CONCORDIA

LES DROITS DE LA PERSONNE À L'ÈRE NUMÉRIQUE

RAPPORT DE LA CONFÉRENCE RIGHTS CITY 2021

Université Concordia University
MONTREAL INSTITUTE FOR GENOCIDE AND HUMAN RIGHTS STUDIES

National Defence Défense nationale

Les droits de la personne à l'ère numérique

Rapport de la conférence Rights City 2021

Partenaires

Kingdom of the Netherlands

Centre de recherche et d'enseignement sur les droits de la personne

Human Rights Research and Education Centre

Défense nationale National Defence

EMBASSY OF THE UNITED STATES Ottawa, Canada

GLOBAL ACTION AGAINST MASS ATROCITY CRIMES GAAMAC Platform for Prevention

RAOUL WALLENBERG CENTRE FOR HUMAN RIGHTS POUR LES DROITS DE LA PERSONNE

United Nations Educational, Scientific and Cultural Organization

Canadian Commission for UNESCO

Les droits de la personne à l'ère numérique
Rapport de la conférence Rights City 2021

Introduction

La conférence #RightsCity 2021, tenue en ligne du 15 au 18 juin 2021, se concentrait sur l'interaction entre les droits de la personne, la sécurité et la technologie. #RightsCity est le principal forum canadien de discussion sur les droits de la personne. Créée en 2017 comme initiative conjointe de l'Institut montréalais d'études sur le génocide et les droits de la personne et du Centre Raoul Wallenberg pour les droits de la personne, la conférence en est maintenant à sa troisième édition. Organisé par l'Institut montréalais d'études sur le génocide et les droits de la personne de l'Université Concordia, l'événement était financé par le ministère canadien de la Défense nationale et réalisé en partenariat avec le Centre Raoul Wallenberg pour les droits de la personne, le Centre de recherche et d'enseignement sur les droits de la personne de l'Université d'Ottawa, l'ambassade du Royaume des Pays-Bas au Canada, l'initiative Global Action Against Mass Atrocity Crimes et l'ambassade des États-Unis au Canada, avec l'appui de la Commission canadienne pour l'UNESCO.

La conférence réunissait d'éminents experts mondiaux travaillant dans les secteurs gouvernemental, non gouvernemental et privé pour examiner les menaces et les possibilités que représente la révolution numérique pour le respect et la protection des droits de la personne et des valeurs démocratiques.

Le débat portait sur les thèmes suivants :

- La démocratie peut-elle survivre à Internet? L'ingérence étrangère et les campagnes de désinformation
- Faire face à l'autoritarisme numérique
- L'importance d'une Convention de Genève numérique
- Les attaques numériques dirigées contre les militants des droits de la personne ou de la démocratie
- Comment unir les démocraties vis-à-vis de la technologie
- Les médias sociaux comme outil d'enquête et de poursuite contre les atrocités criminelles
- La lutte contre les discours de haine sur Internet

Le présent document résume les principaux thèmes des discussions et propose des recommandations pour faire progresser les droits de la personne et les valeurs démocratiques à l'ère numérique.

Mot du directeur

#RightsCity est le principal forum canadien de discussion sur les droits de la personne. Organisé pour la première fois en 2017 – expressément pour coïncider avec les célébrations du 375^{e} anniversaire de Montréal –, l'événement est une initiative conjointe de l'Institut montréalais d'études sur le génocide et les droits de la personne et du Centre Raoul Wallenberg pour les droits de la personne. Sa troisième édition s'est tenue en ligne en raison de la pandémie de COVID-19. Organisé par l'Institut montréalais d'études sur le génocide et les droits de la personne de l'Université Concordia, l'événement était financé par le ministère canadien de la Défense nationale et réalisé en partenariat avec le Centre Raoul Wallenberg pour les droits de la personne, le Centre de recherche et d'enseignement sur les

droits de la personne de l'Université d'Ottawa, l'ambassade du Royaume des Pays-Bas au Canada, l'initiative Global Action Against Mass Atrocity Crimes et l'ambassade des États-Unis au Canada, avec l'appui de la Commission canadienne pour l'UNESCO.

Contexte et discours d'ouverture : La tendance dystopique de la révolution informatique

- Irwin Cotler, fondateur et président du Centre Raoul Wallenberg pour les droits de la personne
- Jason Munyan, administrateur de programme, Bureau du conseiller spécial de l'Envoyé spécial du Secrétaire général des Nations Unies pour la technologie

> « Quand la technologie s'emballe, le droit est à la traîne. » – Irwin Cotler, fondateur et président du Centre Raoul Wallenberg pour les droits de la personne

Le réseau Internet connecte deux tiers de l'humanité à l'information, aux possibilités économiques et aux plateformes de communication. Il a dominé les changements sociaux, politiques et économiques des 15 dernières années. La dépendance à Internet s'est encore accrue au cours de la pandémie, car il a permis aux habitants du monde entier de s'informer sur le virus et sur les mesures sanitaires en place, tout en donnant la possibilité de travailler, d'étudier et de communiquer. Cependant, la révolution technologique coïncide avec le déclin mondial de la démocratie et des espaces citoyens ouverts et transparents. La menace – que l'on observait déjà manifestement avant la pandémie – que ce phénomène représente pour la sécurité et les droits de la personne n'a fait que grandir avec l'accroissement de la dépendance à Internet.

Irwin Cotler a profité de son discours d'ouverture pour présenter les effrayantes caractéristiques dystopiques de la révolution informatique, notamment :

1. la prolifération de la cyberguerre soutenue par l'État pour perturber les infrastructures critiques – par exemple, les cyberattaques et les rançongiciels – et s'immiscer dans les processus politiques nationaux, comme les élections;
2. la transformation des médias sociaux en outil de répression de la dissidence, au service des régimes autoritaires, ce qui leur permet d'étouffer les critiques et de diffuser la désinformation tant dans leur propre pays qu'à l'étranger;
3. l'augmentation exponentielle des discours haineux en ligne – y compris l'incitation à la haine et à la violence sanctionnée par l'État – et l'impact hors ligne de ces discours sur la vie de la population;
4. les menaces pour la démocratie au Canada et dans d'autres démocraties par l'intégration de technologies sophistiquées dans les organismes d'application de la loi d'une manière qui viole le droit national et international en matière de droits de la personne.

M. Cotler a souligné que le droit est à la traîne du progrès technologique, ce qui laisse des failles dangereuses dans les protections juridiques des droits de la personne, tant au Canada qu'à l'étranger.

