rice de services numériques. Ce/cette dernier.ière peut également demander à la plateforme de donner accès à des chercheurs agréés à des fins précises . En vertu de la DSA, les chercheurs.euses ne seront pas autorisés à utiliser les données consultées dans un but lucratif ou pour alimenter des campagnes politiques[22].

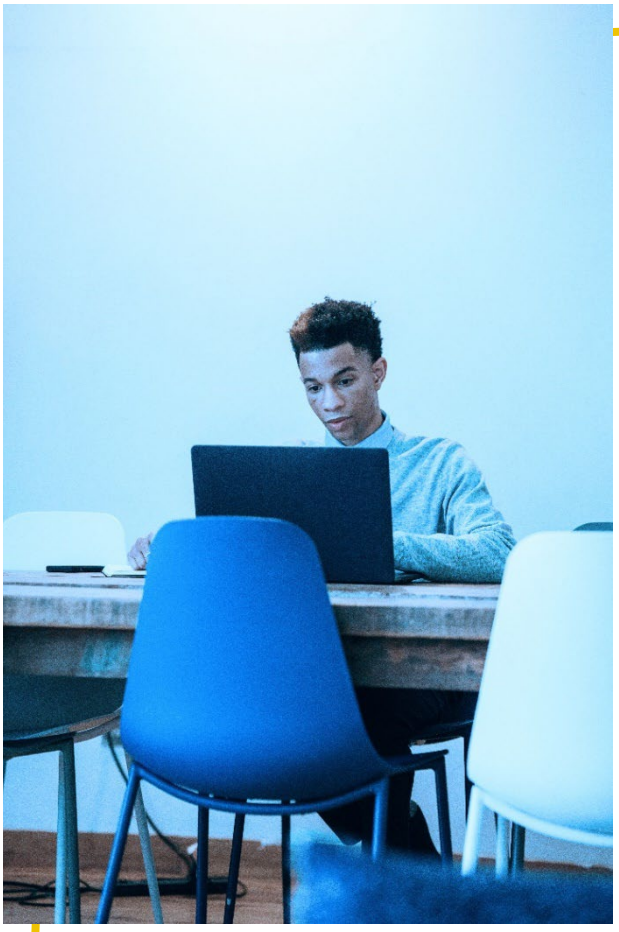
Aux États-Unis, la proposition de loi sur la responsabilité et la transparence des plateformes (Platform Accountability and Transparency Act, PATA), prévoit d'obliger les plateformes à partager des données avec

des « chercheurs.euses qualifiés », définis comme des chercheurs.euses affiliés à une université et probablement élargis pour inclure des acteurs de la société civile qui mènent des projets approuvés par la National Science Foundation (NSF). Le refus de fournir des données à un projet répondant aux conditions requises ferait perdre à la plateforme les immunités prévues par l'article 230 de la Communications Decency Act[23].

Parallèlement aux initiatives législatives visant particulièrement le secteur technologique, des obligations hiérarchisées ont également été instaurées dans d'autres domaines. Par exemple, dans la proposition de directive européenne sur la publication d'informations en matière de durabilité par les entreprises, la Commission européenne doit établir des normes de publication d'informations en matière de durabilité « proportionnées aux capacités et aux ressources d'une PME[24]», par opposition à celles qui s'appliquent aux grandes entreprises. De même, aux États-Unis, la Securities and Exchange Commission a imposé des exigences de divulgation différentes pour les petites sociétés déclarantes, en autorisant par exemple des rapports succincts[25].

1.3. Imposer une transparence universelle sur la publicité numérique.

Instaurer une obligation juridique pour les plateformes de médias sociaux de divulguer régulièrement et d'archiver, sous un format normalisé, des renseignements précis sur chaque publicité numérique et contenu payant publié sur leurs plateformes. De plus, exiger que les paramètres et les catégories utilisés pour cibler les utilisateurs soient divulgués, y compris : l'entité qui a payé pour la publicité; le budget publicitaire et le montant global dépensé; la portée prévue et réelle de la publicité; des informations sur la personnalisation/microciblage et quels codes de conduite volontaires l'annonceur approuve et suit. La divulgation et l'archivage doivent être universels, ce qui signifie que les plateformes doivent présenter les données sous un format normalisé lisible par machine, avec des normes minimales communes de divulgation. Toutes ces données seront conservées dans une archive unique et centrale dont le contenu sera accessible aux trois niveaux d'utilisateurs énumérés dans les recommandations précédentes. Les législateurs doivent également examiner si ces dispositions doivent être appliquées plus largement à d'autres sites en ligne que les plateformes de médias sociaux, étant donné l'omniprésence de la publicité ciblée en ligne.



Après avoir examiné la question de l'interdiction du microciblage publicitaire, la Commission a conclu que le Canada tirerait parti d'une approche plus nuancée de la question et propose que le Commissariat à la protection de la vie privée soit doté de plus de pouvoirs pour examiner la question du microciblage.

La Loi sur la modernisation des élections[26] de 2018 exigeait des plateformes de médias sociaux qu'elles établissent une archive de toutes les publicités politiques diffusées sur leur site pendant une campagne électorale fédérale. Il est maintenant temps de s'appuyer sur cette base en étendant et en élargissant cette exigence à toutes les publicités, en tout temps, qui apparaissent sur les plateformes de médias sociaux. Toutes les publicités doivent être conservées sous un format normalisé dans une base de données unique et centrale accessible au public.

La transparence sur la publicité et les données publicitaires est essentielle aux utilisateurs.rices, aux chercheurs.euses/journalistes et aux organismes de réglementation pour comprendre pourquoi et comment les plateformes ciblent les individus et les groupes avec des publicités précises et comment elles dressent le profil des utilisateurs.rices et des groupes. Cette compréhension permettra aux utilisateurs.rices d'adapter leur comportement en ligne afin de mieux comprendre pourquoi un contenu précis leur est proposé. L'augmentation de la transparence des publicités aidera également les annonceurs. Nous avons entendu des témoignages d'expert.e.s selon lesquels les annonceurs sont de plus en plus frustrés par les renseignements limités qu'ils reçoivent des plateformes où leurs publicités apparaissent. Par exemple, ils aimeraient obtenir plus de détails des plateformes sur le nombre de vues de leurs publicités, sur la façon dont les robots falsifient les chiffres d'audience et sur l'assurance que leurs publicités n'apparaissent pas sur des pages au contenu qui leur semble répréhensible. Une plus grande transparence permettra également de tenir les annonceurs pour responsables lorsque des publicités ciblées trompent ou manipulent les utilisateurs.rices. La transparence des publicités aidera à déceler les pratiques publicitaires discriminatoires et partiales. En ce qui concerne les publicités politiques, le microciblage peut permettre à la désinformation politique de se répandre rapidement et avoir une incidence grave sur le débat public et les résultats électoraux.

Plusieurs plateformes, dont Twitter et Facebook, ont déjà mis en place des outils permettant aux entreprises et aux annonceurs d'accéder à certaines données, mais ces outils ne sont pas partagés avec les chercheurs.euses pour lesquels le coût d'utilisation est souvent prohibitif. Même les annonceurs bénéficieraient d'une transparence qui leur fournirait plus de données sur la façon dont les plateformes gèrent leurs publicités, des détails sur les vues et les clics sur la publicité et l'influence des robots de recherche plutôt que des humains, que ce qui est actuellement mis à leur disposition.

De plus, Facebook a mis à la disposition des utilisateur.rice.s un lien « Pourquoi est-ce que je vois cette publicité? » dans le coin supérieur droit de toutes les publicités de son fil d'actualité. En cliquant sur ce lien, on découvre les données démographiques de base que Facebook conserve sur chaque individu et sur lesquelles repose la décision automatisée d'afficher cette publicité à son attention. C'est un bon début de transparence et cela vaut la peine d'envisager de l'imposer à d'autres plateformes, mais des données plus précises sont nécessaires pour évaluer la responsabilité de ces systèmes dans la promotion des préjudices en ligne.

Précédents

La proposition de loi sur le service numérique de l'Union européenne (Considérations n°52, 63, 66 (interopérabilité des référentiels publicitaires); article 24; l'article 30 exige que les très grandes plateformes en ligne mettent à disposition un référentiel publicitaire par le biais d'une interface de programmation d'applications (API). L'article 34(1)(e) impose à la Commission l'obligation de mettre au point un format de divulgation normalisé pour assurer l'interopérabilité); Code de bonnes pratiques contre la désinformation II.D (« Les signataires du présent code reconnaissent qu'il convient de garantir la transparence pour permettre aux utilisateurs.rices de comprendre pourquoi ils/elles ont été ciblés par une publicité à caractère politique ou publicité engagée donnée »). Des membres du Parlement européen ont également demandé l'interdiction du ciblage publicitaire basé sur des données sensibles (croyances religieuses, orientation sexuelle et origine raciale ou ethnique).

1.4. Instaurer une protection renforcée pour les dénonciateurs.rices.

Le Canada a besoin de mesures de protection plus fortes pour les dénonciateurs.rices – les employé.e.s actuels ou anciens qui dénoncent les pratiques frauduleuses des entreprises, notamment les violations de la loi, la mauvaise gestion, le gaspillage de fonds, les abus de pouvoir et les dangers pour la santé et la sécurité. Au regard des risques économiques, professionnels ou personnels auxquels les dénonciateurs.rices peuvent être exposés, toute recommandation visant à protéger les personnes qui signalent et exposent les pratiques frauduleuses internes des entreprises doit leur garantir une protection contre les représailles juridiques, économiques et l'atteinte à la réputation exercées par leur employeur. Le gouvernement fédéral pourrait s'inspirer d'autres secteurs pour renforcer la protection des dénonciateurs.rices privés.

La protection des dénonciateurs.rices est essentielle pour encourager la divulgation publique des décisions et pratiques préjudiciables des entreprises (plutôt que des données exclusivement techniques) car elle accroît la sécurité juridique des dénonciateurs.rices potentiels. Les dénonciateurs.rices attirent l'attention du public sur un enjeu autrement opaque, ce qui peut inciter les pouvoirs publics à agir. Dans le domaine de la protection des données et de la cybersécurité, le signalement des dénonciateurs.rices peut prévenir les enjeux de cybersécurité qui pourraient nuire aux activités économiques et sociales du Canada, ainsi qu'aux services numériques.

Dans son rapport de janvier 2022, l'Assemblée citoyenne a exhorté le gouvernement fédéral « à réviser et à renforcer la protection des dénonciateurs afin de protéger les personnes qui peuvent démontrer que les actions de l'entreprise contribuent intentionnellement à la prévalence de désinformation[27]».

Précédents

Actuellement, seuls le Programme de dénonciateurs de l'inobservation fiscale à l'étranger (PDIFE) de l'Agence du revenu du Canada et la loi sur les dénonciateurs de la Commission des valeurs mobilières de l'Ontario protègent ces personnes dans le secteur privé[28].

Les États membres de l'UE ont mis en œuvre la directive européenne sur la protection des dénonciateurs. Des pays comme l'Australie, la Nouvelle-Zélande, le Japon et le Royaume-Uni disposent de lois sur l'emploi qui protègent les employés qui dénoncent des abus dans un contexte professionnel. Les États-Unis disposent d'un certain nombre de lois fédérales en vertu desquelles les dénonciateurs des secteurs public et privé peuvent recevoir des versements monétaires si leur employeur est condamné à la suite de leurs révélations.

THÈME 2 : RESPONSABILISATION

Définition

La responsabilisation désigne l'action de demander aux sociétés de plateforme de rendre compte de leurs opérations et de leurs pratiques commerciales ainsi que de leurs effets sur la société, en particulier pour les préjudices causés aux groupes historiquement marginalisés et aux personnes directement touchées par les pratiques discriminatoires. Les pratiques des plateformes peuvent être évaluées de différentes manières. Les évaluations indépendantes des risques sur un système effectuées avant la mise en œuvre peuvent évaluer les incidences et les performances potentielles, tandis que celles effectuées sur le comportement réel d'un système peuvent déterminer les préjudices et les menaces réels pour les différentes communautés et fournir des conseils sur l'atténuation. Les audits réalisés par différentes parties peuvent évaluer si une entreprise de plateforme a satisfait à un critère objectif ou universel[29]. Les organismes de réglementation, les politicien.ne.s, les représentant.e.s de la société civile et le public peuvent faire pression sur les plateformes pour qu'elles respectent leurs engagements de différentes manières, notamment par des sanctions en cas de non-respect, des mesures réglementaires plus strictes, de nouvelles lois, des enquêtes sur les fautes commises et des campagnes de sensibilisation du public.

Contexte

La responsabilisation des plateformes de médias sociaux doit d'abord commencer par la communication accrue d'informations relatives à leur fonctionnement aux utilisateurs.rices, aux annonceurs, aux organismes de réglementation, aux gouvernements et au grand public.

C'est une première étape essentielle, comme nous l'avons souligné sous le thème de la transparence. Mais le simple fait de savoir ce qui se passe ne suffit pas – si certaines formes de collecte, de recyclage et d'analyse des données compromettent l'expression démocratique, il ne suffit pas de donner aux gouvernements et aux chercheurs.euses la possibilité de reproduire ces effets.

Mais ces plateformes doivent être rendus responsables de quoi, devant qui, et par rapport à quelles règles et normes ? Nous pensons que la réponse commence par une recommandation formulée dans le premier rapport de la Commission en 2021. Elle demandait au gouvernement fédéral d'accorder une autorité législative à un nouvel organisme de réglementation qui serait chargé « de superviser et de faire respecter » un nouveau devoir d'agir de manière responsable sur les plateformes de médias sociaux[30].

La recommandation ajoute qu'il « faut constituer un organe indépendant du gouvernement en poste, et qui fonde les décisions des autorités judiciaires sur la primauté du droit et qui font l'objet d'un processus de révision », ajoutant qu' « une telle surveillance et application de la loi est essentielle pour atténuer les préjudices causés par le contenu en ligne et garantir l'imputabilité des plateformes ».

Le rapport poursuit en notant que les incitations « commerciales » de l'économie numérique et sa dimension mondiale font qu'il est difficile d'imaginer comment le système actuel de simple autorégulation pourrait un jour réussir. Du point de vue de la gouvernance, la protection des individus et des groupes identifiables incombe à juste titre aux autorités et aux institutions publiques. De par la nature même du média numérique, les plateformes continueront d'être la première ligne de défense contre les contenus préjudiciables. Elles seront toutefois dorénavant redevables de leurs responsabilités envers les gardiens légalement sanctionnés du bien public.

Ce devoir d'agir de manière responsable récuse la fausse prémisse selon laquelle le seul devoir des entreprises est de maximiser les bénéfices pour leurs propriétaires. Le devoir de responsabilité à exiger des plateformes doit également inclure la reconnaissance de l'incidence négative que leurs activités peuvent générer. Gagner de l'argent en vendant de la publicité, diffuser de l'information, orienter l'information vers un segment particulier de la population qui peut être vulnérable, ne se fait pas dans le vide et n'est pas sans

conséquence. Nous nous concentrons sur les préjudices à l'expression démocratique qui peuvent résulter de ces activités, mais comme le note le rapport de l'Assemblée citoyenne, les incidences négatives et les préjudices peuvent être beaucoup plus larges et s'étendre bien au-delà des menaces à l'expression démocratique.

L'obligation d'agir de manière responsable est la référence par rapport à laquelle les activités automatisées qui se produisent dans les « systèmes en boîte fermée » devraient être évaluées. Réfléchir et agir avec circonspection quant aux incidences négatives potentielles lors de la conception d'algorithmes afin d'éviter les préjugés et de s'assurer que les préjudices sont évités ; disposer de mécanismes de surveillance pour répondre aux préoccupations et aux plaintes ; consulter les plaignants sur la plateforme – tout cela peut réduire les sanctions imposées par un organisme de réglementation si une plateforme est jugée responsable de la violation de son devoir d'agir de manière responsable. Ces tactiques, ainsi que d'autres visant à prévenir les préjudices, peuvent toutes être codifiées dans le cadre du devoir de responsabilité de chaque plateforme individuelle lié à ses activités.

Recommandations

2.1 Accroître les capacités des organismes publics : Veiller à ce que les organismes de réglementation existants soient correctement habilités et outillés pour fonctionner dans le monde numérique du 21e siècle de manière efficace et efficiente. De plus, mettre en place un nouvel organisme fédéral de réglementation indépendant (comme indiqué ci-dessus et proposé dans le premier rapport de la Commission) doté de pouvoirs et de responsabilités en matière d'enquête, d'audit et de contrainte pour faire en sorte qu'une nouvelle obligation législative d'agir de manière responsable soit imposée aux plateformes. Au fil du temps, le nouvel organisme sera également chargé d'examiner systématiquement les politiques et les réglementations et de formuler des propositions de réforme si nécessaire.

