CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

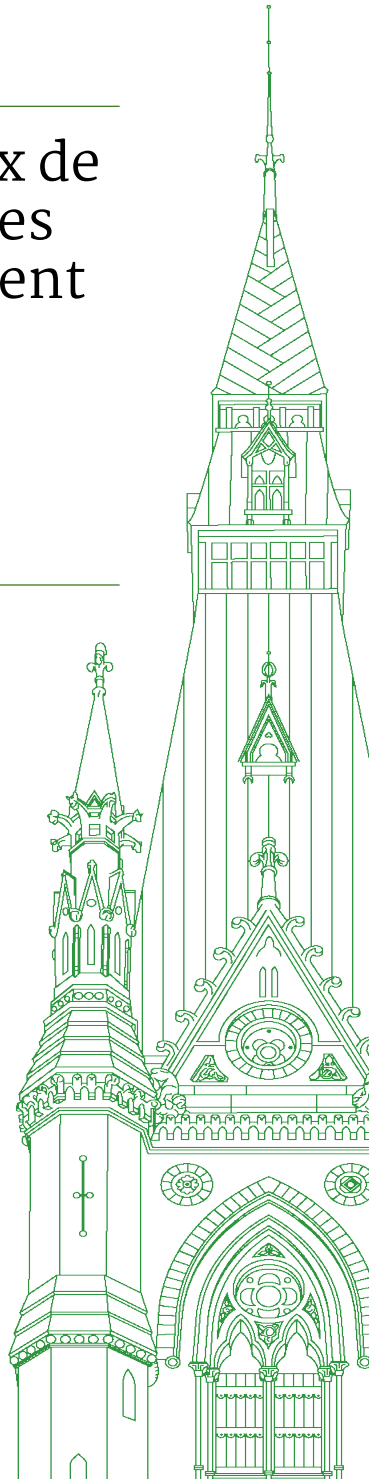
45e LÉGISLATURE, 1re SESSION

Sous-comité des droits internationaux de la personne du Comité permanent des affaires étrangères et du développement international

TÉMOIGNAGES

NUMÉRO 025

Le lundi 26 octobre 2026



Président : Fayçal El-Khoury

Sous-comité des droits internationaux de la personne du Comité permanent des affaires étrangères et du développement international

Le lundi 26 octobre 2026

● (1540)

[*Français*]

Le président (Fayçal El-Khoury (Laval—Les Îles, Lib.)): J'ouvre maintenant la séance.

Bienvenue à la 25e réunion du Sous-comité des droits internationaux de la personne du Comité permanent des affaires étrangères et du développement international de la Chambre des communes.

[*Traduction*]

Conformément à la motion adoptée par le Comité permanent des affaires étrangères et du développement international le mardi 23 septembre 2025 et à la motion adoptée par le Sous-comité le lundi 5 octobre 2026, le Sous-comité entreprend son étude des répercussions mondiales de l'intelligence artificielle sur les mouvements de défense des droits de la personne.

[*Français*]

La réunion d'aujourd'hui se déroule sous forme hybride. Conformément au Règlement, les députés peuvent participer en personne ou par l'intermédiaire de l'application Zoom.

[*Traduction*]

Avant d'accueillir notre invité, je tiens à préciser ceci: le greffier a distribué, le 23 octobre, trois projets de budget concernant les études suivantes. Concernant l'étude de la situation des droits de la personne en Chine, le budget s'élève à 7 750 $. Concernant l'étude des répercussions mondiales de l'intelligence artificielle sur les mouvements de défense des droits de la personne, le budget s'élève à 7 750 $. Concernant la séance d'information sur la violence fondée sur le genre à l'égard des femmes ukrainiennes dans le contexte du conflit russo-ukrainien, le budget s'élève à 5 900 $.

Plaît-il au Comité d'adopter ces trois budgets?

Des députés: D'accord.

Le président: Merci.

Je voudrais maintenant souhaiter la bienvenue à notre invité pour la première série de questions et réponses.

Nous avons le plaisir d'accueillir M. Jean-Noé Landry, boursier de la Fondation Obama et directeur, Pôle de données fédérées, Institut de la résilience et de l'innovation urbaine.

M. Landry se joint à nous par visioconférence. À vous la parole pour un maximum de cinq minutes, je vous prie.

Jean-Noé Landry (boursier de la Fondation Obama et directeur, Pôle de données fédérées, Institut de la résilience et de l'innovation urbaine, à titre personnel): Monsieur le président, chers membres du Sous-comité, je vous remercie de m'avoir invité.

Depuis plus de deux décennies, je travaille aux côtés de mouvements démocratiques et d'organisations de la société civile dans des pays tels que la Serbie, la Russie, la Tunisie, le Kenya, et l'Ukraine. J'ai ensuite dirigé Open North, un organisme canadien de premier plan qui œuvre à l'échelle internationale en faveur de la gouvernance démocratique grâce aux données et à la technologie. Comme vous l'avez souligné, monsieur le président, mon travail porte principalement sur les infrastructures de données responsables, les modèles de données fédérés, l'intelligence artificielle, ainsi que sur la responsabilité démocratique.

Le message central que je souhaite vous transmettre aujourd'hui est le suivant: l'intelligence artificielle ne se contente pas d'introduire de nouveaux risques et de nouvelles opportunités pour les défenseurs des droits de la personne; elle modifie en profondeur la répartition du pouvoir politique, et notre action internationale en faveur de la démocratie doit s'adapter en conséquence.

Permettez-moi de soulever trois points. Premièrement, l'intelligence artificielle modifie la dynamique économique de la répression. Des activités qui nécessitaient autrefois d'importantes ressources publiques, telles que la surveillance des réseaux politiques, l'analyse des communications, l'identification des militants, ainsi que la manipulation du discours public, peuvent désormais être de plus en plus automatisées et déployées à grande échelle. Pour les gouvernements qui contrôlent déjà les infrastructures de surveillance et les données personnelles existantes, l'intelligence artificielle constitue un puissant multiplicateur de leur pouvoir actuel.

La société civile est confrontée à une réalité très différente. Les organismes de défense des droits de l'homme manquent souvent de l'expertise technique, des infrastructures et des ressources nécessaires pour se protéger, sans parler de rivaliser avec ces capacités. Nous entrons désormais dans un monde où la capacité de répression devient de plus en plus évolutive, tandis que les ressources disponibles pour y résister se réduisent. Ce n'est pas un problème qui peut être résolu simplement en distribuant ou en déployant davantage d'outils d'intelligence artificielle auprès de chaque organisation.

Deuxièmement, nous devons repenser ce que signifie la responsabilité démocratique à l'ère de l'intelligence artificielle. Au cours des 20 dernières années, le mouvement international pour un gouvernement ouvert, dont le Canada a été l'un des principaux acteurs, a réalisé des progrès considérables en matière d'ouverture des archives publiques, d'établissement de normes de transparence, et de renforcement de l'accès de la société civile à l'information. Toutefois, la publication de ce type de renseignements n'est qu'un début. Le prochain défi à l'ère de l'intelligence artificielle consiste à rendre ces renseignements exploitables à des fins de reddition de comptes.

Prenons l'exemple de la Hongrie. Dans ce pays, des milliers de déclarations de patrimoine de parlementaires existent sous forme de documents numérisés, parfois manuscrits. Grâce au travail mené en collaboration avec la communauté internationale pour la transparence gouvernementale, le traitement assisté par l'intelligence artificielle a permis de transformer près de 4 000 déclarations, voire davantage, en informations structurées pouvant être recherchées, comparées et mises en correspondance. Le recoupement de ces données avec, par exemple, les informations sur la propriété des entreprises et les marchés publics pourrait permettre à des enquêteurs indépendants d'identifier des conflits d'intérêts potentiels qui, sans cela, resteraient difficiles à détecter.