> « Les coupures d'Internet sont devenues plus sophistiquées, durent plus longtemps, touchent plus de personnes et ciblent les groupes vulnérables. » – Jason Munyan

Jason Munyan, du Bureau du conseiller spécial de l'Envoyé spécial du Secrétaire général des Nations Unies pour la technologie, a souligné que le plan d'action du Secrétaire général pour la coopération numérique était une réponse à la vulnérabilité croissante des citoyens face aux atteintes à la vie privée, aux technologies de surveillance, au harcèlement et aux violations des droits de la personne. La Feuille de route appelle les États membres à placer les droits de la personne au centre des cadres réglementaires pour le développement et l'utilisation des technologies. Elle appelle également les entreprises technologiques à reconnaître l'importance des droits de la personne dans l'espace numérique. Le Conseil des droits de la personne des Nations Unies a affirmé à plusieurs reprises que les droits des personnes en ligne doivent être les mêmes que ceux hors ligne. Cependant, les normes qui guident le comportement en ligne n'ont pas été pleinement réalisées. Une récente déclaration commune de neuf rapporteurs spéciaux des Nations Unies l'a affirmé :

> « Certains États continuent d'utiliser ces technologies pour museler la dissidence, surveiller et réprimer les actions collectives en ligne et hors ligne, et les entreprises technologiques n'ont pas fait grand-chose pour éviter ces violations des droits de la personne. Ces abus nous préoccupent profondément. Ils sont devenus encore plus fréquents avec la pandémie et vont – en se poursuivant – exacerber les inégalités dans le monde entier. »[1]

M. Munyan a encouragé les États membres de l'ONU à collaborer avec l'organisme international et d'autres intervenants du secteur des technologies pour « veiller à ce que les avancées technologiques de demain ne se fassent pas au détriment des droits de la personne fondamentaux universels que nous nous engageons à soutenir, à promouvoir et à défendre. »

Panel 1 : La démocratie peut-elle survivre à Internet? L'ingérence étrangère et les campagnes de désinformation

- Rafal Rohozinski, fondateur et directeur, SecDev Group (modérateur)
- Emily Dreyfuss, membre et rédactrice en chef du Centre Shorenstein sur les médias, la politique et les politiques publiques
- Alice Stollmeyer, directrice générale, Defend Democracy
- Sophie Zhang, ancienne employée de Facebook et lanceuse d'alerte

> « Demander si la démocratie peut survivre à Internet, c'est comme demander si le climat peut survivre aux combustibles fossiles… je vois de nombreuses similitudes entre le lobby des grandes entreprises technologiques et celui des combustibles fossiles. »
> – Alice Stollmeyer, directrice exécutive de Defend Democracy

Rafal Rohozinski a entamé le débat en décrivant comment la révolution numérique transforme le contrat social entre les institutions et les citoyens. Les gardiens traditionnels de l'opinion publique et du changement social tels que la famille, les écoles et les gouvernements sont contournés par un accès direct à l'information, à la conversation et au divertissement dans les médias sociaux et, de plus en plus, dans les jeux interactifs. La jeunesse d'Internet – avec deux tiers des utilisateurs âgés de moins de 35 ans et la moitié de tous les utilisateurs âgés de moins de 25 ans – se mêle à cette nouvelle technologie pour libérer sa créativité et remettre en question le *statu quo*. M. Rohozinski a déclaré que « la révolution actuelle est susceptible de redéfinir nos institutions et les processus dont elles dépendent ». L'absence de normes acceptées régissant le comportement des entreprises, des États

[1] Bureau du Haut Commissaire aux droits de l'homme, https://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=27140&LangID=F

et des utilisateurs dans le cyberespace a permis à quiconque de façonner le discours, les opinions et d'influencer les choix démocratiques locaux.

> « Comme les précédentes révolutions technologiques, cette révolution pourrait redéfinir nos institutions et les processus dont elles dépendent. » – Rafal Rohozinski

Les panélistes ont tous convenu que les gouvernements démocratiques sont gravement compromis par une crise de la désinformation. L'accès à des informations exactes, opportunes et pertinentes est un pilier fondamental de la démocratie, et l'engagement des citoyens doit être cultivé et entretenu pour prospérer. Or, les plateformes Internet – tant les moteurs de recherche que les médias sociaux – ne sont pas structurées de façon à faciliter l'accès des utilisateurs aux informations confirmées et de sources fiables. La désinformation en ligne – la diffusion d'informations fausses – constitue actuellement la pire menace pour les démocraties. La conception des plateformes Internet actuelles privilégie, d'une part, les opinions les plus populaires plutôt que les informations fiables, et joue, d'autre part, sur la polarisation et les extrêmes pour encourager l'engagement des utilisateurs.

Un défi majeur pour les États, les entreprises et les acteurs de la société civile dans la lutte contre la désinformation est qu'il n'existe pas actuellement de définitions convenues des termes pour décrire les différentes facettes du problème. Sophie Zhang a souligné que les entreprises telles que Facebook doivent faire face à un double problème d'authenticité du messager et du message : tout le monde peut facilement créer un faux compte pour diffuser des informations erronées. Ce contenu peut ensuite être partagé de manière malveillante par d'autres faux comptes, voire par de vrais utilisateurs qui croient réellement, ou non, à l'authenticité de ces informations. Le caractère transnational du contenu généré par les utilisateurs complique davantage la distinction entre la source et le message. En effet, la désinformation peut provenir tant du pays concerné que de l'étranger. Les participants s'accordent à dire que l'ingérence étrangère dans le discours public occidental est beaucoup moins importante qu'on ne le croit généralement. Cette importance excessive accordée à l'ingérence étrangère a conduit les politiciens et les experts occidentaux à négliger les convictions politiques peu recommandables de leurs propres citoyens et de leur propre culture. Les opposants instrumentalisent ensuite ces opinions, amplifiées par des défenseurs rémunérés (trolls) ou de faux comptes d'utilisateurs payés. M^{me} Zhang a noté que « la perception exagérée de l'omniprésence et de l'influence en ligne de la Russie sert ses intérêts ».

Les participants ont souligné l'importance d'une approche globale de la sécurité et des droits de la personne pour protéger la démocratie. L'une des suggestions avancées pour répondre à la nécessité de mettre fin à l'importance actuelle de la polarisation et de la fragmentation des utilisateurs sur Internet et de changer d'approche consiste à encourager les entreprises technologiques à diversifier activement les intervenants dans la conception de plateformes en utilisant un processus de conception participative. Le renforcement des directives de la communauté et l'utilisation d'un code source libre pourraient également y contribuer. De plus, certains participants ont affirmé que les incitations capitalistes des entreprises privées devaient être limitées pour empêcher la diffusion de contenus extrêmes sur Internet. En brisant les monopoles et en repensant l'économie des contenus Internet à succès (tels que la publicité et les pages vues), on pourrait permettre à des solutions de rechange plus éthiques de se développer.