Le mandat principal du nouvel organisme de réglementation est de superviser et de faire respecter le devoir d'agir de manière responsable. Ce devoir fait partie intégrante de toutes nos recommandations adressées aux plateformes. La coopération aux efforts de recherche fait partie de ce devoir d'agir de manière responsable, tout comme la réalisation d'évaluations d'incidence algorithmique et d'évaluations d'incidence sur les droits de l'homme, le cas échéant (voir recommandation 2.4). Il en va de même pour le respect des autres mesures de transparence et de responsabilisation que nous proposons tout au long de ce rapport.

L'organisme de réglementation se concentrerait sur les systèmes et opérations opaques des plateformes pour promouvoir et assurer la transparence et la responsabilisation, pour enquêter sur les préjudices perçus, pour évaluer la responsabilité des plateformes et pour déterminer et appliquer des solutions lorsque la responsabilité des plateformes est établie. L'organisme de réglementation doit être officiellement indépendant du gouvernement, des médias grand public et des plateformes. Le Conseil des médias sociaux,

que la Commission a proposé dans son premier rapport et dont les membres sont issus des plateformes, de la société civile, des citoyens et d'autres parties intéressées, serait le forum chargé de conseiller l'organisme sur la gouvernance, les politiques et les pratiques des plateformes. Cela garantirait, d'une part, l'impartialité de la prise de décision et, d'autre part, la coopération avec toutes les parties intéressées. Il est crucial de doter l'organisme de ressources adéquates et de le concevoir correctement, sur la base de consultations publiques visant à étoffer son champ d'action et ses attributions. L'organisme de réglementation doit fonctionner de manière transparente et responsable, et rendre compte au Parlement à intervalles réguliers, conformément à la loi.

Alors que l'organisme de réglementation se concentrerait sur les nouvelles capacités requises pour superviser et juger l'étendue et le degré des préjudices que peuvent causer les systèmes opaques et/ou automatisés, les enjeux liés à la protection de la vie privée demeureraient la responsabilité des commissaires à la protection de la vie privée fédéraux et provinciaux. Les questions sur la façon dont la politique de la concurrence pourrait aborder les systèmes fermés resteraient sous le contrôle du Bureau de la concurrence. Le mandat du nouvel organisme de réglementation comprendrait les approches détaillées dans les recommandations ultérieures du présent rapport concernant les évaluations de l'incidence des algorithmes et des droits de la personne et les vérifications algorithmiques, le respect par les plateformes de l'obligation d'agir de manière responsable, l'étendue de la responsabilité des plateformes pour les préjudices identifiés et les mesures correctives imposées en réponse.

Pour que l'organisme de réglementation puisse s'acquitter de ces responsabilités, le gouvernement a le devoir de s'assurer que toutes les personnes qui participent à la surveillance et à la réglementation de tout aspect des activités des plateformes sont correctement habilitées et outillées. Cela inclut celles œuvrant au sein de l'organisme que nous proposons ainsi que tout membre de groupes chargés de faire respecter la politique de concurrence et les lois et règlements fédéraux et provinciaux sur la protection de la vie privée. Il n'est pas approprié ou acceptable que ces groupes ne disposent pas des ressources et de l'autorité nécessaires pour travailler dans le monde numérique du 21e siècle. Ils doivent disposer :

- Du personnel qualifié suffisant qui comprend le monde numérique et qui peut y naviguer (tels que les scientifiques des données, les praticien.ne.s de l'IA, les spécialistes des sciences sociales, etc.).
- De la flexibilité financière pour concurrencer le secteur privé dans le recrutement des meilleurs talents.
- De la flexibilité et de l'autorité pour communiquer entre eux, permettant une plus grande coopération inter-agences pour répondre au besoin de réponses coordonnées au fait que la cause de certains préjudices peut dépasser les limites juridictionnelles d'un seul organisme de réglementation.

- De la capacité d'imposer des solutions proportionnelles à la situation financière des plateformes lorsqu'une évaluation de la responsabilité se termine par une indétermination de la responsabilité de la plateforme.

Il s'agit du contexte et de l'environnement institutionnels qui, selon nous, sont essentiels tant pour les plateformes que pour les organismes de réglementation pour s'assurer que nos recommandations sur la surveillance et la responsabilité permettent de répondre efficacement aux préjudices.

Précédents

Le Online Harms White Paper (« Livre blanc sur les préjudices en ligne ») au Royaume-Uni a proposé de conférer à un organisme de réglementation existant des télécommunications et des médias (Ofcom) de nouveaux pouvoirs et responsabilités pour surveiller le respect par les entreprises de leur obligation juridique de diligence envers leurs utilisateurs.rices. L'organisme britannique de réglementation vérifiera si les entreprises prennent les mesures nécessaires pour empêcher la propagation des préjudices sur leurs plateformes et limiter les contenus problématiques[31].

Des organismes de réglementation ont également été créés en Australie (eSafety Commission) et proposés dans l'Union européenne (Conseil européen des services numériques). Au Canada, une proposition antérieure sur les préjudices en ligne prévoyait la création de la Commission de la sécurité numérique, afin d'offrir un recours concernant des éléments de contenu précis, de superviser et d'enquêter sur les systèmes de modération des plateformes et de permettre l'imposition d'importantes pénalités administratives aux plateformes non conformes. La proposition comprenait également la création d'un conseil de recours et d'un conseil consultatif.

2.2. Imposer des obligations à plusieurs niveaux pour différents types de plateformes et/ou pour les services susceptibles d'être consultés par des mineurs et des adultes.

Toutes les plateformes, quelle que soit leur taille, ont le devoir d'agir de manière responsable. Toutefois, les obligations imposées aux plateformes individuelles peuvent différer selon le type et la taille de celles-ci et en fonction de leur capacité à se conformer aux exigences de la législation. Il y aurait également une différenciation entre les obligations imposées aux plateformes en fonction de leur utilisation par les mineurs (moins de 18 ans), et les adultes.

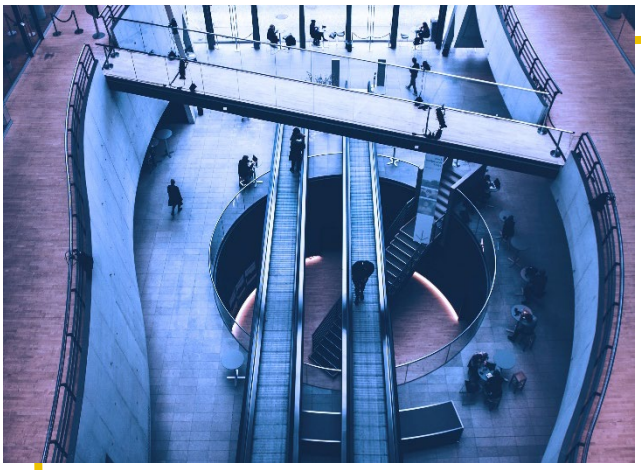
Les petites plateformes ne disposent pas des mêmes ressources que les grandes. Par conséquent, fixer les mêmes exigences reviendrait à imposer des obligations trop lourdes aux premières et insuffisantes aux secondes. Comme la Commission l'a noté dans son premier rapport, « le régime réglementaire mis en place pour les grandes plateformes mondiales pourrait imposer un fardeau trop lourd à leurs plus petits ou nouveaux concurrents dans l'espace numérique. Notre but n'est pas d'entraver par inadvertance la concurrence ou l'innovation. Le gouvernement et l'organisme de réglementation devront tenir compte des

différents niveaux de demandes imposées aux différentes entreprises[32]». Mais les petites plateformes peuvent aussi être des diffuseurs actifs de contenus préjudiciables. Cependant, l'obligation d'agir de manière responsable doit également s'appliquer, quelle que soit la taille de la plateforme. À d'autres égards, cependant, faire correspondre les obligations à la taille des plateformes permettrait de s'assurer que les grandes et les petites plateformes disposent de tous les moyens pour se conformer aux obligations qui leur sont imposées par les organismes de réglementation. Cela pourrait également protéger les petites plateformes ou les plateformes en démarrage contre le risque d'être submergées par les réglementations et de s'effondrer avant d'avoir eu l'occasion de s'établir. Des politiques appliquées de manière égale à toutes les plateformes, quelle que soit leur taille, pourraient consolider davantage le pouvoir des grandes plateformes, qui possèdent plus de moyens pour gérer la charge réglementaire[33].

Adapter les exigences au type de plateforme permettrait de faire en sorte que les obligations ciblent la résolution des enjeux propres à ce groupe de plateformes. Par exemple, les règlements visant les préjudices liés au contenu s'appliqueraient aux plateformes qui facilitent le partage de contenu généré par les utilisateurs.rices, mais pas aux plateformes de partage de services, tandis que les règlements visant la collecte de données et les audits algorithmiques concerneraient toutes les plateformes.

Adapter les obligations de la plateforme en fonction de l'âge de ses utilisateurs.rices permet de veiller à ce que les garanties établies au niveau international protègent l'intérêt supérieur des enfants.

La Convention des Nations Unies relative aux droits de l'enfant (CNUDE) reconnaît que les enfants ont besoin de garanties et de soins particuliers dans tous les aspects de leur vie et exige que ceux-ci soient garantis par des protections juridiques appropriées. La législation européenne sur la protection des données reflète ce principe et fournit ses propres garanties supplémentaires pour les enfants.



Précédents

Sur l'enjeu plus large des obligations hiérarchisées, la proposition de loi sur les services numériques de l'Union européenne établit une distinction entre les plateformes et les très grandes plateformes (celles dont la base d'utilisateurs.rices actifs représente plus de 10 % de la population européenne). Par exemple, les micro ou petites entreprises sont exemptées de l'obligation de fournir des rapports de transparence.

Aux États-Unis, lors d'une audience conjointe du Congrès, Mark Zuckerberg de Meta a soutenu une réforme de l'article 230 du Communications Decency Act qui obligerait les plateformes à mettre en place des « systèmes adéquats pour traiter les contenus illicites » et a soutenu que « les définitions d'un système adéquat pourraient être proportionnelles à la taille de la plateforme et fixées par un tiers » – en d'autres termes, il suggère qu'on impose des normes différentes selon la taille des plateformes[34].

Le projet de loi sur la sécurité en ligne du Royaume-Uni crée trois catégories de préjudice, chacune d'entre elles ayant des exigences différentes en matière de gestion des risques. Les catégories de préjudice sont les contenus illicites, les services susceptibles d'être consultés par des enfants et les contenus préjudiciables (mais non illicites) pour les adultes. Pour chacune d'entre elles, les entreprises doivent procéder à des évaluations des risques et se conformer à des « obligations de sécurité[35] ».

2.3. Légiférer sur les protections de la responsabilité des intermédiaires et les exceptions pour la responsabilité des plateformes.

En précisant la responsabilité des conséquences préjudiciables générées par les systèmes de recommandation algorithmique et les outils d'amplification des plateformes, on encouragerait ces dernières à mieux modérer le contenu généré par les utilisateurs.rices. Il faut autoriser, avec discernement, les utilisateurs.rices à exprimer librement leurs opinions en ligne (dans les limites prévues par la loi canadienne). En même temps, le fait de rendre les plateformes responsables de toute expression problématique des utilisateurs peut entraîner une suppression excessive de contenu et la censure. Néanmoins, la mesure dans laquelle le contenu problématique est amplifié et l'incidence des systèmes de recommandation sur l'opinion publique doivent être prises en considération dans l'examen du rôle des plateformes dans les sociétés démocratiques. L'imposition d'une responsabilité appropriée des plateformes quant à la manière dont le contenu est modéré inciterait les plateformes à veiller à ce que l'incidence du contenu problématique reste limitée et que les individus conservent leur liberté.

Les lois sur la responsabilité des intermédiaires précisent dans quels cas une plateforme peut être tenue légalement responsable des préjudices résultant du contenu publié par ses utilisateurs.rices.

Le Canada dispose de lois sur la responsabilité des intermédiaires pour traiter des droits d'auteur, mais il est la seule économie du G7 à ne pas avoir une telle loi régissant toutes les autres questions de responsabilité en matière de contenu. La poignée de cas portés devant les tribunaux canadiens qui ont examiné la question de savoir si les plateformes devraient être responsables du contenu affiché par leurs utilisateurs.rices ont fourni aux plateformes des protections très limitées en matière de responsabilité. Pourtant, l'élaboration de telles

normes est importante pour protéger à la fois la liberté d'expression et l'innovation dans l'économie numérique.

Le Canada a besoin d'une loi sur la responsabilité des intermédiaires. Nous pensons que le gouvernement fédéral devrait instaurer une législation qui intègre des protections en matière de responsabilité des intermédiaires conformes à l'article 19.17 de l'Accord Canada-États-Unis-Mexique (ACEUM) de 2020 sur le commerce entre les trois pays. Une telle législation permettrait de préciser quand les plateformes peuvent être tenues responsables des préjudices découlant du contenu affiché sur la plateforme par les utilisateurs.rices. L'adoption d'une telle législation au Canada pourrait stimuler le développement de nouvelles plateformes sociales ici au Canada qui serviraient d'options autres que les grandes plateformes basées dans d'autres pays.

En vertu d'une telle loi, les utilisateurs de la plateforme seront tenus responsables du contenu qu'ils publient et pourront être poursuivis par le biais du système juridique pour tout préjudice qu'ils causent – par exemple en portant atteinte à la réputation d'une personne ou en violant sa vie privée.

Une telle législation peut et doit laisser ouverte la possibilité que les plateformes soient tenues responsables de la violation de leur devoir d'agir de manière responsable en ce qui concerne la curation algorithmique et l'amplification de certains types de contenu.

Sous le nouveau régime de transparence et de responsabilité que nous proposons, le nouvel organisme de réglementation et les membres du public disposeraient des informations nécessaires pour évaluer si les entreprises technologiques doivent être poursuivies en justice pour violation du devoir d'agir de manière responsable (ou de leurs autres obligations juridiques). Les tribunaux peuvent imposer des pénalités financières pour de telles violations de la loi, ou émettre des injonctions pour obliger les entreprises à agir de manière plus responsable.

Le Parlement pourrait envisager de promulguer des dispositions dites de « sphère de sécurité » dans une telle législation, qui permettraient aux entreprises technologiques de s'opposer à des poursuites fondées sur des violations présumées de leur devoir d'agir de manière responsable, en démontrant qu'elles ont agi de bonne foi pour s'acquitter de ce devoir – par exemple en mettant en œuvre les mesures de transparence et de responsabilité que nous proposons dans ce rapport (en participant à des évaluations d'incidence algorithmique ou en coopérant de bonne foi avec des chercheurs.euses indépendants, par exemple).

Précédents

La directive européenne sur le commerce électronique étend les protections en matière de responsabilité aux services en ligne lorsque leur activité est « de nature purement technique, automatique et passive ». La proposition de loi sur les services numériques contient des dispositions similaires, mais ajoute également un certain nombre de nouvelles obligations.

Aux États-Unis, l'article 230 de la loi sur la décence en matière de communications (Communications Decency Act) accorde une immunité aux plateformes pour le contenu des tiers (sauf lorsque le contenu en question viole les droits d'auteur, comporte une exploitation sexuelle des enfants ou un trafic sexuel, ou est en violation du droit pénal fédéral). L'article 512 du Digital Millennium Copyright Act limite la responsabilité des intermédiaires si la plateforme réagit rapidement pour retirer ou désactiver certains contenus illicites publiés sur sa plateforme par un autre individu. La proposition de Justice Against Malicious Algorithms Act (loi américaine sur la justice contre les algorithmes malveillants) supprimerait l'immunité de l'article 230 si une plateforme en ligne utilise sciemment ou par imprudence un algorithme personnalisé pour recommander du contenu à un utilisateur en fonction de ses renseignements personnels, et si cette recommandation contribue matériellement à un préjudice physique ou émotionnel grave (par exemple, discours haineux ou contenu sur les troubles alimentaires)[36].

2.4. Habiliter les organismes de réglementation à développer et mettre en œuvre un cadre de responsabilité algorithmique fondé sur les droits qui comprend des évaluations de l'incidence algorithmique (EIA), des évaluations de l'incidence sur les droits de la personne (EIDP) et des audits algorithmiques.