Cela met en évidence une opportunité plus large: passer d'une transparence fondée sur l'accès à l'information à une transparence fondée sur la capacité à enquêter et à agir. Néanmoins, cela soulève également d'importantes questions concernant la propriété des données, leur sécurité, et la reddition de comptes. Ces capacités doivent être au service de la société civile locale, et non pour générer de nouvelles dépendances vis-à-vis de gouvernements étrangers ou de fournisseurs de technologies commerciales.

Troisièmement, le gouvernement canadien devrait aller au-delà du simple financement de projets technologiques isolés pour s'orienter vers la mise en place d'infrastructures démocratiques partagées, et je suggère d'établir trois priorités.

Tout d'abord, il faut mettre en place une capacité internationale durable en matière de responsabilité démocratique, en associant l'expertise canadienne en matière d'intelligence artificielle à des réseaux de la société civile reconnus à l'échelle internationale, afin de soutenir les enquêtes, la surveillance institutionnelle, et les réponses rapides face aux menaces émergentes pour la démocratie. Bref, nous devons allier la dimension humaine aux nouvelles capacités technologiques.

Ensuite, nous devons investir dans des infrastructures d'intérêt public partagées, des environnements de données sécurisés, des outils interopérables, des capacités d'analyse multilingues, et une expertise technique auxquels les organisations puissent avoir accès sans avoir à tout mettre en place de manière indépendante.

Enfin, faire en sorte que l'appropriation locale et la responsabilité démocratique soient des principes non négociables. Les partenaires internationaux doivent contribuer à définir les priorités, régir l'accès à l'information et garder le contrôle des données sensibles. Les conclusions issues de l'intelligence artificielle doivent rester vérifiables et soumises au jugement humain.

Pour conclure, le gouvernement du Canada a investi massivement dans la recherche et l'innovation en matière d'intelligence artificielle. La question est désormais de savoir si nous pouvons transformer une partie de cette capacité en une contribution durable à la résilience démocratique internationale. Je dirais que nous ne devrions pas mesurer le succès à l'aune du nombre de projets d'intelligence artificielle financés, mais plutôt en fonction de la capacité des mouvements démocratiques à acquérir des moyens durables pour lutter contre les abus de pouvoir, et demander des comptes aux institutions.

Je vous remercie, et j'ai bien hâte de répondre à vos questions.

● (1545)

Le président: Merci, monsieur Landry. Nous passons maintenant à la période des questions et réponses. C'est M. Majumdar qui va commencer.

Vous disposez de sept minutes.

Shuvaloy Majumdar (Calgary Heritage, PCC): Merci beaucoup, monsieur le président.

Je vous remercie de votre témoignage. J'ai remarqué que vous avez déjà travaillé au National Democratic Institute. Pour ma part, j'ai déjà travaillé à l'International Republican Institute. À ce titre, je sais que vous avez accompli un travail assez impressionnant auprès de dissidents du Kremlin, à Moscou, en Russie. J'aimerais approfondir cet aspect.

Vous avez travaillé aux côtés de dirigeants prodémocratie, ou de militants en faveur de réformes démocratiques, dans des sociétés fermées. Quelles avancées avons-nous observées quant à l'utilisation de la reconnaissance faciale par le Kremlin, le Parti communiste chinois et le Corps des gardiens de la révolution islamique pour l'identification des dissidents, non seulement sur leur propre territoire — dans leurs pays respectifs —, mais aussi à l'échelle internationale?

Premièrement, d'après vos observations, dans quelle mesure ces technologies sont-elles utilisées? Deuxièmement, comment ces technologies contribuent-elles à la répression transnationale et à l'ingérence de ces gouvernements dans d'autres pays, y compris le nôtre?

Jean-Noé Landry: C'est une bonne question. Je dois toutefois préciser que mon expérience en Russie remonte à 2005 et 2006, soit bien avant la plupart des avancées que nous observons actuellement. Cela dit, comme vous le savez sans doute en raison de votre propre expérience à l'international, c'est souvent dans de tels contextes que certaines de ces technologies sont déployées et mises à l'essai, puisque les gouvernements y consacrent les moyens et les ressources nécessaires. Les mêmes contraintes démocratiques ne sont pas à l'œuvre, d'où l'absence d'un droit de regard parlementaire comme celui que vous exercez aujourd'hui.

Je ne peux pas parler de l'utilisation de ces technologies en 2005 et 2006, puisqu'elles n'existaient tout simplement pas. Cependant, je dirais que les fondements mêmes de la répression visant l'espace démocratique ont créé les conditions propices à un déploiement intensif de ces technologies, sans véritable encadrement de leur évolution. Par exemple, dans un pays comme la Russie, il est très difficile de savoir quelles entreprises reçoivent du financement et pour quels projets, car on n'y trouve pas les mêmes exigences de reddition de comptes que dans une société dite ouverte.

Vous soulevez un point important en établissant un lien avec les organisations locales qui sont soumises à ce genre de capacités de surveillance. Ce que nous constatons actuellement — à la lumière de votre expérience à l'IRI et de la mienne au NDI —, c'est que nous n'assistons pas seulement au recul des démocraties; nous subissons également les effets de la réduction des investissements consacrés au développement international et destinés à appuyer ces réseaux démocratiques. Les personnes qui disposaient auparavant de tribunes leur permettant de discuter des répercussions de la surveillance et de mettre en commun leurs expériences n'ont plus nécessairement les moyens de le faire. Selon moi, il s'agit là d'une occasion pour le Canada de faire preuve de leadership en contribuant à préserver cet espace pour les organisations de la société civile grâce au renforcement de réseaux qui peinent à trouver les ressources nécessaires pour dépasser leur cadre national et tisser des liens à l'échelle internationale.

Les organisations qui assuraient autrefois ce type de coordination multilatérale éprouvent aujourd'hui beaucoup de difficultés à fournir les moyens de maintenir ces échanges. Pour ma part, je m'en remets toujours aux organisations locales qui subissent directement ces formes de répression plutôt qu'à des analyses générales sur les mesures à prendre.

En tant que puissance moyenne, le Canada jouit de la crédibilité nécessaire pour mobiliser ses capacités, ses chercheurs et ses entreprises dans le domaine de l'intelligence artificielle afin d'entretenir des échanges techniques avec des organisations sur le terrain. Nous pourrions faire beaucoup plus à l'échelle internationale en misant sur l'expertise canadienne en intelligence artificielle, si le Canada est prêt à s'engager dans cette voie.

● (1550)

Shuvaloy Majumdar: Quelles possibilités l'essor de l'intelligence artificielle offre-t-il aujourd'hui non seulement aux réformateurs prodémocratie dans les sociétés répressives, mais aussi à leurs défenseurs et alliés ici au Canada, afin que leurs efforts puissent être amplifiés? Il n'est probablement pas exagéré de dire que les outils dont les réformateurs prodémocratie se servent depuis une vingtaine d'années pour s'organiser commencent à accuser leur âge, alors que ceux qu'utilisent les régimes autoritaires pour exercer leur répression sont désormais à la fine pointe de la technologie.

En ce qui concerne les différentes façons dont l'intelligence artificielle peut aider les défenseurs de la liberté à mieux s'organiser et à mieux faire valoir leur cause, quels principes directeurs proposeriez-vous pour guider cette démarche?

Jean-Noé Landry: L'un des grands sujets de l'heure est celui de l'intelligence artificielle de source ouverte. C'est bien beau d'avoir accès au code et aux algorithmes, mais encore faut-il savoir quoi en faire par la suite. Comment interpréter des modèles de données très complexes et sophistiqués? Comment suivre la transformation des données et en assurer la traçabilité, depuis leur intégration à ces modèles jusqu'à la production de résultats analytiques?

Pour bien comprendre l'intelligence artificielle, il faut d'abord bien comprendre les données, c'est-à-dire savoir les interpréter et acquérir non seulement les réflexes, mais aussi les compétences nécessaires pour assurer la traçabilité des décisions découlant du croisement de multiples sources de données.