Panel 2 : Faire face à l'autoritarisme numérique

- Michael Petrou, rédacteur en chef, *Open Canada* (modérateur)
- Chris Meserole, directeur de recherche, AI and Emerging Tech Initiative, et *Fellow*, Foreign Policy Program à la Brookings Institution

- Sophie Richardson, directrice pour la Chine, Human Rights Watch
- Margaret McCuaig-Johnston, Membre associée, Institut pour la science, la société et la politique de l'Université d'Ottawa

> « Il est très important d'envisager la manière dont les États utilisent cette technologie dans des environnements où ils ne peuvent pas chasser un gouvernement par les urnes, ou essayer de changer une loi, ni même envoyer une lettre à un journal local pour se plaindre de l'utilisation de cette technologie. » – Sophie Richardson, Human Rights Watch

Les États autoritaires ont rapidement reconnu le potentiel du numérique pour consolider leur emprise sur les citoyens. La Chine a exploité les outils numériques pour se faire une idée précise de l'opinion et du comportement de ses citoyens, en renforçant la surveillance de la population et le contrôle des dissidents, des militants et des groupes minoritaires. Le traitement des Ouïgours dans la province chinoise du Xinjiang a été décrit comme un crime contre l'humanité par Human Rights Watch (HRW). Sophie Richardson a détaillé certains des outils utilisés par la Chine, tels que les cartes d'identité biométriques à puce, les bases de données ADN, les logiciels de reconnaissance faciale et de reconnaissance de la démarche, pour examiner, contrôler et finalement détenir les Ouïgours. Dans un cas, HRW a découvert une application de surveillance utilisée par la police et les forces de sécurité dont l'algorithme combinait des données provenant de diverses sources. L'algorithme évaluait différents types de comportements pour décider si un individu était suspect. Ces preuves, qui comprennent des comportements tels que l'utilisation de la porte avant ou arrière de la maison ou le fait de parler plus souvent aux voisins, ont ensuite été utilisées pour placer les Ouïgours en détention arbitraire. Cette surveillance accrue de l'État est d'autant plus préoccupante lorsque l'État ne laisse aucun espace pour l'engagement civique et la responsabilité.

L'importance accordée aux possibilités offertes par la technologie a également exacerbé les tendances existantes à l'autoritarisme dans les démocraties fragiles et dans les institutions internationales. Les entreprises chinoises investissent dans l'exportation de leurs technologies à l'étranger, guidées par des objectifs géostratégiques. Le gouvernement est prêt à subventionner les technologies destinées aux États autoritaires et aux démocraties fragiles. Les panélistes ont convenu qu'il fallait faire davantage pour contrer cette stratégie d'exportation déstabilisante. Au-delà de l'exportation et de l'utilisation de technologies déterminées, la Chine s'est efforcée de saper les normes internationales en matière de droits de la personne et de légitimer son approche de la technologie à l'échelle internationale. Au cours de la dernière décennie, la Chine a cherché à influencer les normes industrielles, les réglementations commerciales et les normes internationales en faveur de valeurs autoritaires. Parce qu'il place la souveraineté de l'État sur Internet au-dessus de la responsabilité et des droits de la personne, l'engagement diplomatique chinois en matière de technologie au niveau international peut être considéré comme une tentative de faire valoir ses propres points de vue et valeurs comme le comportement par défaut en ligne. Les panélistes ont convenu que les États démocratiques n'avançaient pas les ressources nécessaires pour représenter les valeurs démocratiques dans les forums internationaux pertinents, ce qui permettait à Pékin de faire de sérieuses avancées dans la gouvernance d'Internet. Margaret McCuaig-Johnston a fait remarquer que les diplomates, comme l'actuel ambassadeur du Canada auprès de l'ONU, Bob Rae, se sont montrés plus francs sur cette question au Conseil de sécurité de l'ONU et devraient continuer à le faire.

> « La politique de Xi Jinping vise à combiner le développement des technologies civiles et militaires. Ce qui signifie que les chercheurs canadiens qui s'associent à des homologues en Chine dans des domaines tels que l'IA, la nanotechnologie, la biotechnologie, la photonique, l'informatique quantique et les matériaux avancés peuvent ne pas se rendre compte que les

idées qu'ils partagent avec leurs collègues pourraient servir des applications militaires à leur insu. » – Margaret McCuaig-Johnston

Tout aussi inquiétante est la complicité d'entreprises et d'universités d'États démocratiques occidentaux, comme le Canada, dans la répression menée par l'État. M^me^ McCuaig-Johnston a expliqué que plusieurs universités canadiennes effectuent des recherches en partenariat avec des entreprises technologiques chinoises qui sont impliquées dans la répression d'État, y compris celle des Ouïgours. La société chinoise de logiciels de reconnaissance faciale SenseTime est associée à l'Université de l'Alberta par l'intermédiaire d'un partenaire mutuel, le Hong Kong AI Institute; IFlyTech, qui a développé des bases de données de reconnaissance vocale et de modèles vocaux pour soutenir la surveillance et la persécution des Ouïgours, a créé une chaire de recherche à l'Université de l'Alberta et à l'Université Queen's. M^me^ McCuaig-Johnston a souligné que la portée de l'État chinois est telle que l'on peut supposer que les informations détenues par ces entreprises sont transmises au gouvernement chinois, avec le soutien implicite d'étudiants et d'universitaires canadiens. Tous les panélistes ont appelé les universités canadiennes à faire preuve d'une meilleure diligence raisonnable et d'un meilleur raisonnement éthique dans leur prise de décision sur les partenariats, en plus des examens en cours des partenariats chinois par les autorités provinciales en Alberta et le gouvernement fédéral. M^me^ McCuaig-Johnston a suggéré que le Service canadien du renseignement de sécurité pourrait faire davantage pour aider les universités à élaborer des critères de diligence raisonnable pour éclairer la prise de décision.

Les entreprises occidentales doivent être conscientes des dangers de la vente de technologies à des régimes autoritaires comme la Chine. M. Meserole a expliqué que si le Canada dispose de lois strictes en matière d'exportation de technologies ayant des applications militaires, la dangerosité des applications civiles des logiciels n'est pas souvent prise en compte dans les règlements d'exportation actuels. M. Meserole a suggéré qu'étant donné que les données et l'IA sont difficiles à réglementer au niveau transnational, le cœur de la réglementation future devrait se concentrer sur la limitation de la puissance de calcul. Très peu de pays (États-Unis, Pays-Bas et Japon) possèdent la capacité de produire les équipements nécessaires à la fabrication des processeurs d'ordinateurs. Des sanctions ciblées sur ces équipements pourraient être la voie à suivre pour la réglementation des exportations.

Panel 3 : L'importance d'une Convention de Genève numérique

- Megan Roberts, directrice de la planification des politiques, Fondation des Nations Unies (modératrice)
- Stéphane Duguin, PDG, CyberPeace Institute
- Yves Daccord, *Fellow*, Berkman Klein Center for Internet and Society, Université Harvard, ancien directeur général du Comité international de la Croix-Rouge
- Ana Beduschi, professeure associée à l'Université d'Exeter, et chercheuse associée à l'Académie de droit international humanitaire et de droits humains à Genève

« Il y a un problème d'application [**des** mesures de protection actuelles] et un problème de responsabilité... je ne vois pas comment la création d'un nouvel instrument de droit international pourrait résoudre ce problème. » – Ana Beduschi, Université d'Exeter et Académie de droit international humanitaire et de droits humains à Genève

Les cyberattaques sont largement sous-déclarées, et la majorité d'entre elles ont lieu en dehors des zones de conflit actif. Elles sont dirigées à la fois par des États et des acteurs non étatiques, qui peuvent

avoir des affiliations avec certains États. Les secteurs traditionnellement protégés – tels que les soins de santé – sont de plus en plus attaqués par des acteurs étatiques et non étatiques. Le CyberPeace Institute a documenté une augmentation de 45 % des attaques de rançongiciels contre les infrastructures de santé critiques pendant la pandémie, comparativement à une augmentation de 20 % dans d'autres secteurs pendant la même période. Ces attaques visent généralement à voler des données médicales, qui ont plus de valeur que les données financières sur le marché noir. Les données peuvent également être volées, puis modifiées pour alimenter des campagnes de désinformation. Le cyberespionnage des données relatives aux soins de santé a également augmenté, les États cherchant à utiliser ces informations pour acquérir une influence géopolitique sur un rival.