Les systèmes algorithmiques sont de plus en plus utilisés dans le cadre de processus décisionnels automatisés, tant dans le secteur privé que dans le secteur public, souvent sans consentement valable, sans protection de la vie privée ni recours pour ceux/celles qui risquent d'être les plus touchés par leurs décisions. Les entités de réglementation concernées devraient pouvoir élaborer et mettre en œuvre un cadre de responsabilité algorithmique solide, centré sur des approches de la gouvernance algorithmique fondées sur les droits. Le fait de placer les droits au centre des cadres de responsabilité des systèmes automatisés de prise de décision est conforme aux normes internationales visant à traiter les ris7ques accrus pour la sécurité et les libertés fondamentales, tels que le droit à la non-discrimination[37]. Les approches fondées sur les droits doivent être à l'épreuve du temps face aux risques posés par les systèmes d'intelligence artificielle, et les obligations imposées aux acteurs déployant des systèmes d'intelligence artificielle à haut risque doivent permettre de rendre des comptes aux personnes directement touchées par ces systèmes. Les évaluations de l'incidence algorithmique (EIA), les évaluations d'incidence sur les droits de la personne (EIDP) et les audits algorithmiques devraient servir à protéger les droits et à assurer réparation aux personnes touchées par l'intelligence artificielle (IA).

Les plateformes devraient être tenues de s'engager à respecter les droits de la personne et à réduire de façon satisfaisante toute incidence négative que leurs services pourraient avoir.

Les évaluations d'incidence sur les droits de la personne (EIDP) ont traditionnellement été utilisées pour évaluer l'incidence des pratiques commerciales, des politiques publiques et des technologies sur les droits

de la personne pour anticiper la conformité avec les lois et les cadres relatifs aux droits de la personne[38]. Par conséquent, le fait de rendre les EIDP obligatoires obligerait les plateformes à entreprendre un examen systématique et périodique de l'incidence que leurs services pourraient avoir sur les droits de la personne avant leur mise en œuvre et à voir dans quelle mesure atténuer ces risques[39]. Les organisations spécialisées dans les droits de la personne évalueraient les politiques, les pratiques, les produits et les services d'une plateforme afin de cerner les violations des droits de la personne[40].

Les évaluations de l'incidence algorithmique (EIA) ont les mêmes objectifs, à savoir comprendre les incidences d'un système algorithmique ex ante (avec un certain potentiel de réponses ex post). Toutefois, elles encouragent principalement les développeurs.euses à cerner et à atténuer les risques potentiels des systèmes algorithmiques en s'appuyant sur un cadre axé sur les préjudices algorithmiques plutôt que sur les droits de la personne (par exemple, les enjeux des préjugés, les préoccupations concernant la transparence et la possibilité de réduire les incidences d'un système, les incidences environnementales du système) et l'éthique des données[41]. Au regard des changements continus qui touchent le fonctionnement des algorithmes, les EIA doivent non seulement être réalisées avant leur mise en œuvre, mais aussi régulièrement, avant d'entreprendre un nouveau traitement de données. Des évaluations de risque rigoureuses devraient déterminer, dans les cas à haut risque ou sensibles[42], si certains systèmes doivent être conçus. Les EIA servent à atténuer le risque de préjudice. Cela est particulièrement pertinent pour les groupes connus pour être touchés de façon disproportionnée par les systèmes algorithmiques dans les processus décisionnels privés et publics, notamment les groupes historiquement marginalisés.

L'atténuation et la prévention proactives des préjudices sont particulièrement importantes pour les services auxquels les enfants sont susceptibles d'accéder en raison du traitement spécial qui leur est accordé, au regard de leur vulnérabilité en matière de développement et de leur statut d'utilisateurs précoces de services en ligne.

Outre l'obligation de réaliser des EIDP et des EIA, il est fondamental d'exiger des développeurs.euses (créateurs.trices) et des « déployeurs.euses » (ceux/celles qui achètent ou mettent en service le système) qu'ils/elles tiennent un document détaillant la procédure de prise de décision pendant le processus de conception et le déploiement d'un algorithme, afin de déterminer si celui-ci a une incidence négative sur les utilisateurs.trices. Ces renseignements devraient être présentés publiquement dans une documentation cohérente, claire et accessible, laquelle devrait clarifier l'utilisation prévue d'un système automatisé de prise de décision et inclure une description des politiques et processus dans le cadre desquels l'algorithme fonctionne.

Cette documentation pourrait être divulguée dans le cadre des rapports d'audit des algorithmes, qui seront mis à la disposition du public. Dans l'ensemble, les audits algorithmiques sont une méthode permettant d'évaluer systématiquement a posteriori si les algorithmes et leurs résultats causent des préjudices, tels que des violations de la vie privée, la prévalence de discours haineux, et si leurs décisions sont de nature partiale ou discriminatoire. Pour être efficace, la méthodologie d'audit doit être adaptée à l'architecture technique, aux possibilités et aux caractéristiques précises des différentes organisations[43]. En outre, les audits peuvent avoir des objectifs différents selon l'entité qui les réalise. Les audits de premier niveau et de deuxième niveau sont réalisés à l'initiative de l'organisation elle-même, respectivement par des membres de l'organisation ou par de tiers contractuels. Ces deux types d'audits permettent un contrôle et une évaluation proactifs par les plateformes qui causent des préjudices[44]. En revanche, les audits de troisième niveau sont réalisés par un.e vérificateur.trice indépendant sans l'autorisation de l'organisation. Ces audits sont particulièrement importants, car ils permettent une évaluation véritablement indépendante et crédible. Toutefois, ils sont souvent entravés par le manque d'accessibilité aux données dont les tiers ont besoin pour les réaliser.

Précédents

Dans l'Union européenne, les analyses d'incidence relatives à la protection des données sont déjà exigées par le Règlement général sur la protection des données (RGPD), et d'autres formes d'évaluation des risques sont proposées à la fois dans la Législation sur les services numériques (LSN) et dans le règlement sur l'intelligence artificielle[45]. De plus, la proposition de la LSN rend également obligatoire la réalisation d'audits par des vérificateurs.trices indépendants possédant des connaissances techniques des algorithmes et d'autres compétences, et donne aux autorités nationales (« coordonnateurs de services numériques ») et, dans certaines circonstances, à la Commission européenne, le pouvoir de procéder à des inspections sur place de ces entreprises[46].

Au Canada, la directive sur la prise de décision automatisée est un exemple concret d'un processus d'évaluation de l'incidence algorithmique (EIA) en cours. Elle utilise un modèle de questionnaire sur les EIA qui exige qu'un format de questions-réponses soit rempli avant le déploiement d'un système de prise de décision automatisé dans le secteur public[47]. L'Ontario[48] et le Québec[49] ont déjà mis en place des audits algorithmiques. Les évaluations de l'incidence algorithmique et les audits s'aligneraient sur les recommandations formulées par le Commissariat à la protection de la vie privée du Canada[50].

À l'étranger, le Commissariat à l'information du Royaume-Uni a récemment élaboré un cadre d'audit des algorithmes, qui met l'accent sur la gouvernance et la responsabilité, ainsi que sur les risques propres à l'IA[51]. La responsabilité algorithmique a également fait l'objet de nombreux projets de loi aux États-Unis, notamment dans l'Algorithmic Accountability Act[52] et l'Algorithmic Justice and Online Transparency Act[53].

En ce qui concerne les études d'incidence sur les droits de la personne, l'exemple phare se trouve dans les principes directeurs des Nations unies relatifs aux droits de la personne et aux entreprises, qui exigent que les entreprises garantissent le respect des droits internationaux de la personne par l'entremise d'un processus de diligence raisonnable visant à identifier, prévenir, atténuer et rendre compte de la façon dont elles réduisent l'incidence des algorithmes sur les droits de la personne[54].

2.5. Élaborer un code de bonnes pratiques contre la désinformation.

Le Canada devrait élaborer un code de bonnes pratiques sur la désinformation, conformément aux efforts similaires déployés par l'Union européenne pour établir des engagements et des exigences en collaboration avec les principales plateformes en ligne. L'objectif général du Code est de promouvoir l'élaboration de politiques et de procédures relatives aux plateformes pour lutter contre la désinformation, notamment en démonétisant les contenus problématiques, en améliorant la transparence des publicités politiques et thématiques, en donnant aux utilisateurs.rices les moyens de mieux contrôler leurs activités en ligne et en permettant un accès aux données respectueux de la vie privée pour les activités de vérification des faits et de recherche.

Le code représenterait un moyen efficace de collaboration entre les institutions publiques et les entreprises technologiques, surtout si l'on considère que la lutte contre la désinformation doit être une responsabilité et un objectif communs. Les mesures juridiques non contraignantes, telles que le code de bonnes pratiques sur la désinformation, se caractérisent par leur flexibilité et leurs faibles coûts de transaction avant la conclusion d'une entente. Les normes juridiques non contraignantes facilitent également les révisions systémiques, afin de s'assurer que les dispositions ciblent constamment les enjeux sociétaux contemporains.

Précédents

Au cours des deux années qui ont suivi son adoption, le Code de bonnes pratiques de l'UE sur la désinformation s'est révélé être un instrument précieux pour améliorer la collaboration des plateformes signataires et a fourni un cadre pour un dialogue structuré entre les parties prenantes concernées, afin d'assurer une plus grande transparence des politiques des plateformes contre la désinformation au sein de l'Union européenne. Au cours des premiers mois de son fonctionnement, le code prévoyait des discussions mensuelles avec ses signataires, afin de permettre une évaluation de son fonctionnement et une rétroaction réciproque. De plus, en comparant les rapports au fil du temps, tous les signataires ont montré des améliorations sur les cinq engagements décrits dans le code, ce qui pourrait renforcer encore les avantages d'un outil de collaboration tel que le code.

Le code de conduite de l'UE sur la lutte contre les discours haineux illégaux en ligne a servi d'approche introductive pour encourager les efforts des plateformes. Ses exigences en matière de transparence n'ont pas, à elles seules, permis la mise en place de mécanismes de responsabilisation, car elles mettaient l'accent sur le taux et la vitesse de suppression des contenus plutôt que sur une analyse du type de contenu

supprimé. Le code est réputé avoir jeté les bases des exigences plus strictes, qui sont maintenant imposées dans la Loi sur les services numériques[55].

THÈME TROIS : AUTONOMISATION

Définition

L'autonomisation consiste à donner aux utilisateurs.trices de plateformes en ligne la capacité de gérer leur présence en ligne, en accordant la priorité à la protection et à la mobilisation de leurs droits démocratiques. Elle vise à corriger les déséquilibres de pouvoir sociétaux et les inégalités structurelles qui peuvent être amplifiés par les systèmes technologiques. Dans un cadre général, l'autonomisation peut comprendre les droits des utilisateurs.trices (par exemple, la protection des données, l'accès à l'information, la liberté d'expression, etc.), les obligations liées aux plateformes (par exemple, la protection intégrée, les outils de contrôle des utilisateurs.trices, la transparence significative, la modération du contenu), des mesures réglementaires (par exemple, les mécanismes d'application rigoureux) et des programmes publics (par exemple, des initiatives d'éducation civique et numérique pour que le public comprenne les choix qui s'offrent à lui en ligne).

Contexte

Le respect et la protection des droits de la personne sont essentiels à l'expression démocratique pour permettre aux individus et aux groupes de participer librement et en toute sécurité à notre société sans que ces droits soient menacés ou restreints. Le respect et la protection de ces droits sont également des principes clés intégrés dans toutes nos recommandations tout au long du présent rapport.

Les utilisateurs.trices des plateformes sont des détenteurs.trices de droits en vertu du droit canadien et international, et nos recommandations sont conçues pour permettre aux individus de jouir et d'exercer leurs droits tout en respectant les droits des autres.

Au Canada, ces droits de la personne comprennent à la fois des protections prévues par la loi et des enjeux relatifs aux interactions entre les utilisateurs.trices et les plateformes de médias sociaux, comme le droit à la vie privée, le droit à la propriété et au contrôle de sa propre identité et le droit à la protection contre les discours haineux, les abus et le harcèlement et les préjudices qui en découlent.

Les activités des plateformes doivent être conformes au droit canadien et aux normes internationales en matière de droits de la personne, mais au-delà de cela, nous pensons que des mesures supplémentaires doivent être prises pour remédier au déséquilibre de pouvoir mentionné plus haut dans notre rapport entre les plateformes et les droits dont disposent les utilisateurs.trices, afin de s'assurer que leurs droits fondamentaux ne sont pas menacés ou violés. Cela commence par donner aux utilisateurs.trices les moyens de décider du degré de contrôle qu'ils/elles souhaitent exercer sur les informations et données démographiques qu'ils/elles fournissent aux plateformes et sur l'utilisation de ces données dans leurs systèmes. De telles décisions ne peuvent être prises qu'avec un consentement éclairé et une compréhension raisonnable des systèmes opaques, et avec la liberté de quitter un service particulier sans la menace de perdre les connexions existantes avec ces plateformes.

Cela implique également l'obligation que nous recommandons d'imposer aux plateformes afin qu'elles agissent de façon responsable. Cela consiste à connaître, comprendre et à s'assurer que ce qui se passe à l'intérieur des systèmes automatisés et autrement fermés fait progresser les droits de la personne. Les utilisateurs.trices doivent avoir les renseignements et la capacité de déterminer si leurs droits ne sont pas protégés et, le cas échéant, de se plaindre qu'une plateforme a manqué à son devoir d'agir de façon responsable.

Cette obligation pour les plateformes d'agir de façon responsable doit également inclure des dispositions particulières pour la protection des droits des enfants, universellement reconnus comme une population vulnérable, contre le harcèlement, les menaces et les brimades en ligne – dans certains cas même de la part d'autres jeunes – qui peuvent être particulièrement dommageables pour les enfants et les adolescent.e.s. Ils représentent également une part importante et croissante des utilisateurs.trices de plateformes de médias sociaux. Leur vie privée en ligne doit faire l'objet d'une protection particulière, peut-être par voie législative. De plus, les données relatives aux enfants ne devraient pas être recueillies ni conservées par les plateformes de médias sociaux.

Cette lacune dans les lois sur la protection de la vie privée des enfants témoigne d'un besoin plus large de renforcer et de moderniser toutes les législations sur la protection de la vie privée, tant à l'échelle fédérale que provinciale. Une grande partie d'entre elles sont obsolètes et doivent être révisées pour s'adapter à l'ère numérique et surmonter les nouveaux défis qu'elle a créés, en particulier pour les plateformes de médias sociaux. Sans une telle révision, nous ferons face à un éventuel « effet paralysant » sur l'expression démocratique, dans la mesure où les individus deviennent plus conscients de la voracité de la collecte et de l'analyse des données, mais n'ont aucun moyen d'y remédier[56]. Les responsables de la protection de la vie privée ont formulé des recommandations dans le passé. Il est maintenant temps pour les gouvernements d'agir et d'adopter une législation contemporaine relative à la protection de la vie privée dont nous avons tant besoin.

Recommandations

3.1 Soutenir le développement des connaissances, des relations et des protocoles autochtones ainsi que la gouvernance des données des Autochtones pour les collectivités autochtones.

Soutenir une participation significative des Autochtones et veiller à intégrer les relations et protocoles autochtones dans l'élaboration des politiques, outils et mécanismes technologiques et sociaux. Il s'agit notamment de fonder la recherche sur des épistémologies autochtones élaborées par et avec les peuples et les communautés autochtones, de former des scientifiques et des technologues autochtones spécialisés dans les données, d'attribuer des sièges au sein des comités, des conseils de surveillance et d'autres organismes de réglementation, de veiller à ce que les valeurs autochtones propres aux communautés soient intégrées aux protocoles fondamentaux régissant la façon dont l'IA est développée et déployée par les peuples et les communautés autochtones, et d'accorder la priorité au financement pour soutenir les épistémologies autochtones en ligne. Les initiatives visant à sauvegarder la gouvernance des données des Autochtones doivent également être soutenues. Le gouvernement fédéral doit collaborer avec les Autochtones, les collectivités et les organisations pour s'assurer que les droits de gouvernance des données des Autochtones sont respectés et que ceux-ci/celles-ci possèdent les moyens de mener à bien les programmes qu'ils/elles ont eux-mêmes définis. Le soutien supplémentaire devrait inclure le financement, la création de nouvelles propositions législatives, des programmes de littératie autour de la propriété des données et de l'autodétermination, et d'autres besoins recensés en partenariat avec les peuples et collectivités autochtones.

Internet et les technologies numériques en général peuvent jouer un rôle dans la transmission au grand public de connaissances importantes sur l'histoire et les traités, les tactiques de colonisation et d'assimilation en cours, et la quête permanente d'une vie digne en tant que peuple autochtone au Canada.

En garantissant une participation significative des représentant.e.s des peuples autochtones, nous préserverons les intérêts des peuples autochtones en abordant les enjeux de démocratie en ligne et nous éclairerons les valeurs collectives de réciprocité et d'autodétermination dans son ensemble.

L'expression démocratique par l'entremise de l'intégration des savoirs autochtones dans l'éducation est également une réponse à la haine en ligne, à la désinformation et au racisme permanent visant les communautés autochtones, qui représentent certaines des populations les plus vulnérables du Canada. Le soutien officiel et substantiel apporté à l'élaboration des connaissances, des relations et des protocoles autochtones permettra de remédier à des pratiques problématiques courantes, telles que la non-citation

d'auteurs autochtones dans des articles traitant de sujets autochtones et la participation symbolique d'universitaires autochtones à des propositions de subventions impliquant des recherches autochtones[57].