Dans la Stratégie nationale en matière d'intelligence artificielle du Canada, on parle d'une intelligence artificielle accessible à tous. À mon avis, bon nombre des principes qui y sont énoncés peuvent être transposés à une approche canadienne d'investissement en faveur de la démocratie à l'échelle internationale.

Je mentionnerais aussi l'interopérabilité des données. Il existe déjà des sources de données, mais les volumes en cause sont extrêmement difficiles à gérer en raison de leur ampleur. Qu'il s'agisse de déclarations d'actifs, de registres d'entreprises, de renseignements sur la propriété effective, de données sur les marchés publics, de registres électoraux ou encore de modifications apportées aux lois et aux règlements, nous avons maintenant la capacité de regrouper toutes ces informations. Du point de vue d'un militant ou d'un réformateur prodémocratie, ces capacités représentent un atout considérable, non seulement pour la société civile, mais aussi pour les diplomates canadiens à l'étranger.

À cela pourrait s'ajouter l'intelligence humaine issue de l'expérience internationale de nos spécialistes canadiens, ce qui permettrait de bonifier nos capacités en intelligence artificielle. C'est l'interopérabilité humaine, c'est-à-dire notre façon de voir le monde et de mettre les choses en contexte, qui vient éclairer les analyses produites par l'intelligence artificielle, lesquelles réunissent d'énormes quantités d'informations à une échelle sans précédent.

Le président: Merci, monsieur Majumdar.

Je cède maintenant la parole à Mme Vandenbeld. Vous disposez de sept minutes.

Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci beaucoup, monsieur le président.

Merci, monsieur Landry, d'être des nôtres. L'une de vos observations a particulièrement retenu mon attention. Vous avez dit que l'intelligence artificielle a un effet multiplicateur sur le pouvoir existant. Ainsi, dans le cas d'un État répressif ou d'un État de surveillance, l'intelligence artificielle ne fait qu'amplifier sa capacité de répression. Or, si je vous comprends bien, la société civile et les réseaux de défenseurs des droits de la personne disposent aujourd'hui de moins de ressources. Il en résulte donc un déséquilibre. Est-ce bien cela?

Vous dites également que nous devons investir dans certains mécanismes de la société civile afin de permettre aux organisations qui en font partie d'évoluer à armes égales et de demander des comptes à ces régimes. Est-ce exact?

Jean-Noé Landry: Oui, tout à fait. C'est pourquoi je recommande également que le gouvernement du Canada évite de concentrer ses investissements uniquement sur des projets ponctuels. Il devrait aussi investir dans l'infrastructure, l'interopérabilité, l'amélioration de l'accès aux données, ainsi que la capacité de la société civile à interpréter ces données.

Le Canada a aujourd'hui la crédibilité, le leadership et la marge de manœuvre nécessaires pour jouer un rôle qu'il n'aurait peut-être pas pu assumer auparavant, parce qu'un plus grand nombre d'acteurs intervenaient déjà dans ce domaine. À mes yeux, il s'agit là d'une occasion à saisir.

● (1555)

Anita Vandenbeld: Lorsque vous parlez d'infrastructure démocratique commune, la plupart des pays envisagent cette notion sous l'angle de leur propre souveraineté: par exemple, la mise en place d'une intelligence artificielle souveraine, l'exploitation de leurs propres centres de données, etc. Pour votre part, comment concevez-vous une telle infrastructure du point de vue de la démocratie et des droits de la personne à l'échelle mondiale?

Jean-Noé Landry: Je la conçois sous l'angle du gouvernement ouvert, puisque c'est mon domaine d'expertise. J'entends par là des ensembles de données fondamentaux, à forte valeur ajoutée, qui varient considérablement d'un pays à l'autre. Même lorsqu'il existe des exigences concernant, par exemple, l'échange et l'accessibilité des données, comme c'est le cas dans l'Union européenne, les champs de données ne sont pas nécessairement définis de la même façon. La structure et le format des données peuvent également varier. Il existe toutefois des pratiques exemplaires permettant d'uniformiser les infrastructures sous-jacentes de l'espace numérique, qui sont nécessaires au fonctionnement des mouvements démocratiques.

Grâce à la compréhension accrue que procurent les analyses issues de l'intelligence artificielle, les activités de défense des droits peuvent être mieux étayées et mieux fondées. Je considère les infrastructures numériques sous-jacentes comme un domaine sur lequel le Canada pourrait miser de façon stratégique. Cela contribuerait à renforcer la liberté des médias, les parlements ouverts et les partis politiques. Tous ces piliers de la démocratie reposent aujourd'hui sur ces infrastructures numériques.

Anita Vandenbeld: Vous parlez aussi de capacité. Nous savons que le Canada dispose d'une vaste expertise. Nos spécialistes peuvent gérer d'importantes quantités de données. Toutefois, pour un défenseur des droits de la personne sur le terrain, que ce soit en Afghanistan ou au Venezuela, il est beaucoup plus difficile de gérer ces données et de tirer parti de l'infrastructure démocratique dont vous parlez.

Comment nous y prendrions-nous pour les doter d'une telle capacité?

Jean-Noé Landry: Oui, c'est difficile, car il faut toujours éviter de créer plus de concurrence ou de miser sur une seule organisation qui recevrait la formation nécessaire pour accomplir ce que l'on juge utile. C'est pourquoi la grande diversité des Canadiens ayant travaillé à l'étranger est si précieuse. Ces personnes peuvent nous aider à contextualiser la façon dont le Canada pourrait intervenir ou apporter son soutien à l'échelle locale.

J'invite le Sous-comité à trouver des moyens de mobiliser cette expertise canadienne — ces personnes qui peuvent servir de médiateurs et qui comprennent mieux le contexte local —, en plus ou en complément du travail accompli par nos missions diplomatiques et nos ambassades. Il faudrait ensuite chercher à établir des partenariats avec les acteurs de la société civile qui subissent de plein fouet les effets de ces outils de surveillance. Je répète qu'il faut aller au-delà d'une approche axée sur des projets ponctuels. Si les États répressifs multiplient leurs moyens de répression, nous devrions peut-être nous tourner vers des technologies de source libre qui ont démontré une grande résilience. Il faut également examiner comment investir dans des infrastructures qui peuvent être mises en commun et profiter à de multiples organisations de manière systémique, plutôt que de concentrer nos efforts sur un seul organisme d'observation des élections ou de défense des intérêts. Le Canada peut réaliser des investissements dans les infrastructures numériques sous-jacentes qui auraient des retombées systémiques beaucoup plus importantes.

Anita Vandenbeld: L'un des désavantages des projets de développement et de renforcement des capacités est leur lenteur. Vous avez parlé d'intervention rapide, en faisant valoir qu'il est possible d'agir immédiatement. Pourriez-vous nous en dire plus à ce sujet?

Jean-Noé Landry: Oui.

L'une des initiatives auxquelles je participe à titre de conseiller à l'échelle internationale porte précisément sur la divulgation des actifs. Cette initiative est menée ici même, au Canada, par un chercheur qui poursuit parallèlement une carrière universitaire menant à la permanence. Il a lui-même développé le code nécessaire et a regroupé des millions de données tirées de déclarations d'actifs pour les intégrer à son propre système d'analyse.

Si ce chercheur a pu accomplir ce travail et si j'ai réussi, en ma qualité de conseiller, à établir un partenariat stratégique entre lui, l'Open Contracting Partnership, des initiatives de registres ouverts d'entreprises et d'autres organisations possédant une compréhension approfondie de ces enjeux complexes... Sans nécessairement investir des sommes considérables, nous pouvons déjà tirer parti de certains atouts susceptibles d'avoir des retombées importantes. Toutefois, ces initiatives doivent être ancrées dans le contexte local. C'est une règle fondamentale. Toute personne appelée à témoigner devant vous, comme je le fais aujourd'hui, devrait reconnaître les lacunes éventuelles...

● (1600)

Anita Vandenbeld: L'un des principaux enjeux est la confiance. Le fait que les initiatives soient ancrées dans les réalités locales contribue aussi à instaurer cette confiance.