Face à de telles attaques sur ce qui est traditionnellement un espace neutre entre les États, la communauté internationale s'efforce de développer des approches visant à protéger les personnes contre les atteintes sur Internet. En 2017, le président de Microsoft, Brad Smith, a appelé à la création d'une nouvelle Convention de Genève numérique pour répondre au défi de l'augmentation des cyberattaques menées par des États-nations. Les participants se sont montrés sceptiques quant à l'apport d'une Convention de Genève numérique aux protections actuelles des droits de la personne, sans une compréhension approfondie des lacunes des cadres disponibles. Ana Beduschi a souligné que « les cyberopérations ne se déroulent pas dans un vide juridique » : les cadres internationaux existants s'appliquent au cyberespace. En cas de conflit armé, le droit international humanitaire s'applique, tandis qu'en temps de paix, c'est le droit international relatif aux droits de la personne qui prime. Le secteur privé est également censé adhérer aux principes directeurs des Nations Unies sur les entreprises et les droits de la personne. L'applicabilité de ces mécanismes a été réaffirmée par le groupe de travail à composition non limitée et le groupe d'experts des Nations Unies, ainsi que par d'autres parties du système des droits de la personne des Nations Unies. Les panélistes ont convenu que le fait de demander la création d'un nouveau système de lois pour couvrir le comportement en ligne suggère que le cadre actuel ne fonctionne pas, ce qui risque de saper sa légitimité.

Cela ne veut pas dire, cependant, que le système actuel est sans problème. Les panélistes ont tous convenu que la lacune la plus difficile à combler dans les protections actuelles des droits de la personne – en ligne et hors ligne – est celle qui existe entre les protections sur papier et leur application dans la pratique. Ce manque de responsabilisation est d'autant plus flagrant en ligne qu'il n'existe pas de mesures convenues de ce qu'est la paix numérique et de la fréquence à laquelle elle est violée. Stéphane Duguin a décrit comment le CyberPeace Institute documente et mesure les cyberattaques pour comprendre comment les gens sont ciblés, quels sont les impacts sociétaux et comment les victimes peuvent obtenir recours, réparation et justice à travers les systèmes juridiques nationaux et internationaux existants.

La conclusion d'une nouvelle convention présenterait toutefois l'avantage de rassembler tous les acteurs afin de définir un cadre et un vocabulaire communs pour décrire les menaces et les protections en matière de droits de la personne. Malheureusement, étant donné le climat géopolitique actuel, les panélistes doutent que les États, la société civile, les entreprises privées et les groupes non étatiques soient en mesure d'élaborer une nouvelle convention qui résisterait aux normes juridiques actuelles : en l'absence d'un désir commun de coopération mondiale, les États risqueraient de parvenir à un accord offrant des protections insuffisantes. Dans ce contexte, il convient d'encourager et de maintenir l'intérêt du secteur privé et sa volonté de discuter de la manière de protéger ses utilisateurs contre les atteintes en ligne. Tous les intervenants ont convenu que cette volonté devait être exploitée pour relever le défi de l'application des cadres existants, en commençant par une transparence accrue sur les attaques et les mécanismes dont disposent les victimes pour obtenir recours, réparation et justice.

> « Nous devrions vraiment nous préoccuper des individus avant tout… nous n'essayons pas seulement de gérer la dynamique du pouvoir entre les États… il s'agit de protéger les personnes concernées. » – Yves Daccord

Enfin, Yves Daccord a réfléchi à la nécessité pour les organisations humanitaires de changer d'orientation pour tenir compte de la nécessité de protéger les infrastructures critiques en ligne, en plus des secteurs humanitaires classiques tels que les soins de santé ou l'eau, l'assainissement et l'hygiène. Il a avancé l'idée d'une zone neutre et impartiale du cyberespace, que les États devraient s'engager à protéger sans surveillance. M. Daccord a suggéré que les intervenants « s'organisent de manière plus agressive autour de la protection des soins de santé » à tout moment et dans tous les domaines, hors ligne et en ligne. Les panélistes ont souligné que la société civile et le secteur privé devraient sensibiliser davantage le public à l'importance de la protection des données personnelles. Ils devraient également fournir des informations plus claires sur l'efficacité des lois pour les victimes et sur la manière dont elles doivent être adaptées pour tenir compte des attaques numériques.

Panel 4 : Les attaques numériques contre les militants des droits de la personne et de la démocratie

- Melody Patry, directrice de la promotion des droits, Access Now (modératrice)
- Steven Feldstein, *Senior Fellow* au Carnegie Endowment, auteur du livre *Rise of Digital Repression*
- Bethany Allen-Ebrahimian, reporter couvrant la Chine pour Axios
- Isabel Linzer, analyste de recherche, Technologie et démocratie, Freedom House

> « L'idée qu'il existe une séparation entre les techniques d'oppression numériques et classiques est une fiction. » – Steven Feldstein

L'oppression en ligne prend sa source dans le monde réel. Un bon indicateur pour savoir si un pays utilisera des outils numériques d'oppression contre ses citoyens est que ce pays est autoritaire ou a des tendances autoritaires. En outre, l'utilisation d'outils d'oppression en ligne dépasse largement la sphère des seuls États autoritaires. Les démocraties fragiles sont également enclines à utiliser la technologie pour éroder l'espace citoyen. L'Inde, le Brésil, la Turquie, les Philippines, la Thaïlande et l'Éthiopie sont autant d'exemples dans lesquels la surveillance de masse, le contrôle intensif des médias sociaux ou la désinformation sont utilisés par l'État pour réprimer la dissidence. De nombreux dirigeants considèrent les outils numériques comme un moyen d'étendre leurs objectifs de répression. De plus, l'IA devenant moins chère, les petits gouvernements, voire les services de police locaux, peuvent acheter des programmes de surveillance des médias sociaux afin de trouver des comptes d'utilisateurs et d'éradiquer toute dissidence. Isabel Linzer a déclaré que « la démocratisation de ce type de technologie est plus importante que de discuter des produits d'espionnage sur mesure » actuellement disponibles.

Les attaques numériques ont également des conséquences dans le monde réel. Les conséquences psychologiques du harcèlement – ainsi que l'augmentation de la censure en ligne, des coupures d'Internet, et l'intensification des arrestations en réponse à l'expression politique, sociale et religieuse – impactent la capacité et la volonté des militants de continuer à agir. Le rapport *Freedom on the Net* de Freedom House suit les risques en ligne dans 65 pays et a constaté qu'en 2020, l'activité en ligne a entraîné des attaques hors ligne dans 32 pays, tandis que les critiques du gouvernement et les organisations de défense des droits de la personne ont été piratées en réponse à leur travail dans 38 pays. L'intimidation peut atteindre un point où les activistes se retirent du discours public et les panélistes ont donné des exemples de campagnes de trollage contre les activistes ouïgours. En dépit

de leur vulnérabilité aux attaques en ligne, les militants continuent d'innover et de tirer parti des possibilités offertes par les plateformes technologiques. Un exemple est celui d'une enquête récente de Buzzfeed, qui a utilisé les cartes censurées de Baidu, en Chine, pour aider à localiser les lieux de détention massive des Ouïgours, utilisant effectivement la censure comme une forme de preuve des violations des droits de la personne.