Des consortiums internationaux sur les protocoles autochtones à l'égard de l'IA mettent au point des outils d'IA et adoptent des approches conceptuelles et de gouvernance pour le développement une IA qui met l'accent sur l'expérience et les relations des peuples autochtones avec l'IA.

S'agissant de la gouvernance, les données constituent un atout culturel, stratégique et économique pour les peuples autochtones. En garantissant que les peuples autochtones ont et conservent la gouvernance des données autochtones, on s'assure que les renseignements sont utilisés pour réaliser des programmes de développement autochtones. La gouvernance des données peut également être un outil stratégique de décolonisation. Au plan interne, la gouvernance des données permet à la communauté autochtone de mieux se connaître et peut aider à soutenir les projets de décolonisation et d'autodétermination. Au plan externe, la gouvernance des données garantit que les communautés autochtones sont bien placées pour interagir avec les entités coloniales et pour obliger ces dernières à repenser la méthodologie de recherche conventionnelle et les données défectueuses qui y sont associées[58].

Précédents

Le groupe de travail sur le protocole autochtone et l'intelligence artificielle adoptent de nouvelles approches conceptuelles et pratiques pour construire la prochaine génération de systèmes d'IA[59]. L'International Wakashan AI Consortium développe des outils d'IA pour représenter et protéger les langues parlées dans plusieurs communautés des Premières nations[60].

Le projet de loi C-11 récemment présenté par le Canada prévoit l'obligation pour les services de radiodiffusion d'offrir des possibilités aux personnes autochtones et une programmation reflétant les cultures autochtones, dans les langues autochtones et accessibles à tous[61].

En Australie, le gouvernement finance le « Carrefour de la propriété intellectuelle sur les connaissances autochtones » qui offre un espace aux personnes qui souhaitent travailler sur les connaissances autochtones[62].

3.2 Renforcer considérablement l'éducation civique en matière de respect des droits, de littératie numérique et d'accès à l'information de qualité pour soutenir les groupes de défense de l'équité et les programmes pilotés par les collectivités.

Les initiatives d'éducation publique et de littératie numérique doivent permettre au public de comprendre ses droits et libertés, le fonctionnement des médias numériques, l'incidence qu'ils peuvent avoir sur l'opinion publique et la manière dont les préjugés structurels y opèrent et renforcent les inégalités dans la vie réelle. Il s'agit notamment de doter les citoyen.ne.s de compétences leur permettant de reconnaître les préjugés et d'évaluer la fiabilité de l'information, de savoir

comment rechercher, naviguer, synthétiser et évaluer le contenu en ligne, et de savoir comment participer utilement aux communautés en ligne. Bien que les programmes doivent être accessibles et axés sur l'amélioration de la culture numérique dans l'ensemble de la population, notamment les communautés plus difficiles à atteindre, certains groupes doivent être ciblés afin de minimiser l'effet de préjudices en ligne et structurels particuliers. Par exemple, les parents, les tuteurs.trices et les enfants devraient être informés des risques liés à l'accès des enfants aux services en ligne, en plus de la culture numérique des enfants. Les groupes sous-représentés devraient être soutenus par des politiques et des programmes ciblés qui renforcent l'équité, y compris le financement de la production numérique des cultures et des connaissances autochtones. Les programmes doivent être proposés dans plusieurs langues, y compris les langues autochtones.

Les initiatives numériques et civiques devraient être mises en œuvre de concert avec des mesures visant à soutenir l'information de qualité en ligne, telles que l'incitation à l'information de qualité et à la réduction des préjudices (par exemple, le renforcement des réseaux de vérification des faits et la recherche sur l'authenticité en ligne), l'investissement dans le journalisme communautaire et le journalisme de qualité, et le soutien de certaines formes de création et de partage de l'information (par exemple, les médias communautaires, les médias locaux, les médias traditionnels et les médias numériques).

Les connaissances civiques profitent à la fois aux simples citoyen.ne.s et à la société dans son ensemble. Elles doivent désormais englober l'alphabétisation numérique pour refléter l'engagement civique à l'ère numérique. Elles encouragent les citoyens à voter, favorisent la connaissance de ses propres intérêts politiques et de la façon de les faire progresser, diminuent la probabilité d'être manipulé par des campagnes politiques négatives et polarisées et améliorent le développement général de la collectivité[63].

La culture numérique, qui comprend un large éventail de pratiques sociales et réflexives intégrées au travail, à l'apprentissage, aux loisirs et à la vie quotidienne, peut prévenir de nombreux préjudices en ligne, notamment la diffusion de contenus illégaux/préjudiciables en ligne.

Les enfants sont particulièrement vulnérables aux préjudices numériques, et la recherche a montré que l'éducation à la culture numérique à un jeune âge entraîne une plus grande résilience à la fois pour les jeunes et leur entourage[64]. L'inclusion de l'alphabétisation raciale dans la culture numérique permet d'aborder les implications raciales indissociables de la technologie[65]. L'inclusion de l'alphabétisation raciale dans les programmes disciplinaires aidera également les personnes impliquées dans la conception, le développement et le déploiement de la technologie à prendre en compte les enjeux raciaux[66].

Le renforcement du soutien public aux groupes marginalisés et en quête d'équité encourage les mesures proactives et la résilience des communautés face aux préjudices en ligne.

Des recherches ont montré que l'accès à un plus grand nombre de connaissances autochtones en ligne augmenterait non seulement la viabilité de ces connaissances, mais faciliterait aussi de meilleures relations entre les allochtones et les communautés autochtones[67]. Des renseignements fiables et exacts, partagés par un écosystème journalistique et médiatique solide, sont essentiels pour permettre au public de prendre des décisions en connaissance de cause et pour garantir un contrôle indépendant des acteurs puissants.

De même, le rapport final de janvier 2022 de l'Assemblée des citoyens canadiens sur l'expression démocratique a présenté une série de recommandations sur l'éducation et la sensibilisation du public, dont une qui demande au gouvernement fédéral de créer et de financer un Centre de prévention de la désinformation qui jouerait un rôle majeur dans l'éducation des Canadiens et Canadiennes sur tous les aspects de la désinformation[68].

3.3 Rendre obligatoires l'interopérabilité et la mobilité des données.

Les systèmes d'information doivent pouvoir interagir et échanger régulièrement des informations entre eux, ce qui permettrait entre autres aux jeunes entreprises et les coopératives de plateformes de se connecter aux services existants. Le Canada devrait assurer l'interopérabilité des services numériques afin de donner aux personnes un plus grand choix et un meilleur contrôle sur leurs interactions en ligne. De plus, le Canada doit introduire le droit à la portabilité des données – donnant aux gens le droit de voir leurs données personnelles transmises directement d'une plateforme à une autre, sans entrave.

Garantir l'interopérabilité des systèmes d'information en rendant obligatoire l'existence d'une infrastructure permettant aux systèmes d'information de communiquer entre eux et d'échanger l'information est nécessaire pour mieux outiller les utilisateurs.trices. L'interopérabilité peut favoriser la concurrence et l'innovation en permettant à d'autres acteurs tels que les entreprises en démarrage et les coopératives de plateformes de se connecter aux services existants, entravant ainsi la tactique des sociétés de plateformes dominantes qui consiste à tirer parti d'un service à leur avantage en mettant les utilisateurs.trices « sous les verrous ». Le principal avantage de l'interopérabilité est qu'elle peut donner aux utilisateurs.trices plus de pouvoir sur leurs données et permettre aux utilisateurs.trices insatisfaits de quitter les systèmes d'information tout en conservant des liens avec d'autres utilisateurs.trices, notamment les familles, les collectivités et les client.e.s. Bien que l'interopérabilité puisse entraîner de nouveaux risques pour la vie privée des utilisateurs.trices et la sécurité des données, si elle est développée de façon adéquate, l'interopérabilité peut être un gain net pour le droit à la vie privée des utilisateurs.trices[69].

L'interopérabilité a également été abordée au niveau des solutions antitrust et des contrôles réglementaires. Le projet de loi sur l'accès à l'information aux États-Unis exige que les plateformes applicables n'apportent pas de modifications à leurs interfaces d'interopérabilité sans l'approbation de la Federal Trade Commission[70]. L'Union européenne a également exprimé la nécessité de renforcer l'interopérabilité dans le

projet de loi sur les marchés numériques qui exigerait une interopérabilité totale dans les services essentiels et auxiliaires[71].

Rendre l'interopérabilité obligatoire renforcera l'efficacité du droit à la portabilité des données, qui offre aux utilisateurs.trices un choix et un contrôle sur leurs données, tant au sens démocratique que commercial.

La portabilité des données peut améliorer la vie privée grâce à un contrôle accru confié aux utilisateurs.trices. En effet, dès lors que les utilisateurs.trices peuvent décider de transférer leurs données vers une autre plateforme automatiquement et sans charges supplémentaires, les plateformes seront contraintes de se faire concurrence pour offrir des garanties solides en matière de traitement des données afin d'attirer les utilisateurs.trices.

Le règlement général sur la protection des données de l'Union européenne codifie le droit à la portabilité des données à l'article 20. Par analogie, la portabilité des données est également garantie par la *Loi brésilienne sur la protection des données* et par la *Loi californienne sur la protection de la vie privée des consommateurs*. Aux États-Unis, le droit à la portabilité des données a été proposé dans le projet de loi sur l'accès à l'information.

3.4 Moderniser la législation canadienne sur la protection de la vie privée.

La protection de la vie privée est fondamentale pour les droits de la personne et l'expression démocratique. La collecte systématique de données et le ciblage en ligne n'interfèrent non seulement avec l'expression démocratique, mais peuvent aussi menacer les droits de la personne et les libertés civiles et priver les utilisateurs.trices de leur autonomie. Le Canada doit mettre à jour sa législation sur la protection de la vie privée afin d'adopter un cadre basé sur les droits pour les développements technologiques actuels et futurs. Il faudrait conférer au commissaire à la protection de la vie privée du Canada une plus grande autorité pour moderniser le cadre législatif actuel du Canada en matière de protection de la vie privée et décider de la manière dont les entreprises de plateformes privées peuvent recueillir, traiter et cibler les données des individus.

Le régime canadien actuel de protection de la vie privée dans le secteur privé date de 20 ans et ne reflète pas les changements technologiques, sociaux et juridiques importants survenus au cours des deux dernières décennies.

Au cours de leurs témoignages devant la Commission, des expert.e.s canadiens et internationaux ont encouragé le Canada à moderniser sa législation actuelle sur la protection de la vie privée pour l'adapter à

un cadre fondé sur les droits. En parallèle, l'Assemblée citoyenne canadienne sur l'expression démocratique 2021-22 a réuni plusieurs expert.e.s qui ont également mis l'accent sur le renforcement des lois sur la protection de la vie privée pour enrayer la diffusion de la désinformation et interdire l'utilisation des données personnelles en vue d'un microciblage. L'Assemblée citoyenne a reconnu qu'en renforçant la protection de la vie privée des utilisateurs.trices et le droit des individus à contrôler qui utilise et accède à leurs données, les groupes vulnérables et marginalisés seraient davantage en mesure de tenir les entreprises de plateformes responsables des préjudices indus en ligne[72].

Sans un solide régime de protection de la vie privée fondé sur les droits, le Canada ne peut protéger adéquatement les droits d'expression démocratique des enfants, des peuples autochtones et des autres groupes marginalisés.

La sensibilisation accrue du public à la collecte et au ciblage des données en ligne sans moyens de recours adéquats peut en outre avoir un « effet paralysant » sur l'expression démocratique en limitant la participation en ligne des individus, en particulier des groupes vulnérables.

Dans le cadre de la modernisation de la législation canadienne sur la protection de la vie privée, le Commissariat à la protection de la vie privée du Canada devrait se voir conférer une plus grande autorité pour prendre des décisions sur la pratique du microciblage – des messages publicitaires destinés à des communautés précises – en particulier l'importance de connaître qui a vu une publicité en fonction de certains critères d'intérêt plutôt que de connaître les catégories utilisées pour cibler la publicité en premier lieu. Bien que certains expert.e.s, qui ont informé le Commissariat, aient soutenu les propositions faites dans d'autres provinces pour interdire le microciblage, le Commissariat pense que le Canada bénéficierait d'une approche plus nuancée de la question du microciblage qu'une interdiction et suggère que le Commissariat à la protection de la vie privée ait plus de pouvoir pour décider de la façon de réglementer le microciblage.

Jusqu'à présent, les efforts visant à protéger et à promouvoir l'expression démocratique et à protéger la vie privée ont été traités comme des enjeux distincts au Canada. Le renforcement du droit à la vie privée des personnes est un levier essentiel, qui permet d'aborder les questions centrales entourant l'expression démocratique, notamment la transparence et la responsabilité de quoi et à l'égard de qui. Par conséquent, le Commissariat estime que la protection de la vie privée est essentielle et fondamentalement liée à la protection et à la promotion de l'expression démocratique au Canada.

Précédents

Dans l'Union européenne, le règlement général sur la protection des données a fait date. Il impose des obligations plus strictes aux organisations qui ciblent ou collectent des données relatives aux personnes dans l'UE, en limitant les données qui peuvent être collectées, la façon dont elles peuvent être utilisées et les circonstances dans lesquelles elles le sont[73].

De même, la *Loi californienne sur la protection de la vie privée des consommateurs* a renforcé le droit des individus à connaître les renseignements collectés à leur sujet, à supprimer ces renseignements, à refuser la vente de leurs données personnelles et le droit à la non-discrimination pour l'exercice de ces droits[74].

Ces deux législations ont guidé des réformes dans d'autres États américains, comme la Virginie et le Colorado, et dans le monde entier, comme au Brésil, au Japon, en Uruguay, au Nigeria, en Afrique du Sud et en Corée du Sud. Toutes ces réformes reflètent la plupart des obligations présentes dans le RGPD relativement à la façon dont les organisations peuvent collecter et traiter les données.

CONCLUSION

Nous ne prétendons pas savoir ce qui pourrait se dégager au cours des prochaines années. L'innovation technologique est rapide et les formes de technologie évoluent rapidement. Mais nous croyons que les droits fondamentaux, les principes et les valeurs qui constituent depuis longtemps la base de la société canadienne demeurent aussi pertinents aujourd'hui et à l'avenir qu'ils l'ont été dans le passé.

Notre objectif est de défendre l'intérêt public à une époque où les géants du numérique dominent non seulement la distribution de l'information, mais également le débat public qui l'entoure. Nous espérons que la mise en œuvre de nos recommandations commencera à rétablir le sentiment de confiance et de sécurité que les individus, les groupes et les collectivités doivent avoir pour participer pleinement et équitablement à notre démocratie. Sans cela, notre démocratie est en péril.

Pour éviter que cela ne se produise, nous avons tous/toutes le devoir d'agir de façon responsable dans toutes nos communications, et cela s'applique également aux utilisateurs.trices et aux plateformes de médias sociaux. Les un.e.s et les autres doivent toujours agir avec prudence, en veillant à ce que tout ce qui est publié, partagé et diffusé aille au-delà de la norme minimale pour ne pas être illégal. En tant que membre du Commissariat, nous avons consulté des expert.e.s, effectué des recherches et débattu au cours de 15 sessions d'étude et de délibération, en ligne et en personne, afin de parvenir aux conclusions et recommandations contenues dans le présent rapport, qui permettront aux organismes publics d'exercer une surveillance qui, selon nous, préservera au mieux les droits du public et les libertés d'expression démocratique.

ANNEXES

ANNEXE UN

LA LIBERTE D'EXPRESSION DANS LE CONTEXTE CANADIEN

Comme nous l'avons indiqué dans notre rapport, une grande partie du débat sur l'expression démocratique et les plateformes a porté sur les risques des possibles contraintes sur la liberté d'expression et la liberté de parole. À cet égard, le Canada est également différent des États-Unis et ces différences doivent être comprises.

Pour cette raison, nous croyons qu'il vaut la peine de fournir beaucoup de détails dans ce rapport pour expliquer le contexte dans lequel la liberté d'expression a été appliquée et interprétée par les tribunaux canadiens.

Aux États-Unis, les contraintes proposées en matière de liberté d'expression se transforment rapidement en débats sur l'étendue de la protection offerte par le premier amendement de la constitution.

LE DEBAT SUR LA LIBERTE D'EXPRESSION

La très honorable Beverley McLachlin PC, CC

La liberté d'expression bénéficie également d'une protection constitutionnelle au Canada, mais cette protection n'est pas absolue. L'alinéa 2b) de la Charte des droits et libertés prévoit ce qui suit :

2. Chacun a les libertés fondamentales suivantes :

b. liberté de pensée, de croyance, d'opinion et d'expression, y compris la liberté de la presse et des autres moyens de communication.