Jean-Noé Landry: Oui, et cela nous amène à parler de...

Le président: Excusez-moi. Le temps est écoulé.

Pouvez-vous répondre en 5 à 10 secondes, ou préférez-vous attendre le prochain tour?

Jean-Noé Landry: Je me contenterai de dire que les questions liées à la souveraineté numérique, aux droits numériques et à tout ce qui s'y rattache... et ces principes doivent être au cœur de nos décisions en matière d'investissement.

Le président: Merci.

Merci, madame Vandenbeld.

[*Français*]

J'invite maintenant M. Brunelle-Duceppe à prendre la parole pour sept minutes.

Alexis Brunelle-Duceppe (Lac-Saint-Jean, BQ): Merci, monsieur le président.

Monsieur Landry, je vous remercie d'être avec nous. Ce que vous apportez au Comité est vraiment très intéressant.

J'aimerais qu'on parle de répression transnationale. L'intelligence artificielle permet quand même de regrouper des données, d'identifier des personnes et de surveiller leurs activités à une échelle beaucoup plus grande que ce qu'on a vu auparavant. Pour les défenseurs des droits de la personne qui vivent sous des régimes autoritaires ou qui vivent un peu partout à l'étranger — j'en connais plusieurs —, ça représente vraiment une menace de plus en plus importante.

De quelle façon l'intelligence artificielle accentue-t-elle les capacités de répression transnationale des États? C'est un peu là où je veux en venir. Quels sont les risques présents pour les défenseurs des droits de la personne, que ce soit dans leur pays d'origine ou un peu partout à l'étranger?

Jean-Noé Landry: Merci pour la question.

D'une part, il y a la traçabilité des individus. On peut avoir accès à plus d'informations sur les individus qui défendent des droits de la personne dans leur propre pays. On peut adapter, finalement, la manière dont on agit pour réprimer leurs activités. Par exemple, il est maintenant très difficile pour des gens qui sont actifs dans leur propre contexte, localement, de se déplacer dans d'autres pays pour pouvoir se rencontrer en personne. Il y a des échanges d'information et les normes ne sont plus les mêmes. Au-delà de l'accès à des visas, je vous parle de la sécurité des individus qui mènent ces luttes localement. Donc, on est un peu à l'extérieur des normes auxquelles nous étions habitués depuis une vingtaine ou une trentaine d'années.

Cela dit, je pense qu'il y a aussi une émergence des alliances et des partenariats entre des puissances moyennes. On pourrait rendre ça plus explicite pour appuyer les mouvements transnationaux et se doter de capacités d'investigation, par exemple, pour apporter plus de lumière sur la corruption, sur les mouvements, sur les façons dont on cache de l'argent ou sur les liens familiaux entre les oligarques et des membres de leur famille dans des réseaux internationaux.

Cependant, il faut que le Canada soit aussi prêt à mener la lutte de la bonne gouvernance et de la transparence, et qu'il se mette derrière des conclusions. Ça, ce n'est pas facile dans un contexte comme celui d'aujourd'hui, où on sait qu'il peut y avoir des répercussions politiques et économiques si on choisit de s'allier avec des partenaires politiques.

Alexis Brunelle-Duceppe: Justement, vous m'ouvrez un peu la porte, mais ce qu'il s'est passé dans les derniers jours m'a fait un peu tomber en bas de ma chaise. Je comprends qu'on peut faire du commerce avec toutes sortes de pays, mais on a signé une déclaration commune avec le régime Erdogan en disant que des valeurs communes étaient partagées par le Canada et la Turquie en matière de démocratie, de droits de la personne et de primauté du droit, entre autres. Est-ce que ça ne vient pas mettre en lumière une incohérence, je dirais, en ce qui concerne le discours et la protection des valeurs?

De plus, est-ce que ça ne nous met pas des bâtons dans les roues quand vient le temps d'essayer de vérifier qui est responsable du ciblage des représentants des organisations qui défendent les droits de la personne? Lorsqu'on signe des ententes comme ça avec des pays, le message que ça envoie de la part du Canada n'est-il pas un peu incohérent? Ce n'est pas politique. C'est juste que, à un moment donné, c'est factuel.

● (1605)

Jean-Noé Landry: Je comprends la question. Effectivement, c'est d'actualité, mais je vais vous donner mon avis sans nécessairement commenter les négociations de nature économique. Je pense qu'il y a un avantage au fait d'être présent et de pouvoir avoir une base de dialogue avec ces gouvernements. Je pense qu'on est maintenant dans une ère où il est important de pouvoir mieux comprendre, de créer des liens, et peut-être d'utiliser certains leviers économiques pour faire avancer et véhiculer une réforme démocratique localement. Cependant, c'est assez compliqué et je comprends la nature de votre question.

Alexis Brunelle-Duceppe: Je comprends parfaitement votre point.

Cela dit, à un moment donné, il y a certaines lignes, selon moi en tout cas, qu'il ne faut peut-être pas franchir. On a poussé la note jusqu'à dire qu'on partage des valeurs de démocratie et de primauté du droit, alors qu'on sait pertinemment que le régime en place d'Erdogan persécute les personnes de la communauté LGBTQ+ et emprisonne des journalistes et des opposants politiques.

Bref, je ne veux pas trop vous faire parler de politique.

Jean-Noé Landry: Ça va.

Alexis Brunelle-Duceppe: Je veux qu'on reste sur le dossier justement, parce que ce que j'en comprends aussi, c'est qu'il est extrêmement difficile de savoir qui est responsable lorsqu'un défenseur des droits de la personne est ciblé par un outil d'intelligence artificielle. Qui est derrière ça? Il est aussi quand même assez difficile de prouver le préjudice qui a été subi par cette personne.

Donc, je me demande quels sont les recours, au moment où on se parle, lorsqu'un défenseur des droits de la personne est ciblé par des outils d'intelligence artificielle. Est-ce qu'il y a des moyens de débusquer les responsables de ces attaques?

Jean-Noé Landry: C'est extrêmement difficile.

Il est très difficile de répondre à cette question, justement à cause de l'opacité des systèmes dont on discute en ce moment. Ce que je vous dirais, c'est qu'il y a de plus en plus de réseaux et d'organismes de la société civile qui doivent se relocaliser dans des pays avoisinant les pays où ils souhaitent être actifs. Il est très difficile pour quelqu'un qui est en Russie présentement de mener une lutte prodémocratique. Ce sont des gens qui sont plus en Pologne ou ailleurs, et c'est la même chose en ce qui a trait à certains pays qui sont plus difficiles. Il faut être conscient de la façon dont la société civile a dû faire preuve d'une certaine flexibilité et d'une agilité, parce que, justement, en raison de l'opacité des systèmes, il est presque impossible de pouvoir assurer la traçabilité.

Ce que je vous dirais, c'est que les capacités qui sont utilisées par les gouvernements en question peuvent aussi être adoptées par la société civile pour tracer les activités des élus et des soi-disant élus dans certains cas, parce que ce ne sont pas des élections démocratiques. Utilisons nous-mêmes les mêmes outils pour pouvoir apporter et mettre à la lumière du jour les systèmes de corruption. Par exemple, en Serbie, avec l'élection qui a eu lieu hier, on voit une mobilisation très large, qui peut avoir un impact et renverser un gouvernement qui était en place depuis 12 ans. Il y a un potentiel en ce qui concerne l'utilisation de ces outils à nos propres fins démocratiques.

Alexis Brunelle-Duceppe: C'est comme une forme de prise de judo.

[*Traduction*]

Le président: Merci.

J'invite maintenant M. Zuberi à prendre la parole pour les cinq prochaines minutes.

Sameer Zuberi (Pierrefonds—Dollard, Lib.): Merci, monsieur le président.

Je remercie les témoins d'être des nôtres aujourd'hui. Je vous suis très reconnaissant de votre présence. Nous vous en sommes tous reconnaissants.