> « Si vous abusez de l'excuse de la liberté d'expression pour maintenir du contenu sur votre plateforme parce que vous ne voulez pas être légalement responsable ou investir des ressources pour éliminer la désinformation… alors vous faites partie du problème. »
> – Bethany Allen-Ebrahimian

Reflétant les discussions des débats précédents, les intervenants ont souligné le rôle de la Chine dans la prolifération des technologies oppressives dans le monde, ainsi que la complicité des entreprises technologiques basées dans les pays démocratiques occidentaux. La Chine codifie ses pratiques autoritaires dans la loi, ce qui fait qu'il est difficile pour les entreprises américaines d'éviter de s'y conformer. Les entreprises qui ont quitté le marché chinois parce qu'elles ne voulaient pas s'y conformer dès le début de leur développement, comme Google, ont exploré des pistes leur permettant de revenir sur le marché par l'intermédiaire d'interfaces distinctes, comme un moteur de recherche précensuré. Des entreprises technologiques plus jeunes, comme Zoom, ont choisi de s'y conformer, permettant ainsi à la Chine d'exercer une gouvernance extraterritoriale accrue. Bethany Allen-Ebrahimiam a cité l'exemple d'une affaire du ministère américain de la Justice qui, fin 2020, a révélé qu'un cadre de Zoom avait partagé des informations sur les utilisateurs chinois de Zoom vivant à l'étranger avec le gouvernement chinois et travaillé à la fermeture de leurs comptes. Melody Patry a noté une autre tendance consistant à offrir des incitations aux entreprises pour qu'elles embauchent du personnel local lorsqu'elles établissent des bureaux à l'étranger. Le personnel local est alors recruté comme informateurs pour l'État, fournissant des informations sur les dissidents. La sécurité du personnel local est un nouveau risque pour les entreprises qui calculent comment répondre à la demande d'un gouvernement de respecter les lois locales à caractère autoritaire.

Les panélistes ont suggéré que les organismes de la société civile offrent une formation à l'hygiène numérique et fournissent une assistance d'urgence aux militants à risque afin d'améliorer les protections. Les entreprises technologiques devraient investir dans la protection des plateformes de communication cryptées et plaider en faveur de cette protection. Elles devraient également assumer une plus grande responsabilité pour empêcher que leurs plateformes ne soient explicitement manipulées pour réprimer la dissidence. Les gouvernements démocratiques doivent restreindre l'exportation des technologies de surveillance, former les forces de l'ordre et le personnel diplomatique à prendre les plaintes au sérieux et s'efforcer de tenir les autres gouvernements responsables de leurs actes

Panel 5 : Comment unir les démocraties vis-à-vis de la technologie

- Colin Robertson, vice-président et associé, Institut canadien des affaires mondiales (modérateur)
- Kristin Lord, présidente et directrice générale, IREX
- Chris Walker, vice-recteur aux études et analyses, National Endowment for Democracy
- Thorsten Benner, cofondateur et directeur, Global Public Policy Institute

> « Nos démocraties n'échoueront pas parce que la technologie est autoritaire en soi. Elles échoueront parce que la technologie sera utilisée à des fins autoritaires. »
> – Thorsten Benner, Global Public Policy Institute

Lors d'une récente intervention à la Conférence de Munich en 2021, Joe Biden a déclaré : « Nous devons fixer les règles qui régiront le progrès technologique et le comportement dans le cyberespace, l'intelligence artificielle, la biotechnologie, afin qu'elles soient utilisées pour élever l'humanité et non pour la clouer au sol. » Depuis lors, il a signalé qu'il souhaitait organiser un sommet des démocraties, le D10, pour discuter de différentes menaces, y compris celles qui sont liées à la technologie. Les panélistes ont approuvé l'idée maîtresse de cette déclaration : les démocraties doivent travailler – tant au niveau national qu'international – à l'élaboration et à la consécration de normes conformes aux valeurs démocratiques. Faisant écho aux débats précédents, Kristin Lord a souligné l'influence néfaste de la désinformation sur les démocraties. Les démocraties peuvent – en collaboration avec des organismes de la société civile et avec les entreprises technologiques – travailler à plusieurs niveaux pour combattre cette tendance, dans les forums internationaux comme dans la politique intérieure.

À l'échelle internationale, les démocraties ont jusqu'à présent eu du mal à établir des normes régissant l'utilisation des technologies dans le respect des droits de la personne et des valeurs démocratiques. Le débat faisait écho à un débat qui avait eu lieu lors d'une édition antérieure de #RightsCity. Cette discussion portait alors, d'une part, sur les efforts diplomatiques de la Chine pour influencer les normes et standards et, d'autre part, sur la nécessité d'une meilleure application des normes et lois existantes pour protéger les principes démocratiques. Chris Walker a fait remarquer que puisque nous ne pouvons pas nous attendre à ce que les gouvernements autoritaires changent, citant son récent rapport sur le pouvoir de subversion, « il incombe aux démocraties… de stimuler la course au sommet pour s'assurer que les valeurs démocratiques animent et entourent la technologie, à la fois pour la santé de nos propres sociétés et pour la lutte plus large dans les pays qui décident de la voie à suivre ». Les panélistes ont convenu que tout prochain sommet des démocraties devrait garantir l'existence d'un mécanisme de sécurité collective qui contribue à protéger les démocraties contre la coercition politique des États autoritaires, tout en offrant un espace d'apprentissage mutuel et en amplifiant les voix prodémocratiques.

Thorsten Benner a affirmé que la lutte pour la démocratie se fera principalement sur un front intérieur. Il a présenté deux recommandations. Premièrement, les démocraties devraient adopter un programme défensif afin de s'assurer que les entreprises occidentales ne sont pas complices des régimes autoritaires, de protéger ceux qui fuient les systèmes autoritaires, d'utiliser la technologie pour mettre au jour la répression et de soutenir les poursuites judiciaires en cas de violation des droits de la personne. Deuxièmement, les démocraties devraient montrer l'exemple en utilisant la technologie pour soutenir les processus démocratiques plutôt que de les affaiblir chez elles.

> « La rapidité et la complexité avec lesquelles les ressources technologiques modernes ont frappé chacun d'entre nous représentent un fardeau extraordinaire à porter pour un seul citoyen. » – Chris Walker

À ce titre, les États devraient s'efforcer d'accroître les ressources, les connaissances et les compétences disponibles pour les citoyens. Au niveau national, les démocraties pourraient apprendre les unes des autres, en prenant notamment l'exemple de la Finlande, de l'Ukraine et du Royaume-Uni, qui mettent chacun en œuvre une approche de la sécurité numérique à l'échelle de la société. Les politiques devraient examiner comment éliminer la désinformation en partenariat avec les plateformes technologiques et comment rendre les citoyens plus résistants à la désinformation. Les panélistes ont convenu que les organismes de la société civile constituent un intervenant clé dans la réponse à cette menace et qu'elles doivent être incluses dans les discussions visant à façonner les règles nationales et internationales. Encourager la société civile à jouer un rôle plus important en tant

que traductrice et éducatrice permettra de partager la charge avec les citoyens individuels dans l'appréhension de la désinformation en ligne.