Objet

La protection de la liberté d'expression repose sur des principes et des valeurs fondamentaux – la valeur de la recherche et de la quête de la vérité, la participation à la prise de décision sociale et politique et la possibilité pour l'individu de s'épanouir par l'expression : *Irwin Toy Ltd. c. Québec (Procureur général)*, [1989] 1 RCS 927 et 976.

Interprétation

Les tribunaux ont interprété l'alinéa 2(b) au sens large pour qu'il s'applique à tout ce dont le contenu expressif n'est pas supprimé par la méthode ou le lieu de l'expression – c'est-à-dire l'expression qui prend la forme de violence ou de menaces de violence : *Société Radio-Canada c. Canada (Procureur général),* 2011 CSC 2.

Il n'y a pas de protection contre la violence physique, ni contre les menaces de violence : *Irwin Toy, précité; Suresh c. Canada (Ministre de la Citoyenneté et de l'Immigration),* [2002] 1 RCS 3) aux paragraphes107 et 108. À d'autres égards, la forme ou le moyen utilisé pour transmettre un message est généralement considéré faire partie du message et être visé par l'alinéa 2b) : *Weisfeld* (F.C.A.). Autrement, les discours préjudiciables sont protégés – les discours haineux, la pédopornographie et la désinformation bénéficient de la protection de l'alinéa 2(b).

La référence dans la garantie aux « autres moyens d'expression » indique clairement qu'elle s'applique à Internet. Les messages en ligne de tous types (à l'exception peut-être des menaces de violence) sont présumés protégés par la garantie constitutionnelle de la liberté d'expression. Le contenu de l'expression ne supprime pas la protection conférée par l'alinéa 2(b); il couvre même l'expression odieuse et haineuse.

Article 1 de la Charte

Nonobstant la vaste portée de la garantie de la liberté d'expression, l'État peut imposer des limites à la liberté d'expression en vertu de l'article 1 de la Charte, qui prévoit que les droits qui y sont énoncés sont garantis et qu'« ils ne peuvent être restreints que par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique ».

L'article 1 reconnaît que les droits garantis par la Charte, notamment le droit à la liberté d'expression, ne sont pas absolus. Dans une société civilisée, les droits, notamment le droit à la liberté d'expression, doivent parfois être limités pour éviter de nuire à autrui. La plupart des garanties modernes des droits suivent ce modèle et reconnaissent expressément que la liberté d'expression peut être limitée compte tenu de valeurs et de préoccupations contradictoires. (En revanche, la Déclaration des droits des États-Unis est rédigée en termes absolus – « nul ne peut » restreindre la liberté d'expression. Toutefois, même les tribunaux

américains ont confirmé les limites de la liberté d'expression pour prévenir les préjudices. Personne, pour citer le juge Oliver Wendell Holmes, n'a le droit de crier au feu dans un théâtre bondé).

L'article 1 permet de mettre en balance la liberté d'expression et d'autres droits protégés par la Charte, comme la vie, la liberté et l'égalité (protection contre la discrimination). Pour justifier une limite, le gouvernement doit démontrer un objectif urgent. Il doit également démontrer que la limite n'est pas plus large que nécessaire. À l'étape finale de l'analyse de l'article 1 *(Oakes)*, le gouvernement doit démontrer que l'incidence de la mesure est proportionnelle; la question est de savoir si les avantages de la mesure qui limite la liberté d'expression sont proportionnels au préjudice qui serait causé en permettant l'expression sans restriction.

Grâce à l'application de ces critères, la Charte permet au gouvernement d'imposer des limites « raisonnables » à l'expression. Le discours haineux, l'obscénité, la pornographie et la diffamation sont des catégories courantes de restriction en matière de liberté d'expression au Canada. D'autre part, une interdiction vague et trop large de la diffusion de « fausses nouvelles » (désinformation) a été annulée par la Cour suprême dans l'affaire *R. v. Zundel.*

L'affaire Zundel montre que les tribunaux connaissent parfaitement l'effet paralysant que la restriction de la parole peut avoir sur la liberté d'expression. Les lois restreignant l'expression doivent être claires, concises et ciblées afin de justifier la restriction de la liberté d'expression. Les gens doivent savoir avec un certain degré de précision ce qu'ils peuvent dire et ce qu'ils ne peuvent pas dire.

Qui a le droit de limiter la liberté d'expression et comment cela peut-il être fait?

En vertu de l'article 1 de la Charte, toute limite à la liberté d'expression doit être imposée par la loi, c'est-à-dire par un texte législatif du Parlement ou des assemblées législatives provinciales.

Ces lois prennent deux formes. Premièrement, le Parlement peut criminaliser certains types de discours, comme il l'a fait pour les discours haineux, la pornographie, le complot et le terrorisme. Ces dispositions s'appliquent évidemment aux communications numériques et aux médias sociaux. Toutefois, elles peuvent s'avérer peu efficaces, car leur application nécessite des poursuites pénales et entraîne tous les délais inhérents aux procès pénaux.

La seconde approche consiste pour le Parlement et les assemblées législatives à mettre en place des systèmes de réglementation, comme ceux qui prévoient des commissions des droits de la personne, qui : (a) restreignent certains types de discours; et (b) délèguent l'application de la loi à des conseils composés de membres nommés. Des systèmes similaires pourraient être imposés en ce qui concerne les discours sur les médias sociaux et autres communications par Internet. Cependant, l'application de cette approche a

également été difficile. Les commissions ont été très critiquées pour leurs retards et la lourdeur de leurs procédures et, par certains, pour avoir interféré de façon inappropriée avec la liberté d'expression.

Une troisième approche pourrait consister à nommer un organisme de réglementation et à lui déléguer un rôle important dans la définition des cas où la parole numérique doit être limitée, ainsi que dans l'administration du système. Cette approche pourrait être contestée comme étant inconstitutionnelle, selon la façon dont elle est structurée et mise en place.

La seule « loi » que l'organisme de réglementation pourrait adopter serait des mesures législatives subordonnées, ou des règlements. En général, le pouvoir d'adopter des règlements doit être étroitement lié à la loi adoptée par le Parlement.

Le Parlement ne peut pas simplement déléguer son pouvoir à des fonctionnaires non élus en leur laissant le soin de décider ce qui est autorisé et ce qui est interdit. En d'autres termes, toute restriction de la liberté d'expression doit être formulée par le Parlement avec une précision considérable dans la loi qu'il adopte; il ne peut pas se contenter de transmettre cette tâche à quelqu'un d'autre. Les assemblées législatives provinciales ne peuvent pas non plus le faire. Le faire serait inconstitutionnel.

Cette restriction légale de la portée du règlement reflète la préoccupation très normale que l'on entend souvent au sujet de telles propositions : il est erroné d'armer un fonctionnaire non élu de larges pouvoirs pour restreindre la liberté d'expression. Si quelqu'un doit restreindre ce droit fondamental, ce devrait être les représentants élus du peuple.

Une autre difficulté réside dans le fait que toute loi adoptée par le Parlement devrait tenir compte des pouvoirs provinciaux en matière, par exemple, de propriété, de droits civils et d'administration de la justice. Ces préoccupations, ainsi que la délégation excessive de pouvoirs à un organisme de réglementation, ont conduit la Cour suprême du Canada à annuler une grande partie du régime canadien des droits de reproduction il y a quelques années.

Alors, qui peut imposer des restrictions au discours sur Internet?

La réponse est le Parlement ou les assemblées législatives. Ils doivent définir ce qui est admis et ce qui ne l'est pas. Et qui fait appliquer les lois du Parlement? Il pourrait bien s'agir d'une sorte de commission ou d'organisme de réglementation. Mais les pouvoirs de cet organisme devraient être étroitement liés à la loi adoptée par le Parlement, et il faudrait trouver des moyens d'éviter les problèmes qui ont touché les commissions des droits de la personne.

Alors, quelle est la meilleure façon de procéder dans le contexte canadien?

Nous préférons commencer modestement et développer le régime au fil des ans. Si le Parlement tente d'en faire trop et trop vite, tout le régime risque d'imploser dans une agonie de contestations judiciaires.

Un point de départ pourrait être les restrictions sur les infractions relatives aux discours déjà établis par le Parlement, notamment les discours haineux, la pornographie, les discours terroristes, etc. Le Parlement pourrait adopter un régime permettant de faire respecter ces interdictions dans le contexte d'Internet, avec un organisme réglementé habilité à surveiller et à prendre les mesures d'application appropriées, comme des ordres de fermeture. L'organisme aurait également le pouvoir d'imposer des amendes et autres sanctions après une audition sur le fond. L'organisme aurait également le pouvoir de recevoir des plaintes, qui pourraient faire l'objet d'une médiation et, si la médiation échoue, d'un jugement. Pour éviter les problèmes de retard que nous avons rencontrés avec les tribunaux des droits de la personne, nous nous tournerions vers un nouveau tribunal simplifié, calqué sur le modèle du Civil Resolution Tribunal (CRT) de la Colombie-Britannique, qui fonctionne bien.

Ce cadre pourrait être accompagné d'un conseil de citoyen.ne.s et d'expert.e.s chargé de surveiller et de conseiller la commission et le Parlement sur les changements à apporter.

Le fait de commencer par des catégories de discours restreints, qui ont été approuvés par les tribunaux, éliminera les contestations judiciaires fondées sur le contenu du discours. Si le système d'accompagnement relatif à l'application et au contrôle est bien conçu, il contribuera à limiter les abus. Il aurait également le mérite de fournir des orientations claires aux plateformes et aux utilisateurs.trices.

Conclusion

La réponse à la réglementation d'Internet n'est ni facile ni évidente, étant donné les contraintes constitutionnelles qui découlent de la garantie de la liberté d'expression dans la Charte, les restrictions constitutionnelles sur la délégation de pouvoirs aux organismes de réglementation et la division des pouvoirs entre les gouvernements fédéral et provinciaux.

Les discours préjudiciables peuvent être restreints au Canada – la loi le dit clairement. La question la plus importante est de savoir comment mener cela avec succès.

ANNEXE DEUX

POURQUOI METTONS-NOUS L'ACCENT SUR LES SYSTEMES FERMES

Les boîtes fermées ont été au centre des discussions universitaires, politiques et industrielles sur les systèmes décisionnels et les algorithmes propriétaires opaques dans le monde entier. La technologie avancée fondée sur l'apprentissage machine a apporté de nombreux gains d'efficacité sociétale, de l'économie à la santé, des tendances comportementales aux découvertes scientifiques. Toutefois, elle a également eu une incidence négative sur les processus démocratiques et les droits de la personne de façon plus générale[75]. L'opacité qui caractérise certaines applications d'apprentissage machine (AM) a été fortement critiquée, accusée et jugée coupable d'accroître et de perpétuer les inégalités et les processus décisionnels partiaux[76]. Aujourd'hui, les chercheurs.euses et les décideurs.euses politiques tentent d'éviter les incidences néfastes des applications d'apprentissage automatique en mettant l'accent sur des moyens alternatifs de vérifier les algorithmes qui régissent certaines des décisions sociétales les plus fondamentales, telles que l'accès au financement, à l'éducation, à l'emploi et même au maintien de l'ordre[77]. Pour ce faire, il est essentiel de comprendre ce qui rend l'apprentissage machine (AM) et la boîte fermée si complexes à expliquer.

Les modèles d'AM sont le résultat d'un processus de formation instruit par les programmeurs sur la base d'un ensemble de données spécifique. Il y a plusieurs façons dont un modèle peut produire des décisions injustes et fondées sur des préjugés. Bien que la discussion des aspects techniques n'entre pas dans le cadre du présent rapport, il est important de noter que les décisions fondées sur les AM risquent de refléter les préjugés et les préjudices humains, que ce soit consciemment ou inconsciemment[78]. Pour compliquer davantage les choses, recevoir une explication du modèle qui a été utilisé par l'algorithme pour parvenir à une certaine décision (c'est-à-dire la logique de la boîte fermée) est particulièrement difficile. En effet, les applications d'AM les plus avancées, telles que l'apprentissage profond et les réseaux neuronaux artificiels, utilisent des mégadonnées pour dégager des tendances et prendre des décisions de sorte à ne pas suivre nécessairement les logiques intuitives humaines[79]. Ce faisant, les boîtes fermées risquent d'utiliser les données personnelles de façon abusive. Il faut également mentionner que les protections du secret commercial empêchent encore plus les entreprises de rendre leurs algorithmes plus transparents dans la mesure du possible[80].

À la lumière de cette complexité, le phénomène a été comparé à une boîte fermée, dont « nous pouvons observer les entrées et les sorties, mais nous ne pouvons pas dire comment l'une devient l'autre[81] ». La boîte fermée génère de façon opaque de nouvelles connaissances sur les individus et la société[82]. Toutefois, l'opacité dans laquelle ces connaissances sont obtenues pose problème sous divers angles, notamment l'éthique, les principes de responsabilité[83], la finance[84], la santé[85], la responsabilité industrielle[86] et la recherche scientifique[87].

En outre, la boîte fermée est particulièrement pertinente lorsqu'il s'agit de traiter les préjudices en ligne. Les applications d'apprentissage profond sont, de nos jours, largement utilisées sur les plateformes de médias sociaux et les moteurs de recherche pour analyser le comportement des utilisateurs.trices et proposer des services et des recommandations ciblés ad hoc. Des événements récents[88] ont montré l'incidence des plateformes de médias sociaux sur les sociétés démocratiques du monde entier, par la propagation de fausses informations, l'augmentation de la polarisation et de la radicalisation, et la toxicité permise par les environnements en ligne anonymes. Les systèmes de recommandation ont prouvé qu'ils avaient de graves répercussions sur la quantité et la qualité des renseignements auxquels les individus ont accès, façonnant ainsi leurs opinions et leurs décisions interpersonnelles[89]. Lorsque les algorithmes qui régissent ces systèmes ne peuvent être expliqués, la liberté d'expression, l'accès à l'information, la politique et l'État de droit sont mis à mal.

Actuellement, l'approche la plus prometteuse pour ouvrir la boîte fermée est celle des « explications contre-factuelles ». Celles-ci expliquent comment une décision a été prise en indiquant quelles caractéristiques des données d'entrée devraient être modifiées pour parvenir à une décision différente, indiquant ainsi quelles caractéristiques l'ont influencée[90]. Bien que les explications contre-factuelles ne nécessitent pas une compréhension du processus interne des algorithmes et qu'elles permettent de traiter les enjeux de la divulgation excessive de renseignements susceptibles d'enfreindre le droit à la propriété intellectuelle et le droit à la vie privée, les explications contre-factuelles présentent toujours une limite majeure. Elles fournissent toutes les modifications éventuelles qui conduiraient à un résultat différent. Ainsi, la personne concernée n'a toujours aucun moyen de savoir exactement quel paramètre a été décisif et si ce paramètre était biaisé. Il est donc important de consacrer les ressources nécessaires à une étude plus approfondie de la boîte fermée et d'utiliser ces connaissances pour renforcer les démocraties plutôt que de les affaiblir.

ANNEXE TROIS

BIOGRAPHIES DES COMMISSAIRES

Rick Anderson

Directeur, Earnscliffe Strategy Group

Rick Anderson met à la disposition d'Earnscliffe des dizaines d'années d'expérience de haut niveau en matière de gestion et d'administration, en mettant l'accent sur la fourniture de conseils stratégiques et de conseils sur la stratégie d'entreprise et la gestion des enjeux publics.

M. Rick travaille avec des cadres supérieurs dans les organisations les plus grandes et les plus prospères du monde, tout en aidant les entrepreneurs.euses en démarrage et à fort potentiel de croissance. Fort d'une vaste expérience de travail avec les dirigeant.e.s de la C-Suite, M. Rick connaît bien les politiques publiques, la gouvernance, les affaires politiques et réglementaires, les fusions et acquisitions, les communications et le marketing.

Avant de se joindre à Earnscliffe, M. Rick a travaillé pendant 15 ans au Canada, aux États-Unis et au Royaume-Uni pour une importante société de communications stratégiques et a dirigé son propre cabinet de consultation professionnelle. Il partage actuellement son temps entre Vancouver et Ottawa, travaillant dans les bureaux d'Earnscliffe des deux villes.

Très actif au niveau de la politique et des affaires publiques tout au long de sa vie, il a occupé des postes de conseiller principal auprès de premiers ministres, de chefs de partis et de candidats à la direction de partis. Il est régulièrement invité à commenter les affaires politiques par les principaux organismes de presse du Canada.