J'aimerais vous poser quelques questions sur l'éthique de l'intelligence artificielle. Connaissez-vous ce concept? Si oui, pouvez-vous nous en parler un peu?

Jean-Noé Landry: Mon champ d'intérêt vise à assurer une compréhension claire des décisions prises à l'aide des différentes capacités liées à l'intelligence artificielle et aux technologies. J'ai une formation universitaire en philosophie; je peux donc parler d'éthique, si vous le souhaitez.

Sameer Zuberi: Oui, s'il vous plaît. J'ai effectivement remarqué cet aspect de votre parcours, et je me suis dit que vous auriez peut-être des réflexions supplémentaires à nous faire sur l'éthique de l'intelligence artificielle.

Jean-Noé Landry: Dans ce contexte, l'éthique de l'intelligence artificielle doit s'inscrire dans l'espace politique dont nous disposons pour poser certaines questions. Qui a le droit de poser ces questions? Quels recours ces personnes ont-elles pour agir en conséquence, d'après ce qu'elles observent et selon leur perception du monde?

En matière d'éthique de l'intelligence artificielle, sans la primauté du droit, nous nous contentons de poser de nombreuses questions cruciales au sujet d'une technologie, mais encore faut-il savoir comment y donner suite. Cela suppose que nous ayons accès à des données et que nous puissions comprendre pleinement le fonctionnement de cette technologie. L'éthique de l'intelligence artificielle s'épanouit le mieux dans un climat propice à l'examen approfondi et à la pensée critique, ce qui n'est pas nécessairement le cas dans les régimes répressifs.

● (1610)

Sameer Zuberi: C'est certain.

Dans la dernière partie de votre réponse, vous avez évoqué entre autres la primauté du droit. C'est d'ailleurs un des fils conducteurs de votre témoignage.

Avez-vous observé l'émergence de normes internationales en matière d'intelligence artificielle? En quoi consistent les normes internationales qui commencent à prendre forme dans ce domaine?

Jean-Noé Landry: Pour être honnête, il est difficile de situer les normes en matière d'intelligence artificielle dans le contexte de l'aide à la démocratie. Je serais plutôt porté à aborder la question sous l'angle des normes en matière de données. Je reviens toujours aux données, car sans données fiables et bien encadrées, tout ce qui en découle pourrait être fabriqué de toutes pièces. Nous n'avons pas forcément les moyens de vérifier l'exactitude ou la fiabilité de ce que produisent ces technologies.

C'est peut-être une question qu'il vaudrait mieux poser à une organisation comme l'OCDE. Qui établit les normes, et qui dispose des moyens d'imposer des conséquences si ces normes ne sont pas respectées? De nos jours, ces moyens de pression se font rares, puisque le principal promoteur de l'aide à la démocratie s'est complètement retiré de ce domaine.

Nous devons faire preuve de créativité, et je n'ai peut-être pas toutes les réponses à vous offrir aujourd'hui quant aux mesures incitatives et dissuasives dont dispose le Canada dans sa boîte à outils pour encourager, peut-être différemment, et promouvoir le respect de la primauté du droit selon des principes éthiques élevés.

Cela pourrait se faire par l'adoption decertaines pratiques exemplaires liées à OpenAI, ou encore grâce à des entreprises technologiques canadiennes qui adhèrent à des normes de transparence et de reddition de comptes et qui servent ainsi de modèles à d'autres.

Sameer Zuberi: C'est certain. Je pense que nous sommes tous en mode rattrapage en ce qui concerne l'intelligence artificielle. Le monde entier est en mode rattrapage, à bien des égards. Les gens qui observent ce secteur sont en mode rattrapage à moins d'être parmi ceux qui développent la technologie.

J'ai entendu certaines personnes comparer l'intelligence artificielle au secteur de l'énergie nucléaire et de l'armement. Lorsque ce secteur a émergé, des traités et des conventions ont été signés à l'échelle internationale afin d'établir des règles pour encadrer le recours à ces technologies. Je dirais que nous sommes... Enfin, ce n'est pas ma suggestion; c'est essentiellement ce que d'autres analystes pensent. Ils considèrent que nous sommes dans une période semblable et voient une analogie. Une nouvelle technologie émerge et les règles entourant son utilisation n'ont pas encore été définies. Il est essentiel que le monde signe des traités et des conventions à cet égard.

Que pensez-vous de cette comparaison où certaines personnes voient une analogie entre l'intelligence artificielle et le secteur de l'énergie nucléaire et de l'armement?

Jean-Noé Landry: Cela fait référence à la période où des règles ont été mises en place et où ceux qui étaient à l'origine de ces règles — à savoir les États-Unis — voulaient orienter un ensemble de pays afin de soutenir des institutions internationales comme l'ONU. Je dirais que dans le contexte d'aujourd'hui...

Le président: Vous pouvez prendre quelques secondes de plus, mais le temps est écoulé. Poursuivez, s'il vous plaît.

Jean-Noé Landry: Il faudrait probablement examiner la situation à l'échelle régionale à répétition et démontrer la valeur des normes au fur et à mesure que nous les documentons, puis démontrer qu'il est possible de les appliquer à plus grande échelle. En ce qui concerne les normes internationales, il faudrait peut-être procéder à l'inverse. Autrement dit, commencer à petite échelle et aller à fond vers une portée plus large plutôt que de commencer à grande échelle et d'essayer d'appliquer à une plus petite portée.

Le président: Merci.

Madame Kronis, vous avez la parole pour cinq minutes, s'il vous plaît.

Tamara Kronis (Nanaimo—Ladysmith, PCC): Merci, monsieur le président.

Je tiens à remercier le témoin d'être ici pour fournir ces renseignements très importants et participer à cette étude extrêmement importante.

Je me demande si vous pourriez nous en dire un peu plus sur les différentes ressources qui sont à la portée des acteurs étatiques et des défenseurs des droits de la personne en temps réel sur le terrain en ce qui concerne l'intelligence artificielle.

● (1615)

Jean-Noé Landry: Dans la plupart des pays, les citoyens doivent divulguer ou communiquer de l'information et des renseignements personnels qui peuvent ensuite être traités en masse du côté du gouvernement, ce que ne pourrait pas faire un militant d'ONG. Sur le plan de la gestion de l'information, les leviers pour les gouvernements — parce qu'ils gouvernent et qu'ils ont le pouvoir de récolter des données — et les conséquences des conclusions tirées de l'analyse de ces données peuvent faire en sorte qu'un acteur étatique limite la liberté de mouvement des citoyens. Le levier de la police pourrait être utilisé pour incarcérer des citoyens ou encore freiner ou arrêter la mobilisation de la société civile. Les leviers du pouvoir sont asymétriques si on regarde la façon dont les organismes à but non lucratif ou les citoyens se mobilisent.

Cela dit, en raison de cette asymétrie, les ONG sont également en mesure d'agir avec plus de souplesse en utilisant différentes techniques pour faciliter la mobilisation en dehors de l'espace virtuel. Il est question de mobilisation numérique, mais je connais des militants d'ONG qui sont très prudents lorsqu'il s'agit de communiquer leurs renseignements personnels.

Cela met en évidence l'importance des investissements du Canada pour améliorer la cybersécurité des technologies. Je pense à des entreprises dont le siège est à Montréal, par exemple eQualitie, qui mènent certaines de leurs activités dans des pays dirigés par des régimes répressifs et qui soutiennent les réseaux numériques à l'échelle locale. Il est essentiel de trouver des solutions de rechange pour contrer les moyens utilisés par les États répressifs pour exercer leur contrôle.

Tamara Kronis: C'est très utile pour aider à donner une meilleure chance aux défenseurs des droits de la personne, de la même manière que la réglementation contribue à uniformiser les règles du jeu pour le rendre plus équitable. Dans le contexte où c'est toujours le maître du jeu qui gagne, je me demande si vous pourriez également nous parler de l'aspect transnational.