Les organismes de la société civile ont besoin d'un soutien continu, de recherches et de possibilités de mise en réseau afin de partager leur expérience et leur expertise. Cela est évidemment plus difficile dans les pays où l'espace pour l'engagement civique est réduit. L'intégration de l'éducation aux médias dans les programmes scolaires, tout en s'adressant aux populations plus âgées par l'intermédiaire des bibliothèques et d'autres moyens, comme en Suède et en Ukraine, constitue un bon exemple de changements politiques simples qui ont un impact. Kristin Lord a déclaré : « Là où je vois certaines lacunes, c'est en regardant au-delà des écoles : les jeunes ne votent pas autant, les jeunes représentent un faible pourcentage de la population, les jeunes sont moins susceptibles de transmettre de la désinformation que les personnes plus âgées, et c'est donc là que les démocraties pourraient comparer leurs démarches respectives et trouver des stratégies communes. » Elle a également noté que l'Amérique du Nord a peu d'exemples de programmes d'éducation aux médias, malgré leur succès avéré dans la lutte contre la désinformation.

> « Il ne s'agit pas seulement d'apprendre aux gens à vérifier les faits… mais aussi de reconnaître la manipulation émotionnelle. » – Kristin Lord

Les entreprises technologiques devraient être tenues responsables par l'intermédiaire d'exigences de diligence raisonnable en vertu de la législation actuelle sur les droits de la personne. Le débat a présenté une variété de points de vue sur la force que le Canada devrait avoir dans sa réponse aux menaces à la sécurité provenant de la technologie des états autoritaires – chinois ou autres. Les panélistes se sont concentrés sur le rôle potentiel de la société chinoise Huawei dans le développement du réseau 5G du Canada. Chris Walker a affirmé que le Canada doit avoir confiance dans l'intégrité de ses infrastructures. M^{me} Lord a mis en garde contre les guerres commerciales qui entraîneraient des récriminations importantes à l'encontre des entreprises occidentales désireuses d'exporter vers des pays autoritaires, tandis que M. Benner a fait valoir que la crainte de représailles économiques ne devrait pas empêcher le Canada de disposer d'infrastructures sûres et de maintenir sa souveraineté technologique.

Panel 6 : Les médias sociaux comme outil d'enquête et de poursuite contre les atrocités criminelles

- John Packer, professeur agrégé de droit, directeur du Centre de recherche et d'enseignement sur les droits de la personne, Université d'Ottawa (modérateur)
- Nick Waters, enquêteur principal, Bellingcat
- Stephanie Barbour, conseillère principale sur la violence sexuelle et sexiste, Commission internationale pour la justice et la responsabilité
- Alexa Koenig, directrice exécutive du Human Rights Center, Université de la Californie à Berkeley

> « Chaque événement physique a une répercussion dans le monde numérique. »
> – Nick Waters, Bellingcat

La technologie des téléphones intelligents et les médias sociaux sont des outils puissants pour témoigner d'atrocités criminelles comme le génocide, les crimes de guerre, les crimes contre l'humanité et le nettoyage ethnique. Les informations numériques de source ouverte destinées à soutenir les enquêtes criminelles se présentent sous de nombreuses formes : les images satellites, la documentation numérique, le matériel physique ainsi que le contenu généré par les utilisateurs

(comme les séquences vidéo et les photographies). Cependant, avec des fils de nouvelles tels que Twitter qui se renouvellent avec 6 000 microbillets par seconde, trouver des informations pertinentes est un énorme défi. Nick Waters a souligné que les données sont « en fin de compte éphémères – les vidéos sont effacées et les comptes sont supprimés… mais ce que nous avons, ce sont des fragments figés, des moments de mémoire des événements ». Il a souligné que, dans ce sens, les données numériques à source libre peuvent être incroyablement importantes.

Les intervenants ont décrit comment des organisations telles que Bellingcat, la Commission for International Justice and Accountability (CIJA) et le Human Rights Center de l'Université de Berkeley s'efforcent de rassembler, d'analyser et de préserver les preuves en ligne afin qu'elles puissent être utilisées devant les tribunaux comme éléments de preuve dans le cadre d'enquêtes futures sur des atrocités criminelles. Stephanie Barbour a expliqué que la CIJA s'est concentrée sur la collecte de preuves de crimes de guerre, de crimes contre l'humanité et de génocide en Syrie. La Commission utilise les preuves numériques dans le cadre d'un ensemble plus large de preuves qui peuvent contribuer à l'élaboration des dossiers. Les preuves numériques peuvent fournir des indices sur les points sur lesquels les enquêtes doivent se concentrer, aider à cartographier la structure et les politiques des organisations coupables et servir de matériel de corroboration pour les sources plus classiques.

Alexa Koenig a présenté le travail du Human Rights Center, qui a donné des conseils sur les normes et les protocoles pour la collecte de preuves numériques en réponse à l'approche *ad hoc* des juges pour autoriser ce type de preuves au tribunal. Le protocole de Berkeley sur les enquêtes sur les sources numériques libres décrit un processus en trois étapes pour vérifier le contenu en ligne et réduire au minimum les préjugés. Il comprend l'analyse :

- des données techniques attachées à l'information, telles que les métadonnées ou les données de sortie derrière les images de l'enregistrement des photos, comme le dispositif, la date et les coordonnées;
- des sources et de la fiabilité, par exemple en analysant qui est la source et dans quelle mesure cette information est cohérente avec le reste du contenu de son fil;
- du contenu, par exemple en examinant la cohérence des preuves avec le contexte connu et en les triangulant avec d'autres formes de preuves telles que l'imagerie satellite et les témoignages.

L'utilisation de données à code source libre pose également des problèmes éthiques. Souvent, la source originale des données n'est pas connue, pas plus que l'identité des personnes figurant sur les photos ou les vidéos, ce qui rend difficile la protection de la vie privée et l'utilisation consensuelle des preuves. M. Waters a fait remarquer que même lorsque la source n'est pas connue, certains contenus peuvent toujours être considérés comme étant d'intérêt public. M^{me} Barbour a déclaré que l'approche de la CIJA consistait à examiner chaque élément de preuve individuellement, au cas par cas. Cela était particulièrement vrai lorsqu'il s'agissait de documenter la preuve d'atrocités criminelles, comme les crimes sexuels et sexistes, puisque les victimes se trouvent dans une situation vulnérable et que les normes juridiques actuelles n'imposent pas aux victimes la charge de prouver que des violences sexuelles ont eu lieu.