Wendy Chun

Chaire de recherche Canada 150 en nouveaux médias, Université Simon Fraser

M^{me} Hui Kyong Chun est titulaire de la Chaire de recherche Canada 150 en nouveaux médias de l'Université Simon Fraser et dirige le Digital Democracies Institute. Elle est l'auteure de plusieurs travaux, dont *Discriminating Data* (à paraître chez MIT 2021) et de trois livres chez MIT : *Updating to Remain the Same : Habitual New Media*; *Programmed Visions : Software and Memory* et *Control and Freedom : Power and Paranoia in the Age of Fiber Optics*.

M^me^ Hui Kyong Chun est professeure et présidente du Département de la culture moderne et des médias à l'Université Brown où elle y travaille depuis près de vingt ans. Elle a été plusieurs fois titulaire de chaire invitée et boursière de recherche dans des établissements, dont Harvard, Annenberg School à l'université de Pennsylvanie, le Institute for Advanced Study (Princeton), le Guggenheim, ACLS et le American Academy of Berlin.

Nathalie Des Rosiers

Directrice, Massey College, professeure titulaire, Faculté de droit (Common Law) à l'Université d'Ottawa, visiteuse de marque, Faculté de droit à l'Université de Toronto

M^me^ Des Rosiers est directrice de Massey College. Elle fut députée de 2016 à 2019 pour représenter la circonscription d'Ottawa-Vanier. Elle fut ministre des Richesses naturelles et Forêts de janvier à juin 2018. Avant d'entrer en politique, elle fut doyenne de la Section de common law de la faculté de droit à l'Université d'Ottawa (2013 à 2016), avocate générale à l'Association canadienne des libertés civiles (2009 à 2013), vice-présidente de la gouvernance à l'Université d'Ottawa (2008 à 2009), doyenne de la Section du droit civil de la faculté de droit (2004 à 2008) et présidente de la Commission du droit du Canada (2000 à 2004).

Avec Peter Oliver et Patrick Macklem, elle a coédité *The Oxford Handbook of Canadian Constitutional Law* (2017). Elle a également rédigé avec Louise Langevin et Marie-Pier Nadeau, *L'indemnisation des victimes de violence sexuelle et conjugale* (Prix Walter Owen, 2014). Elle a été nommée à l'Ordre du Canada et à l'Ordre de l'Ontario. Elle a reçu des doctorats honorifiques de l'Université UCL (Belgique) et du Barreau de l'Ontario, le Prix Christine Tourigny (Barreau du Québec) et est membre de la Société royale du Canada.

Amira Elghawaby

Directrice des programmes et de la sensibilisation, Fondation canadienne des relations raciales

Mme Elghawaby est journaliste et défenseuse des droits de la personne.

Elle occupe actuellement le poste de directrice des programmes et de la sensibilisation à la Fondation canadienne des relations raciales.

Auparavant, Mme Elghawaby a travaillé au sein du mouvement syndical du Canada et s'est aussi consacrée pendant cinq ans à la promotion des libertés civiles des musulmans canadiens au Conseil national des musulmans canadiens de 2012 à 2017. Elle a soutenu plusieurs initiatives nationales visant à contrer la haine

et promouvoir l'inclusion, notamment à titre de membre fondatrice du comité du Canadian Anti-Hate Network et d'ancienne membre du conseil du Silk Road Institute.

Mme Elghawaby a obtenu un baccalauréat spécialisé en journalisme et en droit de l'Université Carleton en 2001.

Merelda Fiddler-Potter

Boursière Vanier, candidate au doctorat, et cadre en résidence, Johnson Shoyama Graduate School of Public Policy

Mme Fiddler-Potter est actuellement candidate au doctorat au Johnson Shoyama Graduate School of Public Policy à Regina. Elle a reçu une bourse d'études supérieures du Canada Vanier en 2019. Sa recherche explore le rôle des médias pour aider les Canadiens à s'instruire sur la vérité de nos politiques coloniales et leur impact sur les peuples autochtones, et sur les moyens dont les médias peuvent maintenir les questions autochtones en tête des priorités publiques.

Mme Fiddler-Potter fut aussi anciennement journaliste et documentariste, et a travaillé au sein de la Société Radio-Canada (CBC) pendant 16 ans à la radio, à la télévision et en ligne. Elle a lancé sa propre entreprise de films documentaires, produisant de nombreux films pour les diffuseurs.euses canadiens nationaux. Mme Fiddler-Potter possède une maîtrise ès arts en études des Plaines canadiennes et un baccalauréat en journalisme et communications de l'Université de Regina.

En plus de poursuivre des études au doctorat, Mme Fiddler-Potter est chargée de cours à temps partiel à l'Université des Premières Nations du Canada, où elle enseigne les études autochtones, les arts de la communication autochtone, les affaires autochtones, de même que le certificat en réconciliation. Elle fut également titulaire de la Chaire Dallas W. Smythe à l'École de journalisme de l'Université de Regina de 2017 à 2018.

En sa qualité de femme métisse engagée à créer une place pour les peuples autochtones dans tous les établissements, Mme Fiddler-Potter collabore avec des organisations pour s'instruire sur la réconciliation autochtone et la manière de l'utiliser efficacement dans les lieux de travail.

Philip Howard

Directeur du programme sur la démocratie et la technologie et professeur d'études sur Internet, Balliol College, Université d'Oxford.

À titre de directeur du programme sur la démocratie et la technologie à l'Université d'Oxford, M. Howard supervise une grande équipe de recherche qui travaille à l'utilisation de nouvelles technologies de l'information en politique, dans le but de favoriser l'engagement civique et d'améliorer la vie publique partout dans le monde. En plus de son poste de directeur, M. Howard est professeur et associé au Balliol College.

M. Howard, un érudit des communications politiques et une référence en matière de médias mondiaux, s'est longtemps consacré à l'étude des élections, des conflits et des affaires internationales. Il a travaillé sur le terrain dans 16 pays – dans des démocraties et des régimes autoritaires – et a même travaillé à titre d'observateur électoral.

Les recherches révolutionnaires de M. Howard et de son équipe ont changé le discours mondial sur le rôle des médias sociaux dans la vie publique. Depuis 2014, il mène des études sur la mésinformation dans le monde, par l'entremise de l'écriture publique et de conférences, et a conseillé des gouvernements, des industries de technologie et des groupes clés de la société civile dans le monde sur les meilleures interventions face aux interférences électorales, les fausses nouvelles et la mésinformation.

Au niveau universitaire, M. Howard a donné des cours sur les communications politiques, la mondialisation, les systèmes médiatiques comparatifs, les relations internationales et les méthodes de recherche en sciences sociales. Il a publié dix livres et édité des ouvrages et fut l'auteur de plus de 130 articles universitaires, chapitres de livres et documents de travail. Il a reçu de nombreux prix du meilleur livre de plusieurs organisations professionnelles de la sphère des sciences sociales.

Il a récemment été nommé « Global Thinker » du magazine *Foreign Policy*, et le National Democratic Institute lui a remis le « Democracy Prize » en reconnaissance de son travail pionnier dans les sciences sociales et les fausses nouvelles.

Vivek Krishnamurthy

Professeur de droit de la bourse Samuelson-Glushko à l'Université d'Ottawa

M. Krishnamurthy est professeur de droit de la bourse Samuelson-Glushko à l'Université d'Ottawa et directeur de la CIPPIC, la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko.

L'enseignement, la mission professorale et la pratique juridique clinique de M. Krishnamurthy mettent l'accent sur les défis complexes liés à la réglementation et aux droits de la personne qui surviennent dans le cyberespace. Il conseille les gouvernements, les militants et les entreprises sur les répercussions des nouvelles technologies sur les droits de la personne et commente fréquemment les questions des technologies émergentes et des politiques publiques sur la scène publique.

M. Krishnamurthy fut précédemment directeur adjoint à la Harvard Law School's Cyberlaw Clinic et conseiller juridique pour la responsabilité sociale d'entreprise à la firme Foley Hoag s.r.l. Il est boursier Rhodes et a travaillé pour l'honorable Morris J. Fish de la Cour suprême du Canada jusqu'à l'obtention de son diplôme de la Yale Law School. M. Krishnamurthy est actuellement associé au Centre Carr pour la politique des droits de la personne au Harvard Kennedey School, membre du corps enseignant au Berkman Klein Center for Internet & Society à l'Université de Harvard et associé principal de l'Initiative des droits de la personne au Center for Strategic and International Studies à Washington, D.C.

La très honorable Beverley McLachlin, C.P., C.C.

Mme McLachlin a exercé les fonctions de juge à la Cour suprême du Canada de 1989 à 2000 et de juge en chef de la Cour de 2000 à 2017.

Elle possède une formation postsecondaire de l'Université de l'Alberta : un baccalauréat ès arts (avec distinction) en 1965; une maîtrise ès arts en 1968 et un baccalauréat en droit en 1968. Elle a pratiqué le droit en Alberta et en Colombie-Britannique et enseigné le droit à l'Université de Colombie-Britannique avant d'accéder à la magistrature en Colombie-Britannique où elle a occupé le poste de juge de première instance et d'appel avant d'être nommée à la Cour suprême du Canada.

Depuis sa retraite de la Cour suprême du Canada, Mme McLachlin poursuit ses intérêts dans la résolution des litiges à titre d'arbitre et de médiatrice, en tant que membre de la Cour d'appel de Hong Kong, de la Cour commerciale internationale de Singapour et du Centre international d'arbitrage de Hong Kong. Elle continue de travailler pour l'accès à la justice et elle rédige et donne des allocutions sur des questions juridiques et autres sujets au Canada et à l'étranger.

Mme McLachlin est Compagnonne de l'Ordre du Canada et lauréate de nombreux prix et distinctions.

Taylor Owen

Titulaire de la Chaire Beaverbrook en médias, éthique et communications, et professeur agrégé à l'École de politiques publiques Max Bell de l'Université McGill

M. Owen est titulaire de la Chaire Beaverbrook en éthique, médias et communications, directeur fondateur du Centre pour les médias, la technologie et la démocratie et professeur agrégé à l'École de politiques publiques Max Bell de l'Université McGill. Il anime l'émission en baladodiffusion *Big Tech*, et est agrégé supérieur au Center for International Governance Innovation, associé du Forum des politiques publiques et membre du conseil d'administration du Conseil de recherches en sciences humaines (CRSH). Il a précédemment occupé les postes de professeur adjoint en médias numériques et en affaires mondiales à l'Université de Colombie-Britannique et de directeur de la recherche au Tow Center for Digital Journalism de la Columbia School of Journalism. Titulaire d'un doctorat de l'Université d'Oxford, il a reçu la bourse de la Fondation Pierre Elliott Trudeau et la bourse postdoctorale Banting, et a été nommé membre d'Action Canada et a reçu le prix des leaders émergents 2016 du Forum des politiques publiques.

Il est l'auteur du livre *Disruptive Power: The Crisis of the State in the Digital Age* (Oxford University Press, 2015) et il a coédité les ouvrages *The World Won't Wait: Why Canada Needs to Rethink its Foreign Policies* (University of Toronto Press, 2015) et *Journalism After Snowden: The Future of the Free Press in the Surveillance State* (Columbia University Press, 2016). Son prochain livre avec Emily Bell sera publié par Yale University Press en 2021. Son travail se concentre sur l'intersection des médias, de la technologie et des politiques publiques, lequel peut être consulté à http://taylorowen.com/ et @taylor_owen.

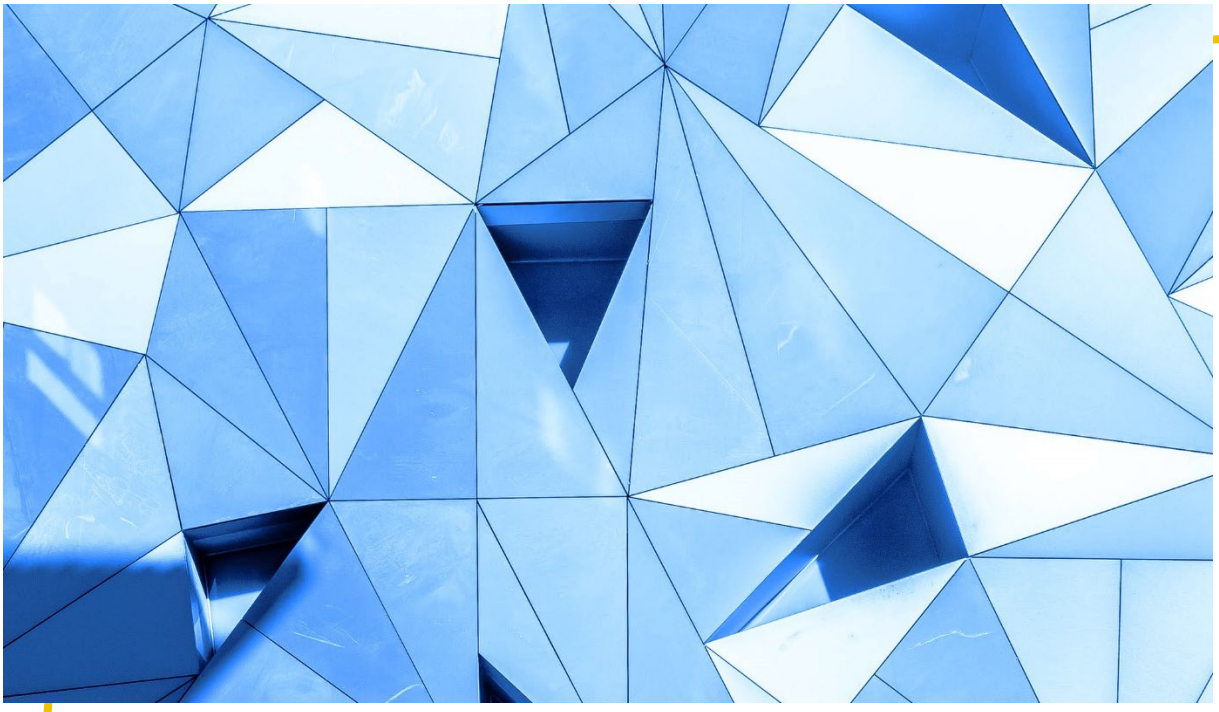
ANNEXE QUATRE

CALENDRIER DES CONVOCATIONS DE LA COMMISSION

Date	Activité
28 septembre 2021	**Séance d'orientation**
7 octobre 2021	**Session d'études** Inclut le témoignage de : **J. Nathan Matias**, professeur adjoint, département de la communication de l'Université Cornell et fondateur du Citizens and Technology Lab **Rebekah Tromble**, directrice de l'Institute for Data, Democracy, and Politics, professeure agrégée School of Media, and Public Affairs à l'Université George Washington
14 octobre 2021	**Session d'études** Inclut le témoignage de : **Catherine Armitage**, conseillère à l'agence AWO **Laura Edelson**, doctorante, NYU Tandon School of Engineering **Ethan Zuckerman**, professeur agrégé de politique publique, de communication et d'information à l'Université du Massachusetts à Amherst et fondateur de l'Institute for Digital Public Infrastructure
28 octobre 2021	**Session d'études** Inclut le témoignage de : **Seeta Peña Gangadharan**, professeure agrégée au département des médias et des communications de la London School of Economics (LSE) **Laura Murphy**, dirigeante des libertés civiles et des droits civils, stratège en politique
4 novembre 2021	**Session d'études** Inclut le témoignage de : **Kate Klonick**, professeure adjointe de droit, École de droit de l'Université St. John's et fellow affilié, Information Society Project, Yale Law School **Ravi Naik**, directeur juridique, agence AWO

	Emily Laidlaw, professeure agrégée, faculté de droit et Chaire de recherche du Canada – droit de la cybersécurité, Université de Calgary
18 novembre 2021	**Session d'études** Inclut le témoignage de : **Divij Joshi**, chercheur doctorant, University College London **Andrew Strait**, directeur associé, Ada Lovelace Institute **Jennifer Wémigwans**, Anishnaabekwe (Ojibwe/Potawatomi) de la Première Nation de Wikwemikong et professeure adjointe, OISE Université de Toronto
21 novembre 2021	Sessions d'études et séances délibérantes Inclut le témoignage de : L'Assemblée citoyenne sur l'expression démocratique 2021 **Meetali Jain**, directrice adjointe, Reset **Marietje Schaake**, directrice de la politique internationale, Cyber Policy Center de l'Université de Stanford et fellow en politique internationale, Institute for Human-Centered Artificial Intelligence de Standford **Mark Scott**, correspondant en chef pour la technologie, POLITHO
22 novembre 2021	**Sessions d'études et séances délibérantes** Inclut le témoignage de : **Evan Balgord**, directeur exécutif, Canadian Anti-Hate Network **Cory Doctorow**, journaliste, écrivain, militant des droits numériques **Willie Ermine**, professeur adjoint à l'Université des Premières Nations du Canada à Regina et à la Première Nation de Sturgeon Lake, située dans le centre-nord de la Saskatchewan **Sue Gardner**, fondatrice et PDG de Tiny Ventures **Michael Geist**, professeur de droit, Université d'Ottawa **Mohammed Hashim**, directeur exécutif, Fondation canadienne des relations raciales **Cynthia Khoo**, avocate et chercheuse en technologie et droits de la personne **Brenda McPhail**, directrice, Programme de protection de la vie privée, de technologie et de surveillance, Association canadienne des libertés civiles
5 janvier 2022	**Sessions d'études et séances délibérantes** Inclut le témoignage de : **Matthew Boswell**, Commissaire de la concurrence, Bureau de la concurrence du Canada

6 janvier 2022	**Sessions d'études et séances délibérantes** Inclut le témoignage de : **Kevin Chan**, directeur mondial principal et chef de la politique publique du Canada, Facebook **Rachel Curran**, gestionnaire des politiques publiques Canada, Facebook **Colin McKay**, chef, Affaires gouvernementales et politique publique du Canada, Google
27 janvier 2022	**Session d'études** Inclut le témoignage de : **Stéphane Perrault**, directeur général des élections du Canada **Daniel Therrien**, Commissaire à la protection de la vie privée du Canada
2 février 2022	**Séance délibérante**
9 février 2022	**Séance délibérante**
16 février 2022	**Séance délibérante**
23 février 2022	**Séance délibérante**



ANNEXE CINQ

DOCUMENTS À L'APPUI

La Commission remercie les personnes ci-dessous d'avoir préparé des documents écrits pour éclairer son étude et ses délibérations.