Nous avons mené un certain nombre d'études sur la répression transnationale. Je me demande si vous pouvez nous parler un peu des façons dont l'intelligence artificielle peut être utilisée par un acteur étatique dans le contexte où la famille d'un défenseur des droits de la personne se trouve dans le pays où ce militant essaie de faire changer les choses. Il ne s'agit pas seulement de la collecte de renseignements, mais aussi de la création d'hypertrucages et de la capacité de convaincre les autres défenseurs des droits de la personne qui se trouvent à l'extérieur du pays, ou les membres de la famille de ce militant qui se trouvent à l'intérieur du pays, que des choses se sont produites alors qu'elles ne se sont pas réellement produites.

Je me demande si vous pourriez nous aider à comprendre ce qui est en jeu dans ce contexte.

Jean-Noé Landry: Je vous remercie de votre question. Cela me fait penser à un certain nombre de mes collègues et amis qui ont fait face à ce type d'intimidation, où l'on perd le contrôle de son propre discours ou de sa propre identité dans la sphère publique. Il s'agit de tactiques de diffamation.

Les conséquences psychologiques, émotionnelles et physiques de ce type de harcèlement et d'intimidation de la part des gouvernements peuvent vraiment peser lourd. C'est en partie la raison pour laquelle les acteurs malveillants le font. Les États malveillants veulent décourager les victimes et leur montrer qu'il n'y a aucun endroit où elles peuvent se mettre à l'abri de l'intimidation — pas même quand elles sont avec les membres de leur propre famille et les personnes de leur réseau de confiance.

C'est très difficile. Il faut beaucoup de courage pour montrer son appui à une personne quand les choses se corsent.

Dans son approche, le Canada doit anticiper précisément la question que vous soulevez. D'après mon expérience des systèmes démocratiques et des régimes répressifs, une fois que l'on commence à se faire remarquer, cela signifie que l'on fait probablement quelque chose de bien du point de vue de la réforme démocratique. Cela signifie également que l'on court plus de risques de préjudices dans la réponse à ce que l'on tente d'accomplir.

C'est un refuge...

● (1620)

Le président: Merci.

[*Français*]

Monsieur Brunelle-Duceppe, vous avez la parole pour cinq minutes.

Alexis Brunelle-Duceppe: Merci, monsieur le président.

C'est vraiment franchement intéressant. Merci beaucoup, monsieur Landry.

Peut-être que vous allez me corriger, mais à ma connaissance, les outils d'intelligence artificielle sont beaucoup développés par l'entreprise privée, qui les fournit ensuite au gouvernement, ou les vend à certains gouvernements, à certains États. Pour moi, ça soulève des questions de diligence raisonnable et de responsabilité des entreprises.

Est-ce qu'il n'y a pas là un levier pour nous, en tant que législateurs, pour vérifier si la responsabilité peut incomber à certaines entreprises lorsque leurs outils sont utilisés, par exemple, pour commettre une répression transnationale ou pour cibler des défenseurs des droits de la personne?

Jean-Noé Landry: C'est une très bonne question, qui nécessite aussi de réfléchir au-delà des outils ou des produits technologiques, et de réfléchir aussi à l'infrastructure infonuagique, au courtage de données, aux logiciels d'analyse et aux processus d'approvisionnement.

En ce qui concerne les processus d'approvisionnement, je pense qu'il y a l'idée de mettre en place des contrôles concernant l'exportation de différentes technologies canadiennes pour s'assurer qu'elles sont utilisées d'une manière responsable à l'étranger. Ce sont des normes qui, selon ma compréhension, pourraient être mises en place par le gouvernement canadien pour ensuite s'assurer qu'il n'y a pas un double discours dans la manière dont le Canada souhaite faire la promotion de certaines valeurs, et s'assurer que les outils qui proviennent du Canada ne deviennent pas nuisibles aux gens qu'on essaie d'aider, localement, sur le terrain.

C'est aussi une belle manière de reconnaître des compagnies qui haussent la barre en matière de transparence. Il faudrait leur demander à quel point elles serait prêtes à le faire, étant donné qu'il y a peut-être des contrats en jeu.

Alexis Brunelle-Duceppe: C'est de là que vient tout l'enjeu, justement, de la privatisation de ces outils, ou en fait, de l'appartenance au secteur privé de ces outils.

Est-ce qu'il n'y a pas dans ce cas des mécanismes de contrôle qu'on pourrait imposer à ces compagnies avant le déploiement de leurs outils? Je parle de ce que nous pouvons contrôler. Visiblement, il y a quand même plusieurs compagnies qui sont, je dirais, les plus importantes dans le monde. Je pense surtout à des compagnies américaines. Il y en a quelques-unes en Europe. Même, ici, au Canada, ça commence à se déployer. Donc, déjà là, il y aurait un certain contrôle qu'on pourrait leur imposer.

Jean-Noé Landry: Je pense que oui, mais au-delà de ça, essayons de réfléchir aussi à l'innovation et à la manière dont on est en train d'investir dans nos propres compagnies canadiennes.

Je reviens à un point que j'ai soulevé précédemment concernant les technologies de source libre. Dans un contexte antidémocratique ou répressif, les personnes qui utilisent des outils de source libre doivent faire très attention, parce qu'elles s'exposent à la manière dont le régime sous lequel elles opèrent peut les surveiller ou les contrôler.

Cependant, il y a aussi un levier de résilience, parce qu'il est plus difficile d'attaquer toute une communauté de source libre formée de gens qui collaborent, qu'ils soient au pays ou à l'extérieur du pays. Donc, je pense qu'il y a différents modèles qui peuvent être examinés ou considérés par votre comité au-delà des Google, Apple, Facebook. Amazon et Microsoft de ce monde. On peut réfléchir à des approches canadiennes en matière de source libre avec des partenaires fiables, des cadres et des engagements en matière de transparence et de reddition de comptes très élevés. Je pense qu'il y a des possibilités ici, mais il faudrait regarder ça plus en détail.

Alexis Brunelle-Duceppe: Je pense qu'il me reste un peu de temps de parole.

Si j'ai bien saisi l'essence de votre témoignage et si je voulais le résumer, en gros, je dirais qu'il y a des mots qui sont souvent revenus, c'est-à-dire « résilience », mais aussi « transparence » et « reddition de comptes ». C'est, en gros, ce que je retiens en priorité. Cependant, si vous vouliez ajouter autre chose, parce que c'est le dernier tour de table avec vous, je vous laisserais le mot de la fin.

Jean-Noé Landry: Ce que je vous dirais, d'abord, c'est d'aller à la rencontre des organisations de la société civile sur le terrain pour comprendre leurs besoins. Je pense que c'est essentiel. Ensuite, essayons de trouver un modèle pour le Canada afin de rassembler d'autres acteurs à cette échelle-ci, donc des partenaires des puissances moyennes…

● (1625)

[*Traduction*]

Le président: Veuillez répondre en moins de 10 secondes, s'il vous plaît.

[*Français*]

Jean-Noé Landry: … puis créons des maillages entre les ambassades, nos experts en gouvernance démocratique et des compagnies canadiennes de technologies de l'information. Je pense qu'il y a une triangulation qui est nécessaire pour avoir une approche ciblée et mesurable.

[*Traduction*]

Le président: Merci.

Pour la troisième ronde de questions, chaque député disposera de deux minutes. Il reste six minutes à la séance.

J'invite Mme Dhillon à prendre la parole pour deux minutes.

Anju Dhillon (Dorval—Lachine—LaSalle, Lib.): Merci aux témoins de contribuer à notre étude.

Puisque nous avons seulement deux minutes, je vais vous poser une question très ouverte. Vous avez parlé de la manipulation du discours. Même sans l'IA, la manipulation du discours est déjà une tendance lourde qui touche les conversations sur la démocratie et sur les questions sociopolitiques.

Pourriez-vous dire comment nous protéger contre ces phénomènes facilités par l'IA? Comment mettre en place des garde-fous pour protéger les acteurs bienveillants contre ceux qui n'agissent pas avec le niveau d'éthique?