> « Le profil de la pratique et du droit en la matière évolue et change constamment, tout comme les documents que nous présentons aux juges; il est donc très difficile de prévoir quelles seront les réactions. » – Stephanie Barbour

M[me] Koenig a présenté une typologie développée par le Human Rights Center pour aider les enquêteurs à résoudre la question du consentement dans les enquêtes numériques. Afin d'aider les enquêteurs dans le traitement des informations numériques, cette approche s'appuie sur un cadre éthique, axé sur trois principes essentiels : la prise en compte des exigences légales en matière de consentement dans chaque cas, la prise en compte des codes professionnels de l'enquêteur individuel – qu'il s'agisse d'un avocat, d'un analyste de données ou d'un chercheur universitaire – et la prise en compte des normes et pratiques émergentes dans ce domaine. Ces dernières se répartissent entre : les exigences en matière de droits de la personne, l'exactitude et la qualité des informations, et les questions de sécurité physique, numérique et psychologique soulevées par l'utilisation des informations. Ce cadre peut aider les enquêteurs à s'orienter dans les questions éthiques liées à la vie privée et au consentement.

Tous les panélistes se sont montrés favorables quant à l'admissibilité d'informations bien traitées devant les tribunaux. Et ils semblaient optimistes vis-à-vis du rôle que les preuves numériques pourraient jouer à l'avenir dans la lutte contre les atrocités criminelles.

Panel 7 : La lutte contre les discours de haine sur Internet

- Naomi Kikoler, directrice du Centre Simon-Skjodt pour la prévention des génocides, United States Holocaust Memorial Museum (modératrice)
- Silvia Fernandez, présidente, Global Action Against Mass Atrocity Crimes
- Fernand de Varennes, rapporteur spécial des Nations Unies pour les minorités
- Iain Levine, conseiller principal en matière de droits de la personne, Facebook

> « Aucune société n'est à l'abri des discours de haine. » – Silvia Fernandez, Global Action Against Mass Atrocity Crimes

Naomi Kikoler a entamé la discussion en décrivant la reconnaissance croissante du discours de haine comme précurseur des atrocités criminelles. À l'instar des outils de communication classiques, tels que la radio ou les brochures, les médias sociaux ont montré qu'ils étaient capables d'amplifier l'intolérance et les préjugés pour créer un environnement où les discours et les crimes haineux sont possibles. Fernand de Varennes, rapporteur spécial des Nations Unies pour les minorités, a souligné que les groupes minoritaires sont la cible principale des discours et des crimes haineux. Au Sri Lanka, au Myanmar, en Inde et ailleurs, la haine en ligne contre les minorités est en hausse, tout comme l'antisémitisme mondial. M. de Varennes a déclaré qu'« il est difficile de prétendre que la technologie est une force du bien dans ces conditions, si nous lui permettons d'être le support du mal ».

M. de Varennes a appelé les sociétés de médias sociaux à reconnaître que la haine est le plus souvent dirigée contre les minorités afin de renforcer leur réponse, par exemple en fournissant des données désagrégées pour permettre aux analystes de mieux comprendre qui sont les groupes vulnérables et comment ils peuvent être protégés. Il a également soutenu qu'il fallait mieux définir dans quelle mesure l'hébergement de propagande haineuse engage la responsabilité des entreprises de médias sociaux, déclarant qu'« aucune entreprise ne devrait être à l'abri du mal auquel elle contribue directement ». Un rapport des Nations Unies sur les violences au Myanmar a révélé que Facebook avait été utilisé pour diffuser la haine et inciter à des attaques contre la minorité rohingya en 2017. Iain Levine, de Facebook, a admis, d'une part, que la plateforme avait honte du rôle qu'elle avait joué, et décrit, d'autre part, la nouvelle approche de Facebook en matière de droits de la personne. Une nouvelle politique en matière de droits de la personne éclaircit les responsabilités de l'entreprise dans le cadre des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, et définit les engagements pris à l'égard des conventions internationales en matière de droits de la

personne. Le déploiement de la politique est complété par une formation pour les modérateurs de contenu. Un défi majeur pour l'application et l'exécution est l'échelle à laquelle Facebook travaille : il y a plus de 1,8 milliard d'utilisateurs, et 100 milliards de contenus sont téléversés sur le site chaque jour. M. Levine a souligné la nouvelle approche de Facebook à l'égard du Myanmar pendant le coup d'État actuel, au cours duquel l'entreprise a retiré la Tatmadaw (les forces armées birmanes) de la plateforme, invoquant les responsabilités qui lui incombent en vertu des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme.

Bien que le problème soit de plus en plus reconnu, on manque encore de recherches visant à comprendre les processus qui mènent de la discrimination aux discours haineux, puis aux crimes haineux. Il n'existe pas de définition commune du discours de haine, bien qu'il soit généralement illégal lorsqu'il incite directement à la violence. Cependant, les discours utilisés pour créer un environnement propice à la haine et à la violence n'ont pas encore fait l'objet de législations. Les panélistes ont convenu que savoir comment définir le discours de haine et ses précurseurs sans porter atteinte à la liberté d'expression est actuellement la question la plus pressante pour ceux qui travaillent dans le domaine.

> « Les mécanismes de suppression de contenu ne fonctionnent pas toujours aussi bien pour les minorités qu'ils le devraient… malheureusement, les modérateurs de contenu peuvent eux-mêmes avoir des préjugés contre ces minorités. » – Fernand de Varennes

L'absence de définition pour les discours précédant l'incitation à la violence est une pierre d'achoppement pour la coopération des États en matière de prévention des atrocités criminelles. Silvia Fernandez a néanmoins décrit les efforts du réseau Global Action Against Mass Atrocity Crimes (GAAMAC), qui s'efforce de « pratiquer une culture de la prévention » parmi ses membres. Le GAAMAC a conscience de l'importance des discours de haine en tant qu'indicateurs de potentielles atrocités criminelles et discute des outils disponibles pour y répondre. Le rôle que l'éducation pourrait jouer pour donner aux gens les moyens de reconnaître les discours de haine nécessite des recherches plus approfondies, tout comme le travail des organisations qui diffusent des contre-récits. Ian Levin a présenté le partenariat noué par Facebook avec Defy Hate Now au Soudan du Sud, en Éthiopie et au Cameroun pour reconnaître la désinformation dans les langues locales sur le réseau social et apprendre aux communautés locales à reconnaître et à contrer les discours de haine.

Une autre réponse possible consiste à réprimer les discours de haine. M^{me} Fernandez a souligné la nécessité d'une définition claire du discours de haine afin que la répression ne porte pas atteinte à la liberté d'expression. Tous les intervenants ont souligné l'importance du Plan d'action de Rabat, qui définit les principes permettant de faire la distinction entre la liberté d'expression et l'incitation à la haine. Les panélistes ont convenu que ces principes sont cruellement sous-utilisés. Le plan d'action présente un test d'acceptabilité en six parties, qui prend en compte le contexte, le statut de l'intervenant, l'intention, le contenu, l'étendue de la diffusion et la probabilité de préjudice.