Catherine Armitage, conseillère à l'agence AWO

Laura Edelson, doctorante, NYU Tandon School of Engineering

Divij Joshi, chercheur doctorant, University College London

Kate Klonick, professeure adjointe de droit, École de droit de l'Université St. John's et fellow affilié, Information Society Project, Yale Law School

Emily Laidlaw, professeure agrégée, faculté de droit et Chaire de recherche du Canada – droit de la cybersécurité, Université de Calgary

J. Nathan Matias, professeur adjoint, département de la communication de l'Université Cornell et fondateur du Citizens and Technology Lab

Laura Murphy, dirigeante des libertés civiles et des droits civils, stratège en politique

Ravi Naik, directeur juridique, agence AWO

Seeta Peña Gangadharan, professeure agrégée au département des médias et des communications de la London School of Economics (LSE)

Andrew Strait, directeur associé, Ada Lovelace Institute

Rebekah Tromble, directrice de l'Institute for Data, Democracy, and Politics, professeure agrégée School of Media, and Public Affairs à l'Université George Washington

Jennifer Wémigwans, professeure adjointe, OISE Université de Toronto

Ethan Zuckerman, professeur agrégé de politique publique, de communication et d'information à l'Université du Massachusetts à Amherst et fondateur de l'Institute for Digital Public Infrastructure

Les communications sont disponibles à l'adresse https://ppforum.ca/fr/project/expression-democratique/

ANNEXE SIX

RECONNAISSANCE

Le Forum des politiques publiques tient à remercier les membres du secrétariat de la Commission pour leur travail acharné et leur dévouement en vue de soutenir les commissaires dans leurs délibérations.

Par ordre alphabétique:

Gareth Chappell, Chef de projet

Heba Elhalees, Coordinatrice d'événements

Peter MacLeod, Facilitateur principal

Adelina Petit-Vouriot, Rédaction et soutien du projet

Lisa Semchuk, Associée de projet et de recherche

Sonja Solomun, Chercheuse principale et analyste politique

Chris Waddell, Rédacteur principal

Sabrina Wilkinson, Chargée de recherche

Alessia Zornetta, Chercheuse

NOTES DE FIN DE TEXTE

[1] Pour des informations plus détaillées sur l'accès aux données pour les chercheurs.euses, y compris les compromis potentiels, voir Caitlin Vogus et Emma Llansó, « Making Transparency Meaningful » (Centre for Technology and Democracy, décembre 2021), https://cdt.org/wp-content/uploads/2021/12/12132021-CDT-Making-Transparency-Meaningful-A-Framework-for-Policymakers-final.pdf

[2] Par exemple, plus de 120 organisations de la société civile ont appelé l'Union européenne à adopter une loi sur l'intelligence artificielle (AIA) portant sur les droits fondamentaux. Voir « An EU Artificial Intelligence Act for Fundamental Rights » (30 novembre 2021), https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf et https://cdt.org/insights/eu-tech-policy-brief-january-2022-recap/

[3] Page 11. https://ppforum.ca/wp-content/uploads/2021/01/UnRapportDeLaCommissionCanadienneDeL%E2%80%99expressionD%C3%A9mocratique-FPP-JAN2021-FR.pdf

[4] https://ppforum.ca/project/demx/

[5] Voir Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *Rapport sur la désinformation,* HCDH, UN Doc A/HRC/47/35 (13 avril 2021), https://documents.un.org/prod/ods.nsf/home.xsp ; Privacy International, « The UN Report on Disinformation: A Role for Privacy », Privacy International, 17 mai 2021, http://privacyinternational.org/news-analysis/4515/un-report-disinformation-role-privacy

[6] Yuan Stevens et Sonja Solomun. Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act, *Cybersecure Policy Exchange*, février 2021. Voir aussi, Penney, Jonathon, Chilling Effects: Online Surveillance and Wikipedia Use (2016). Berkeley Technology Law Journal, vol. 31, nº 1, p. 117, 2016, disponible sur SSRN : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645 Miles Kenyon, « Jon Penney on the Chilling Effects of Online Surveillance », (11 juillet 2017), *Citizen Lab*: https://citizenlab.ca/2017/07/jon-penney-on-the-chilling-effects-of-online-surveillance/#:~:text=Jon%20Penney%2C%20research%20fellow%20at,be%20hesitant%20to%20share%20content

[7] Willie Ermine, « The Ethical Space of Engagement » (2007) vol 6, no 1, Indigenous Law Journal, p. 193-202.

[8] Assemblée citoyenne canadienne sur l'expression démocratique. (2022) « Assemblée citoyenne canadienne sur l'expression démocratique : Recommandations pour renforcer la capacité d'intervention du Canada en matière de diffusion de désinformation en ligne. » Ottawa, Forum des politiques publiques. p. 35

[9] Ibid p. 35

[10] « The Commission on Information Disorder Final Report », The Aspen Institute, novembre 2021. CC BY-NC. https://creativecommons.org/licenses/

[11] Ibid. p .8

[12] Commission européenne, « Train de mesures sur les services numériques | Bâtir l'avenir numérique de l'Europe », (4 mars 2022), en ligne : *digital-strategyeceuropaeu* https://digital-strategy.ec.europa.eu/fr/policies/digital-services-act-package

[13] Gouvernement du Canada, « Document technique », (29 juillet 2017), https://www.canada.ca/fr/patrimoine-canadien/campagnes/contenu-prejudiciable-en-ligne/document-travail-technique.html

[14] Voir Caitlin Vogus et Emma Llansó, « Making Transparency Meaningful » (Centre for Technology and Democracy, décembre 2021), https://cdt.org/wp-content/uploads/2021/12/12132021-CDT-Making-Transparency-Meaningful-A-Framework-for-Policymakers-final.pdf Une véritable transparence passe aussi souvent par des notifications aux utilisateurs.rices, ce qui n'entre pas dans le cadre de ce rapport

[15] Sonja Solomun, Maryna Polataiko, Helen A. Haye, « Platform Responsibility And Regulation In Canada: Considerations On Transparency, Legislative Clarity, And Design » (2021) 34 Harvard Journal of Law & Technology, https://jolt.law.harvard.edu/assets/digestImages/Solomun-Polataiko-Hayes.pdf

[16] Pour les limites des mécanismes de rapport de transparence existants, voir Chris Tenove et Heidi Tworek, *Processus, individus et responsabilité à l'égard du public : comprendre et aborder les communications haineuses en ligne*, Rapport de recherche – Commission canadienne sur l'expression démocratique (2020), https://ppforum.ca/wp-content/uploads/2020/12/ComprendreEtAborderLesCommunicationsHaineusesEnLigneE-DemX-Dec2020-FR.pdf, p. 16; Amélie Heldt, *Reading Between the Lines and the Numbers: An Analysis of the First NetzDG Reports*, 8 Internet Policy Review 2 (2019), https://policyreview.info/articles/analysis/reading-between-lines-and-numbers-analysis-first-netzdg-reports

[17] Composé des Instituts de recherche en santé du Canada (IRSC), du Conseil de recherches en sciences naturelles et en génie (CRSNG) et du Conseil de recherches en sciences humaines (CRSH)

[18] Nate Persily, « U.S. Proposed Platform Transparency and Accountability Act » (2021), en ligne (pdf): https://techpolicy.press/wp-content/uploads/2021/10/Persily-proposed-legislation-10-5-21.docx.pdf

[19] Pour des informations plus détaillées sur l'accès aux données pour les chercheurs.euses, y compris les compromis potentiels, voir Caitlin Vogus et Emma Llansó, « Making Transparency Meaningful » (Centre for Technology and Democracy, décembre 2021), https://cdt.org/wp-content/uploads/2021/12/12132021-CDT-Making-Transparency-Meaningful-A-Framework-for-Policymakers-final.pdf

[20] Commission européenne, « La Commission présente des orientations visant à renforcer le code de bonnes pratiques contre la désinformation » (2021), en ligne : Commission européenne https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_2585

[21] Union européenne, *Proposition de règlement du parlement européen et du conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE*, [2020], en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020PC0825&from=FR

[22] En raison des préoccupations relatives à la surveillance et à l'application régulière de la loi, la DSA peut aussi exclure les organismes d'application de la loi des régimes d'accès aux données

[23] États-Unis, *Proposed Platform Accountability and Transparency Act*, en ligne : https://www.coons.senate.gov/imo/media/doc/text_pata_117.pdf

[24] Union européenne, Proposition de directive du parlement européen et du conseil modifiant les directives 2013/34/UE, 2004/109/CE et 2006/43/CE ainsi que le règlement (UE) nº 537/2014 en ce qui concerne la publication d'informations en matière de durabilité par les entreprises, [2021], art. 19c, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52021PC0189&from=FR

[25] États-Unis, Code of Federal Regulations, 47 FR 11401, partie 229, version modifiée le 31 janvier 2022, https://www.ecfr.gov/current/title-17/chapter-II/part-229

[26] https://laws-lois.justice.gc.ca/fra/LoisAnnuelles/2018_31/page-1.html

[27] Assemblée citoyenne canadienne sur l'expression démocratique, « Assemblée citoyenne canadienne sur l'expression démocratique : Recommandations pour renforcer la capacité d'intervention du Canada en matière de diffusion de désinformation en ligne » (Forum des politiques publiques, Ottawa, 2022), https://ppforum.ca/wp-content/uploads/2022/01/DEMX-R2.pdf

[28] Jamie Linde, « The Importance of EHR Interoperability » (30 septembre 2020), en ligne : Wheel https://www.wheel.com/companies-blog/importance-of-ehr-interoperability#:~:text=Interoperability%20ensures%20that%20patient%20data,between%20referring%20doctors%20and%20specialists.

[29] Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh, Madeleine Clare Elish & Jacob Metcalf, « Assembling Accountability: Algorithmic Impact Assessment for the Public Interest » (Data & Society, 19 juin 2021), https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest

[30] Page 10. https://ppforum.ca/wp-content/uploads/2021/01/UnRapportDeLaCommissionCanadienneDeL%E2%80%99expressionD%C3%A9mocratique-FPP-JAN2021-FR.pdf

[31] Royaume-Uni, Department for Digital, Culture, Media & Sport, « Online Harms White Paper: Full Government Response to the Consultation » (15 décembre 2020), en ligne : *Gov.UK* https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

[32] Page 38. https://ppforum.ca/wp-content/uploads/2021/01/UnRapportDeLaCommissionCanadienneDeL%E2%80%99expressionD%C3%A9mocratique-FPP-JAN2021-FR.pdf

[33] Ysabel Gerard, « 'Too good to be true': the challenges of regulating social media start-ups » in Tarleton Gillespie et al., « Expanding the debate about content moderation: scholarly research agenda in the coming policy debates » (2020) 9:4 Internet Policy Review.

[34] Mark Zuckerberg, Témoignage lors de l'audition devant la Chambre des représentants des États-Unis Comité de l'énergie et du commerce Sous-comités de la protection des consommateurs (25 mars 2015), en ligne (pdf): https://docs.house.gov/meetings/IF/IF16/20210325/111407/HHRG-117-IF16-Wstate-ZuckerbergM-20210325-U1.pdf

[35] Les obligations de sécurité pour les services susceptibles d'être accessibles aux enfants sont les suivantes (clause 10) : « 1. prendre des mesures proportionnées pour atténuer et gérer efficacement le risque et l'incidence des préjudices subis par les enfants de différents groupes d'âge 3. Empêcher les enfants de tout âge de tomber sur certains contenus 4. Protéger les enfants des groupes d'âge jugés à risque de tomber sur des contenus préjudiciables ». Voir Reset, Témoignages écrits en ligne soumis concernant le projet de loi sur la sécurité en ligne (septembre 2021), https://committees.parliament.uk/writtenevidence/39851/pdf

[36] États-Unis, *Justice Against Malicious Algorithms Act of 2021*, [introduite] en ligne : https://www.congress.gov/bill/117th-congress/house-bill/5596

[37] Par exemple, plus de 120 organisations de la société civile ont appelé l'Union européenne à adopter une loi sur l'intelligence artificielle (AIA) portant sur les droits fondamentaux. Voir https://edri.org/

[38] De nombreuses EIDP sont également réalisées *après* la survenance des préjudices

[39] Les études d'incidence sur les droits de la personne constituent la première étape de l'identification des comportements répréhensibles des entreprises et des violations des droits de la personne. Cette identification peut ensuite être utilisée pour faire pression sur les entreprises, afin qu'elles corrigent leurs erreurs procédurales et opérationnelles. Ces études d'incidence permettent de cerner les risques juridiques en vertu de la législation sur les droits de la personne qui n'auraient pas été cernés dans les évaluations de l'incidence algorithmique

[40] Les personnes ou les organisations qui procèdent à des études d'incidence sur les droits de la personne doivent également connaître les éventuels enjeux culturels liés aux collectivités concernées et avoir la garantie de disposer de ressources adéquates pour mener à bien l'audit

[41] Un cadre d'EIA pourrait combiner les caractéristiques des évaluations d'impact existantes, notamment les analyses d'impact relatives à la protection des données (AIPD), les études d'incidence sur les droits de la personne et les évaluations de l'impact sur l'égalité des sexes. Certains modèles d'EIA se distinguent également par le fait qu'ils impliquent la participation active et l'engagement des parties prenantes concernées. Tous ces modèles encouragent les développeurs.euses d'une technologie à réfléchir sérieusement aux incidences potentielles avant qu'elles ne surviennent. Voir, par exemple, Ada Lovelace Institute, *Algorithmic impact assessment : a case study in healthcare*, 8 février 2022, en ligne : https://www.adalovelaceinstitute.org/report/algorithmic-impact-assessment-case-study-healthcare/

[42] Le Comité européen de la protection des données a défini comme « à haut risque » les cas concernant : i) l'évaluation ou la notation (par ex, les activités de profilage et de prédiction); ii) la prise de décision automatisée avec effet juridique ou un effet similaire significatif; iii) la surveillance systématique; iv) les données sensibles ou à caractère hautement personnel; v) les données traitées à grande échelle; vi) le croisement ou la combinaison d'ensembles de données; vii) les données concernant des personnes vulnérables; viii) l'utilisation innovante ou l'application de nouvelles technologies ou solutions; ix) les traitements en eux-mêmes, qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou un contrat. Voir Comité européen de la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le

traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, (2017), https://ec.europa.eu/newsroom/article29/items/611236

[43] Il y a un large éventail de méthodologies d'audit servant à diverses fins, qu'il s'agisse de l'audit sur l'existence éventuelle d'une erreur dans un ensemble de données ou de l'audit sur la prévalence des discours haineux tenus sur une plateforme précise. Voir Ada Lovelace Institute, *Technical methods for regulatory inspection of algorithmic systems in social media platforms : A survey of auditing methods for use in regulatory inspections of online harms*, Décembre 2021, https://www.adalovelaceinstitute.org/report/technical-methods-regulatory-inspection/ pour obtenir un sondage sur certaines méthodes pertinentes pour la prolifération des préjudices en ligne

[44] L'inclusion d'une zone sûre pour les « bons samaritains » pourrait encourager les organisations à réaliser ces audits afin de pouvoir infliger des amendes mineures si des résultats préjudiciables sont identifiés