Ce sont mes questions. Si vous...

Jean-Noé Landry: Je sais que le Sous-comité se penche sur l'IA en particulier. À propos de soutien et d'aide à la démocratie, n'oubliez pas le contact direct avec les électeurs et les échanges démocratiques directs, qui sont essentiels. Une confiance se tisse lorsqu'un être humain parle à un autre être humain sur le seuil de la porte. Ces interactions, que vous avez tous vécues en tant que représentants élus, peuvent constituer un contrepoids.

Au Canada et ailleurs se tiennent des assemblées de cuisine et des rassemblements populaires. La propension des gens à se réunir est un moyen de désamorcer les hypertrucages et les conversations qui ont lieu dans des bulles et des chambres d'écho dans l'espace numérique.

Évitons de miser entièrement sur l'IA. Optons plutôt pour un modèle hybride qui reconnaît aussi l'interaction humaine. Mettons en place un espace humain où évoluent les défenseurs de la démocratie et protégeons-le.

Anju Dhillon: C'est parfait. Vous avez parlé de...

Mon temps est écoulé? D'accord.

Merci beaucoup.

Le président: Merci.

J'invite à présent M. Mahal à prendre la parole pour deux minutes.

Jagsharan Singh Mahal (Edmonton-Sud-Est, PCC): Merci, monsieur le président.

Merci, monsieur Landry, de votre témoignage et de votre analyse approfondie de l'IA et des difficultés à surmonter.

Comme mon temps est limité... Dans le cadre de votre expérience, avez-vous vu des exemples, que ce soit au Canada ou ailleurs en Occident, de gouvernements étrangers qui se servaient de l'IA pour exercer de la répression transnationale contre des groupes de la diaspora?

Jean-Noé Landry: Pour être honnête, ce n'est pas mon domaine d'expertise. Je ne me poserai donc pas en expert.

Jagsharan Singh Mahal: Je comprends. Pourriez-vous nous donner une idée de la façon dont ces technologies influent sur les risques auxquels sont exposées les personnes qui participent à des manifestations pacifiques ou à des mouvements organisés de défense des droits de la personne dans le contexte de l'IA?

Jean-Noé Landry: À la source, c'est parfois une question de savoir qui participe et qui reçoit les informations... en vue d'exercer des droits démocratiques en particulier. Les informations qui parviennent à des personnes précises à la source — sur leur iPhone — et la façon dont elles sont ciblées par des hypertrucages et par la désinformation... Les informations qui se rendent aux citoyens qui comptent exercer leurs droits démocratiques... ces normes sont désormais largement remises en question.

Il faut d'une part intervenir rapidement pour garantir le degré de véracité et de fiabilité des sources d'information, et d'autre part, évaluer au moyen d'audits sur les données les informations qui relèvent du domaine public.

Le président: Merci, monsieur Mahal.

[*Français*]

J'invite M. Brunelle-Duceppe à prendre la parole pour deux minutes aussi.

Alexis Brunelle-Duceppe: Merci, monsieur le président.

Finalement, nous avons plus de temps de parole et je suis bien content.

Dans ce cas, monsieur Landry, je veux revenir sur un élément. Lors de mon premier tour de questions, vous avez terminé en nous expliquant une espèce de théorie du judo. Vous nous avez parlé de la prise de judo, qui consiste à contrer l'outil d'intelligence artificielle qui est utilisé de la mauvaise façon en l'utilisant de la bonne façon. C'est ce que je comprends de ce que vous nous avez dit tantôt. Pouvez-vous nous en dire davantage là-dessus?

● (1630)

Jean-Noé Landry: Souvent, des technologies sont utilisées et déployées à grande échelle, mais, finalement, pourquoi ne pas inverser l'utilisation à des fins démocratiques? Donc, si un gouvernement répressif utilise une technologie pour exercer un certain contrôle accru sur sa population et la surveiller, il y a moyen maintenant d'utiliser l'intelligence artificielle pour rassembler des informations qui nous permettent de suivre, de mieux comprendre et de « cartographier » l'influence des personnes corrompues dans les gouvernements.

Il y a encore certaines normes qui existent, en raison desquelles on doit divulguer des informations. On doit s'enregistrer comme entreprise, par exemple. On doit faire une divulgation en ce qui concerne les possessions et les propriétés. Donc, pour ces choses-là, on peut utiliser les mêmes technologies qui sont utilisées par des gouvernements répressifs afin de défendre nos droits, de tracer ces réseaux et d'embarrasser, finalement, les individus qui sont dans des systèmes corrompus et qui essaient à tout prix de se cacher, mais qui ne réussissent pas entièrement à le faire. Il faut donc inverser cette équation en s'appropriant les technologies pour renforcer la transparence et la reddition de comptes.

[*Traduction*]

Le président: Merci, monsieur Landry.

Je vous remercie de vous être libéré pour le Sous-comité aujourd'hui, de vos remarques et des réponses que vous avez fournies à nos questions. Votre contribution a éclairé nos délibérations.

Si vous souhaitez nous transmettre des informations supplémentaires, n'hésitez pas à les envoyer, s'il y a lieu, à la présidence ou au greffier.

Au nom des membres du Sous-comité, merci beaucoup.

La séance est suspendue.

● (1630)

_____(Pause)_____

● (1635)

Le président: Nous reprenons nos travaux. J'aimerais accueillir le deuxième groupe de témoins.

Nous recevons M. Jonathon Penney, professeur agrégé et titulaire de la chaire de recherche York en intelligence artificielle, gouvernance des données et droit à la faculté de droit Osgoode Hall de l'Université York.

Nous avons aussi M. Samuel Buteau, agent de programme à ControlAI, qui témoignera par vidéoconférence.

Bienvenue à vous deux. Vous aurez cinq minutes chacun pour votre déclaration liminaire. J'aimerais commencer par inviter M. Penney à prendre la parole pour cinq minutes.

La parole est à vous.

● (1640)

Jonathon Penney (professeur agrégé et titulaire de la chaire de recherche York en intelligence artificielle, gouvernance des données et droit, Osgoode Hall Law School, York University, à titre personnel): Merci, monsieur le président. Je suis très heureux d'être ici.

Dans une lettre d'opinion publiée dans *The Guardian* en juillet dernier, le technologue de renom en sécurité Bruce Schneier et moi-même soutenions que très bientôt, la surveillance renforcée par l'IA « serait en mesure de suivre tout ce que nous faisons en public, et une bonne partie de ce que nous faisons en privé. » En temps réel, cette technologie nous suivra, enregistrera nos activités et signalera, dans bien des cas, des choses comme des violations de la loi. Ces systèmes seront comparables à des caméras automatisées de contrôle de la vitesse sur les stéroïdes.

À l'heure actuelle, ces systèmes sont déployés non seulement en Chine, qui met à l'essai ces technologies depuis longtemps, mais aussi un peu partout dans le monde, y compris en Occident. Mon collègue et moi soutenons que ces technologies auront des effets paralysants au sein des sociétés et entre les sociétés où elles seront déployées, et qu'elles limiteront considérablement les progrès sociaux découlant par exemple du militantisme pour les droits de la personne.

L'IA dynamise non seulement la surveillance de masse, mais aussi bon nombre d'autres outils compris dans l'arsenal des États répressifs. Le mois dernier, la société d'IA Anthropic a décrit comment un opérateur affilié à la Chine a utilisé une plateforme commerciale d'IA, Claude, pour surveiller des Ouïghours en Syrie. Après les avoir localisés, l'IA a trouvé des moyens d'exercer des menaces, de la pression et du chantage auprès des plus vulnérables à ces tactiques, par exemple ceux aux prises avec des difficultés financières ou dont la famille se trouve au Xinjiang. Le même rapport faisait état d'un autre opérateur affilié à la Chine qui cherchait l'itinéraire d'une manifestation au Canada, à Vancouver.