Sur Facebook, le contenu est régi par les Standards de la communauté. Quatre-vingt-dix-sept pour cent du contenu qui ne respecte pas ces normes est supprimé automatiquement par un algorithme. Le reste du contenu signalé comme étant abusif est suivi par des modérateurs de contenu humains, qui décident de ce qui est autorisé ou non sur le site. M. Levine a reconnu que l'entreprise doit aller plus loin que la simple suppression de contenu pour pouvoir s'attaquer à la désinformation et aux fausses informations, par exemple en créant des liens vers des informations crédibles pour promouvoir des contre-récits. M. de Varennes a souligné qu'il fallait, d'une part, évaluer la partialité des modérateurs et, d'autre part, les former pour les sensibiliser aux vulnérabilités particulières des groupes minoritaires et à la manière dont ils sont ciblés en ligne.

Les panélistes ont toutefois fait remarquer que les approches individuelles ne suffisent pas à combattre la menace des discours haineux en ligne. Les États, le secteur privé et la société civile doivent se mettre d'accord sur une approche mondiale et juridiquement contraignante qui assure un équilibre entre la liberté d'expression et la protection contre les discours haineux, établit la responsabilité des entreprises de médias sociaux, améliore la modération des contenus et s'engage à protéger les minorités. Bien qu'il existe une volonté politique croissante de s'attaquer au problème, les efforts restent cloisonnés à certaines entreprises et certains pays. Pourtant, la résolution de ce problème est d'autant plus importante face à la propagation de l'autoritarisme et à l'utilisation de ce flou par des gouvernements autoritaires pour réprimer la dissidence et limiter la liberté d'expression tant dans leur propre pays qu'à l'étranger.

Conclusions

Les normes, lois et règles qui régiront le comportement des États, des particuliers et des entreprises en ligne sont contestées quotidiennement. Deux camps se dessinent : d'un côté, l'autoritaire, et de l'autre, le démocratique. Tous deux se livrent depuis cinq ans à un bras de fer centré sur l'utilisation des outils numériques. Jusqu'à récemment, les États démocratiques ont fait preuve de complaisance face aux investissements chinois visant à influencer la création de normes pour les activités en ligne, parallèlement à des efforts plus larges visant à saper le système international des droits de la personne et à réduire l'espace citoyen. Les États démocratiques ont mis du temps à reconnaître et à comprendre la manière dont le fonctionnement actuel de la technologie en ligne influence l'accès des citoyens à l'information et la façon dont la population aborde cette information. Les médias sociaux influencent les affaires publiques et l'élaboration des politiques, en amplifiant l'influence des individus et des problèmes d'une manière tout simplement impossible auparavant. Les avancées de l'intelligence artificielle permettent aux États et aux entreprises de rassembler de vastes quantités de données sur les citoyens et les utilisateurs.

Ces progrès technologiques prennent de court les gouvernements et la société civile : le temps manque pour analyser leur impact et convenir des protections adéquates contre leurs abus. Les normes convenues pour réglementer le comportement national et international en ligne sont en retard sur les changements, ce qui crée un environnement dans lequel les droits des citoyens peuvent être violés. La conception même du monde en ligne, dans lequel la simplification, le mélodrame et la polarisation sont récompensés, et où l'accès aux données personnelles des utilisateurs est vendu à profit, crée un environnement propice aux violations des droits de la personne.

Il est essentiel de reconnaître que le comportement en ligne a des origines et des conséquences dans le monde réel. La façon dont les États, les entreprises et les particuliers abordent la conception, l'utilisation et le partage des outils numériques s'aligne sur leurs identités, stratégies et actions hors ligne. Les protections des droits de la personne en place pour les individus en ligne ne doivent pas être moins fondamentales ou moins valables que hors ligne. Bien que le présent document ne s'intéresse qu'aux manifestations en ligne des violations des droits de la personne, il est évident que toute stratégie visant à protéger ces droits et les valeurs démocratiques sur Internet doit s'accompagner d'actions hors ligne.

Recommandations

Sur le plan international, le gouvernement du Canada devrait :

- travailler par toutes les voies diplomatiques disponibles pour renforcer l'application du droit international des droits de la personne et du droit international humanitaire. Au minimum,

les services de santé devraient être protégés contre les attaques physiques et numériques tant en période de conflit qu'en temps de paix;
- diriger et soutenir les efforts internationaux visant à interdire les technologies de surveillance intrusives, telles que la reconnaissance faciale;
- considérer l'élaboration d'une sanction internationale visant à restreindre l'accès aux équipements nécessaires à la production de processeurs afin de limiter les capacités répressives des gouvernements autoritaires;
- contribuer activement aux discussions et débats internationaux sur la gouvernance démocratique en ligne – soutenir le développement d'une compréhension et d'un langage communs des normes de comportement en ligne, plaider pour une meilleure application du droit international existant, accroître le rayonnement et l'utilisation du Plan d'action de Rabat, encourager la conception démocratique des plateformes en ligne, renforcer la responsabilité des entreprises technologiques hébergeant des discours haineux, et protéger la vie privée et les données personnelles.

Au niveau national, le gouvernement du Canada devrait :

- élaborer un plan d'action à l'échelle de la société avec les gouvernements provinciaux pour renforcer la résilience du public face à la désinformation en ligne, notamment en intégrant un programme d'éducation aux médias dans les programmes scolaires;
- considérer – en plus des utilisations militaires – les utilisations civiles potentielles de la technologie, et donc limiter l'exportation de technologies qui pourraient faciliter la répression étatique;
- protéger la sécurité des infrastructures et des institutions canadiennes en fournissant aux entreprises et aux institutions canadiennes des conseils plus détaillés sur les critères de sécurité des partenariats et des importations;
- offrir un financement accru aux organisations et aux établissements d'enseignement supérieur canadiens qui entreprennent des recherches et des programmes dans le domaine de la technologie numérique, de ses impacts sur la société, de ses implications et applications légales, et de l'augmentation des protections pour les citoyens et les activistes en ligne.

Les entreprises canadiennes de médias sociaux et de technologie devraient :

- élaborer des politiques claires de diligence raisonnable en matière de droits de la personne pour guider le développement, l'utilisation et l'exportation de technologies, conformément aux principes directeurs des Nations Unies en matière de droits de la personne;
- investir dans la protection des données et plaider en sa faveur, notamment en protégeant les plateformes de communication cryptées;
- assumer davantage de responsabilités dans les situations où les plateformes sont explicitement manipulées à des fins de répression ou de désinformation, et apporter des changements qui renforcent la sécurité du public canadien et les normes mondiales en matière de droits de la personne.

Les universités et instituts de recherche canadiens devraient :

- élaborer des critères éthiques clairs pour guider la prise de décision concernant les partenariats universitaires avec des entités basées dans des États autoritaires;

- examiner les partenariats actuels avec des entités basées dans des États autoritaires afin d'explorer les vulnérabilités et le potentiel de complicité dans la répression autoritaire ou les violations de la confidentialité des données.

La société civile canadienne devrait :

- informer le public canadien au sujet des données personnelles et de l'importance de les protéger;
- fournir une formation à l'hygiène numérique et une aide d'urgence aux militants à risque;
- promouvoir et développer des programmes d'éducation aux médias pour aider les Canadiens à reconnaître la désinformation.

Le présent rapport a été rédigé par Alexandra Buskie, consultante, pour l'Institut montréalais d'études sur le génocide et les droits de la personne de l'Université Concordia.

Cette conférence a été en partie sponsorisée par le ministère de la Défense nationale.