[45] Le règlement général sur la protection des données (RGPD) de l'Union européenne exige également que les responsables du traitement des données procèdent à une évaluation des incidences (article 35) lorsqu'ils/elles traitent des données dans des circonstances précises, notamment le traitement automatisé (article 35, paragraphe 3, point a)). L'article 26 de la *Législation sur les services numériques* de l'Union européenne obligerait certaines entreprises du secteur des TIC à procéder à des évaluations annuelles des risques en tenant compte de certains risques précis, y compris l'incidence de leurs services sur certains droits de la personne. La proposition de règlement de l'UE sur l'intelligence artificielle vise à harmoniser le cadre juridique de l'intelligence artificielle entre les États membres de l'UE. L'article 29 impose aux utilisateurs de systèmes d'IA à haut risque (c'est-à-dire des systèmes qui présentent des risques importants pour la santé et la sécurité ou les droits fondamentaux de la personne) l'obligation de procéder à une analyse d'impact relative à la protection des données (AIPD) conformément à l'article 35 du RGPD de l'UE

[46] Commission européenne, « Proposition de règlement du parlement européen et du conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE », Commission européenne, 15 décembre 2020, article 28, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services ; Commission européenne, « Proposition de règlement du parlement européen et du conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, Commission européenne, 15 décembre 2020, articles 41 et 54, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services. Dans certains cas, la Commission serait également habilitée à demander l'accès aux bases de données et aux algorithmes des plateformes et à obtenir des renseignements à leur sujet

[47] La directive exige que les fournisseurs.euses de systèmes automatisés de prise de décision documentent les décisions, testent et surveillent les résultats, valident la qualité des données, effectuent des évaluations des risques de sécurité et communiquent au public l'information sur l'efficacité et l'efficience du système. Décrit comme une approche « légère », le modèle de questionnaire canadien comporte des caractéristiques prometteuses, telles que des exigences à plusieurs niveaux en fonction de l'augmentation du risque, un examen par les pairs et l'intégration d'autres évaluations, comme la loi l'exige. Les autres modèles actuels d'EIA comprennent le modèle du questionnaire, l'analyse d'impact relative à la protection des données (AIPD) et le modèle de l'organisme public. Voir Building a systematic framework of accountability for algorithmic decision making https://www.ifow.org/publications/policy-briefing-building-a-systematic-framework-of-accountability-for-algorithmic-decision-making

[48] La *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario exige que les organisations tiennent un registre d'audit électronique dans le contexte des renseignements personnels sur la santé, qui doit être fourni sur demande au commissaire à l'information et à la protection de la vie privée de l'Ontario. Voir projet de loi 188, https://www.ola.org/fr/affaires-legislatives/projets-loi/legislature-42/session-1/projet-loi-188, article 10.1.

[49] Le projet de loi 64 du Québec exige la traçabilité de la prise de décision automatisée pour les personnes qui en font la demande. Voir projet de loi 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 1re session, 42e législature, Québec, 2020, paragraphe 102 (modifiant l'alinéa 12.1 (2) de la Loi)

[50] Notamment en ce qui concerne la traçabilité et les évaluations des facteurs relatifs à la vie privée Voir Commissariat à la protection de la vie privée du Canada, *Un cadre réglementaire pour l'IA : recommandations pour la réforme de la LPRPDE*, (12 novembre 2020), en ligne : *wwwprivgcca* https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/reg-fw_202011

[51] Le premier guide les entreprises dans le processus de réévaluation de leur gouvernance et de leur gestion des risques, également à la lumière du RGPD de l'UE. Le second propose huit domaines de risque propres à l'IA : l'équité et la transparence dans le profilage, l'exactitude, les modèles de prise de décision entièrement automatisés, la sécurité et la cybernétique, les compromis (par exemple, exactitude contre vie privée), la minimisation des données et la limitation de la finalité, l'exercice des droits individuels et l'incidence sur les intérêts et les droits publics en général. Voir Commissariat à l'information du Royaume-Uni, *AI Auditing Framework*, 2021, en ligne : https://ico.org.uk/about-the-ico/news-and-events/ai-auditing-framework. En outre, en collaboration avec les autorités d'audit de

Norvège, d'Allemagne, de Finlande et des Pays-Bas, le Royaume-Uni a publié le premier livre blanc international sur l'audit des algorithmes d'apprentissage automatique et d'IA dans le secteur public. Voir Institutions supérieures d'audit de Finlande, d'Allemagne, des Pays-Bas, de Norvège et du Royaume-Uni, *Auditing machine learning algorithms*, 24 novembre 2020, en ligne : https://www.auditingalgorithms.net

[52] La proposition d'Algorithmic Accountability Act confierait à la Federal Trade Commission la tâche de publier et d'appliquer des réglementations qui obligeraient certaines entités utilisant des renseignements personnels à réaliser des évaluations d'impact et à « traiter raisonnablement et en temps utile » toute faille ou tout enjeu de sécurité identifié

[53] La loi adopte une approche systématique pour établir une norme de sécurité et d'efficacité pour les algorithmes, de sorte que les plateformes en ligne ne puissent pas utiliser des processus automatisés qui nuisent aux utilisateurs.trices

[54] Haut Commissariat des Nations unies aux droits de l'homme, *Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « Protéger, respecter et réparer »* [2011], en ligne (pdf), Nations unies https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_FR.pdf. De même, à l'annexe A.2 du *Guide OCDE sur le devoir de diligence pour une conduite responsable des entreprises* de l'Organisation de coopération et de développement économiques (OCDE), on exige des entreprises qu'elles identifient et évaluent les incidences négatives avérées et potentielles liées à leurs activités, produits ou services (on mentionne précisément au point 2.2. les études d'incidence sur les droits de la personne). Voir OCDE, *Guide OCDE sur le devoir de diligence pour une conduite responsable des entreprises*, [2008], en ligne (pdf) : https://www.oecd.org/fr/daf/inv/mne/Guide-OCDE-sur-le-devoir-de-diligence-pour-une-conduite-responsable-des-entreprises.pdf

[55] Natasha Lomas, *On illegal hate speech, EU lawmakers eye binding transparency for platforms*, 23 juin 2020, en ligne : *TechCrunch* https://techcrunch.com/2020/06/23/on-illegal-hate-speech-eu-lawmakers-eye-binding-transparency-for-platforms/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADSpS383iySoMG0zqq-psDXcC2iT9TLSr_fGXHUWn4aUmehXKdbTqo_r1gaJi8bWbuAEyUUROO42tD0sY43J5xK4ly1LAo6VOk72CLyr2xVxAoL6T2b9kRRR30rMqHo4Q7eec4tv0Ht4c2yZzphTRKis0AeGXesGOsY4IJ5DTMjm

[56] Yuan Stevens et Sonja Solomun. Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act, *Cybersecure Policy Exchange*, février 2021. Voir aussi, Penney, Jonathon, Chilling Effects: Online Surveillance and Wikipedia Use (2016). Berkeley Technology Law Journal, vol. 31, nº 1, p. 117, 2016, disponible sur SSRN : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645 ; Miles Kenyon, « Jon Penney on the Chilling Effects of Online Surveillance », (11 juillet 2017), *Citizen Lab*: https://citizenlab.ca/2017/07/jon-penney-on-the-chilling-effects-of-online-surveillance/#:~:text=Jon%20Penney%2C%20research%20fellow%20at,be%20hesitant%20to%20share%20content

[57] Kayla Hilstob, *Karrmen Crey – Indigenous Epistemologies*, 7 décembre 2021, en ligne : Digital Democracies Institute https://digitaldemocracies.org/karrmen-crey-indigenous-epistemologies

[58] Chidi Oguamanam, *Indigenous Data Sovereignty : Retooling Indigenous Resurgence for Development*, CIGI Papers, décembre 2019, nº 234, p. 15

[59] Indigenous AI, *Indigenous Protocol and Artificial Intelligence Working Group*, https://www.indigenous-ai.net/

[60] Michael Running Wolf, *International Wakashan AI Consortium*, en ligne : *MIT SOLVE* https://solve.mit.edu/challenges/2020-indigenous-communities-fellowship/solutions/33358

[61] Chambre des communes du Canada, *Projet de loi C-11, Loi modifiant la Loi sur la radiodiffusion et apportant des modifications connexes et corrélatives à d'autres lois*, 2 février 2022, en ligne : https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-11/premiere-lecture

[62] Carrefour australien de la propriété intellectuelle sur les connaissances autochtones https://www.ipaustralia.gov.au/indigenous-knowledge-ip-hub

[63] Michael Morden et al, *Investing in Canadians' civic literacy: An answer to fake news and disinformation*, (Toronto : Le Centre Samara pour la démocratie, 2019), en ligne (pdf) : https://www.samaracanada.com/docs/default-source/reports/investing-in-canadians-civic-literacy-by-the-samara-centre-for-democracy.pdf?sfvrsn=66f2072f_4

[64] Philip N. Howard, Lisa-Maria Neudert, Nayana Prakash et Steven Vosloo, *Digital misinformation/ disinformation and children*, UNICEF, août 2021. https://www.unicef.org/globalinsight/reports/digital-misinformation-disinformation-and-children et Sonia Livingstone,

Mariya Stoilova et Rishita Nandagiri, *Children's data and privacy online Growing up in a digital age : An evidence review*, 2018 https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf

[65] Jessie Daniels, Mutale Nkonde et Darakhshan Mir, *Advancing Racial Literacy in Tech. Why Ethics, Diversity in Hiring & Implicit Bias Trainigns Aren't Enough*, Data & Society, 2019

[66] Rudman, L. A., Ashmore, R. D., et Gary, M. L., *Unlearning » automatic biases : The malleability of implicit prejudice and stereotypes*, Journal of Personality and Social Psychology, 2001, 81(5), 856–868. https://doi.apa.org/doiLanding?doi=10.1037%2F0022-3514.81.5.856

[67] Jennifer Wemigwans, politique de notes de service, session 5, 16 novembre

[68] Assemblée des citoyens canadiens sur l'expression démocratique, « Assemblée des citoyens canadiens sur l'expression démocratique : Recommandations pour renforcer la réponse du Canada à la diffusion de la désinformation en ligne » (Forum des politiques publiques, Ottawa, 2022), https://static1.squarespace.com/static/5f8ee1ed6216f64197dc541b/t/61e97ea8734e895b17210d63/1642692268571/DemX-Recommandations+pour+l%27intervention+du+Canada+dans+la+diffusion+de+de%CC%81sinformation+en+ligne-PPF-Jan2022-FR.pdf p. 42-43

[69] Cyphers, Bennett et Cory Doctorow, *Privacy Without Monopoly : Data Protection and Interoperability*, Electronic Frontier Foundation, 2021. https://www.eff.org/wp/interoperability-and-privacy

[70] États-Unis, Projet de loi HR 3894, *Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021*, 117e Congrès, 2021 (proposition), https://www.congress.gov/bill/117th-congress/house-bill/3849/text

[71] UE, *Proposition de règlement du parlement européen et du conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques)* [2020] com/2020/842 final, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52020PC0842

[72] Assemblée citoyenne canadienne sur l'expression démocratique, « Assemblée citoyenne canadienne sur l'expression démocratique : Recommandations pour renforcer la capacité d'intervention du Canada en matière de diffusion de désinformation en ligne » (*Forum des politiques publiques*, 2022), en ligne https://ppforum.ca/wp-content/uploads/2022/01/DEMX-R2.pdf

[73] *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) [2016] OJ L 119, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

[74] Loi californienne de 2018 sur la protection de la vie privée des consommateurs, S 1. L'alinéa 1798.100 du Code civil, tel qu'ajouté par l'alinéa 3 du chapitre 55 des statuts de 201, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB1121&showamends=false

[75] Frank Pasquale, *Black box society : the secret algorithms that control money and information* (Cambridge, Massachusetts : Harvard University Press, 2016), p. 14

[76] Voir, par exemple, Julia Angwin et al., *Machine Bias*, ProPublica, 23 mai 2016, en ligne : https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing ; Anthony Flores, Kristin Bechtel et Christopher Lowenkamp, *False Positives, False Negatives, and False Analyses : A Rejoinder to "Machine Bias : There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks"*, 80:2 Journal fédéral de la probation, 2016, en ligne : https://www.uscourts.gov/sites/default/files/80_2_6_0.pdf ; Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, vol. 66 n° 1, 2019, UCLA L, rév. 54

[77] Voir, par exemple, Sandra Wachter, Brent Mittelstadt et Chris Russell, *Counterfactual Explanations Without Opening the Black Box : Automated Decisions and the GDPR*, Harvard Journal of Law and Technology, vol 31, n° 2, 2018, pp 842-843; Lilian Edwards & Michael Veale, *Enslaving the Algorithm :* From a "*Right to an Explanation' to a 'Right to Better Decisions*"*?,* IEEE Security & Privacy, vol. 16, n° 3, 2018; Marco Almada, *Human intervention in automated decision-making: Toward the construction of contestable systems* (New York, NY, USA: Association for Computing Machinery, 2019)

[78] Sandra G. Mayson, *Bias In, Bias Out*, Yale L J, vol. 128, n° 8, 2019, pp. 2218-2224; Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, Calif L, vol. 104, n° 3, rév. 671, 2016

[79] Jeff Ward, *Black Box Artificial Intelligence and the Rule of Law,* Law & Contemporary Problems i, vol. 84, n° 3, 2021

[80] Frank Pasquale, *Black box society : the secret algorithms that control money and information* (Cambridge, Massachusetts: Harvard University Press, 2016), p. 4

[81] Frank Pasquale, *Black box society : the secret algorithms that control money and information* (Cambridge, Massachusetts: Harvard University Press, 2016), p. 3

[82] Allison Trites, *How Algorithmic Decision-Making is Changing How We View Society and People: Advocating for the Right for Explanation and the Right to be Forgotten in Canada*, Global Media J, vol. 11, n° 2, 2019, pp. 18-19

[83] Jeff Ward, *Black Box Artificial Intelligence and the Rule of Law*, Law & Contemporary Problems i at ii, vol. 84, n° 3, 2021; Joshua A. Kroll et al., *Accountable Algorithms*, 165 U Pa L, rév. 633, 2017; Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 NYU L, 2019, rév. 15, en ligne

[84] Voir DeltaFreq, Commentaire sur l'article du blog de Barry Ritholtz, *Where's the Note? Leads BAC to Ding Credit Score*, The Big Picture (blog), 14 décembre 2010, 11 h 03, http://www.ritholtz.com/blog/2010/12/note-bac-credit-score

[85] Jeff Harrington, *2010 Adds Its Own Terminology to Business Lexicon*, Tampa Bay Times, 23 décembre 2010, https://www.tampabay.com/news/business/

[86] Alan F.T. Winfield & Marina Jirotka, *The Case for an Ethical Black Box*, dans Yang Gao et al., *Towards Autonomous Robotics Systems* (Springer, 2017), pp. 265-266

[87] Dino Pedreschi et al., *Open the Black Box Data-Driven Explanation of Black Box Decision Systems*, Association for Computer Machinery, vol. 1, n° 1, 2018, pp. 1-2

[88] S'agissant des manipulations électorales, voir : Mark Scott, *Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower*, 27 mars 2018, en ligne : POLITICO https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook (concernant le référendum britannique sur le Brexit et les élections présidentielles américaines de 2016); Bruna Martins dos Santos et Joana Varon, *Analysis of the playing field for the influence industry in preparation for the Brazilian general elections*, Coding Rights for Tactical Technology Collective, 2018, en ligne : https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-data-and-politics-brazil.pdf (sur les élections fédérales brésiliennes de 2018). S'agissant de la désinformation, voir Mieiam Fernández, Alejando Bellogín et Iván Cantador, *Analysing the Effect of Recommendation Algorithms on the Amplification of Misinformation*, 2021, en ligne : https://arxiv.org/abs/2103.14748. S'agissant des préjudices causés aux adolescent.e.s et aux enfants, voir Georgia Wells, Jeff Horwitz et Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, Wall Street Journal, 14 septembre 2021, en ligne : https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

[89] Robyn Caplan et Danah Boyd, *Who Controls the Public Sphere in an Era of Algorithms? Mediation, Automation, Power*, Data and Society, 13 mai 2016, p. 8

[90] Riccardo Guidotti et al, *Factual and Counterfactual Explanations for Black Box Decision Making*n, IEEE Intelligent Systems, vol. 34, n° 6, 2019, p. 14; Sandra Wachter, Brent Mittelstadt et Chris Russell, *Counterfactual Explanations Without Opening the Black Box : Automated Decisions and the GDPR*, Harvard Journal of Law & Technology, vol. 31, n° 2, 2018, pages 842, 849-852, 860-872

DEMOCRATICEXPRESSIONDÉMOCRATIQUE

DEMOCRATICEXPRESSION.CA