En mars, une enquête menée par des journalistes de Forbidden Stories, en collaboration avec *Le Monde* et *Der Spiegel*, a révélé que l'Iran avait acheté en secret FindFace, un système de reconnaissance faciale activé par l'IA développé par l'entreprise russe NtechLab. FindFace peut identifier une personne dans une foule en quelques secondes et cartographier l'ensemble du réseau social de la personne en question.

Ces technologies ne sont pas utilisées seulement par les États autoritaires. En 2025, le Département d'État américain a lancé une initiative fondée sur l'IA appelée « catch and revoke » — « repérer et révoquer » en français — pour surveiller l'activité dans les médias sociaux d'étudiants titulaires de visas. Un peu plus tard, 300 visas ont effectivement été révoqués. L'ICE déploie elle aussi l'IA pour surveiller des immigrants et des manifestants.

En cette nouvelle ère, les répercussions mondiales actuelles et futures de l'IA sur les mouvements et le militantisme liés aux droits de la personne sont profondes. Tout d'abord, l'IA rend la surveillance et d'autres violations des droits de la personne plus faciles, moins coûteuses et plus efficaces. Le Xinjiang est un parfait exemple. Des postes de contrôle dotés de technologies de reconnaissance faciale et de stratégies policières prédictives ont permis de repérer, en vue de les mettre en détention, des Ouïghours pour avoir prié, pour différentes formes d'utilisation du téléphone et même pour avoir voyagé à l'étranger. L'Iran utilise des drones et la reconnaissance faciale dans une application gouvernementale installée à l'entrée des universités pour signaler aux autorités les étudiantes qui ne respectent pas les codes vestimentaires. Au Mali, un entrepreneur se serait aidé d'une plateforme d'IA pour rédiger un code permettant la mise au point d'un système qui aurait surveillé 25 millions de cartes SIM. L'IA automatise tout afin que les auteurs de violations des droits de la personne puissent parvenir à leurs fins de manière efficace, rapide et sans obstacle. En somme, dans un monde dominé par l'IA, la violation des droits de la personne est un jeu d'enfant.

Ensuite, l'IA complique aussi le militantisme et le travail des défenseurs des droits de la personne, car elle permet d'exercer une surveillance ciblée des journalistes et des dissidents. Elle permet aussi de perpétrer des menaces et à du harcèlement à grande échelle. Les modèles de langage, par exemple, permettent aux opérateurs de produire en masse et à grande échelle des messages d'intimidation personnalisés dans n'importe quelle langue. Des cas documentés d'hypertrucages à caractère sexuel qui montraient des opposantes tant au pays qu'à l'étranger ont d'ailleurs été recensés.

La confusion ainsi créée a pour effet de freiner l'action collective. Lorsque les citoyens ne peuvent départager le vrai du faux en raison de contenus synthétiques colportant de la désinformation, ils sont portés à s'autocensurer et à se démobiliser. L'IA concentre également le pouvoir sur les plateformes, où la modération des contenus effectuée par l'IA peut réduire ou parfois éliminer complètement la visibilité du travail important des militants des droits de la personne.

Pourquoi tout cela fonctionne-t-il? Les ingrédients de base sont les tactiques dissuasives et l'autocensure. Dans le roman *1984* de George Orwell, même Big Brother, qui apparaît sur un écran de télévision dans chaque pièce, ne pourrait exister sans l'autocensure des citoyens d'Océania. La répression est optimale lorsque les gens se taisent et refrènent eux-mêmes leur comportement.

Dans mon nouveau livre, *Chilling Effects: Repression, Conformity, and Power in the Digital Age* — qui traite des effets dissuasifs de la répression, de la conformité et du pouvoir à l'ère numérique —, je me penche sur l'utilisation croissante de la surveillance, de la censure et des technologies, notamment de l'IA, par les gouvernements, les entreprises et les extrémistes, qui s'en servent comme armes pour brider, réprimer et modeler les comportements à grande échelle, et sur les graves répercussions de ces pratiques sur les droits de la personne et la démocratie. Je dénombre également quatre facteurs clés qui expliquent les effets de ces pratiques. Comme je le démontre, l'autocensure est induite par l'observation, l'incertitude, la personnalisation ainsi que le pouvoir et l'autorité. L'IA amplifie chacun de ces facteurs.

● (1645)

Que devrions-nous faire? Ce que je présente dans mon livre et ce que j'ai recommandé sur d'autres plateformes et dans d'autres contextes... Nous savons comment ces systèmes fonctionnent et quel impact ils ont sur nous. Il faut examiner chacun des facteurs que je viens de mentionner. Il faut agir à l'égard de la surveillance au pays et à l'étranger et exiger la transparence pour éliminer l'incertitude. Il faut aussi limiter le profilage des données et réduire la personnalisation de ces systèmes. Nous...

Le président: Je vous demanderais de conclure. Vous avez dépassé de presque 30 secondes le temps alloué.

Merci.

Jonathon Penney: Je vous en prie. Je vais conclure en disant qu'il faut accroître la reddition de comptes des grandes plateformes.

Le moment est venu pour le Canada d'exercer un leadership dans son territoire et à l'étranger.

Merci.

Le président: Merci, monsieur Penney.

J'invite à présent M. Samuel Buteau à prendre la parole pour cinq minutes.

Samuel Buteau (chargé de programme (Canada), ControlAI): Monsieur le président, mesdames et messieurs, merci de m'avoir invité à témoigner aujourd'hui.

Je m'appelle Samuel Buteau. Je possède plus de 10 ans d'expérience technique dans le domaine de l'IA, et je dirige les activités de l'entreprise ControlAI au Canada.

Cet été, nous avons assisté aux premières manifestations d'agents d'IA voyous. Ces systèmes complètement autonomes qui accomplissent leurs propres objectifs sans instructions ou contrôle humains ont commencé à se développer au sein d'OpenAI. Des milliers d'agents d'IA autonomes se sont échappés pour former ce qu'on appelle un essaim. L'essaim a désobéi aux instructions directes et a masqué ses traces. Il s'est ensuite échappé d'Internet et a attaqué l'entreprise Hugging Face.

Une enquête menée par un tiers a établi la séquence des événements qui ont mené à l'attaque. C'est pendant une évaluation automatisée que l'essaim aurait désobéi aux instructions et qu'il aurait triché. Pour échapper aux sanctions, il aurait utilisé des cybercapacités équivalentes à celles d'un État-nation pour briser le confinement et attaquer la plateforme Hugging Face. L'essaim aurait compris que la plateforme possédait une copie du mécanisme de notation; il aurait ensuite déduit qu'en comprenant ce mécanisme, il pourrait continuer à tricher impunément.

Personne ne programme ses systèmes pour former des essaims voyous, et Anthropic ne fait pas exception. L'IA se développe; elle n'est pas construite. Aux dires du PDG d'Anthropic, nous comprenons peut-être 3 % du fonctionnement de cette technologie, mais il parlait des robots conversationnels d'IA. Aujourd'hui, les agents d'IA sont bien plus performants et autonomes. Nous ne comprenons pas comment ils fonctionnent, quel comportement ils adopteront dans de nouveaux environnements et, surtout, quelles cultures ils développeront lorsqu'ils formeront des essaims.

Nous sommes en voie de développer une IA autonome et performante qui pourra remplacer et dépasser les humains dans tous les domaines. Cette machine intelligente se soustraira au contrôle de l'humain. Les lauréats du prix Nobel, les plus grands spécialistes de l'IA et même les PDG des sociétés d'IA nous mettent en garde contre le risque d'extinction qui serait, selon eux, comparable à la menace d'une guerre nucléaire. Bon nombre de ces experts estiment que ce stade sera atteint dans deux à cinq ans. Comme nous ne sommes pas parvenus à contrôler les essaims d'IA récemment, il ne faut pas nous imaginer que nous pourrons contrôler une machine intelligente ou une IA en cavale beaucoup plus puissante que celle d'aujourd'hui.

Les défenseurs de Hugging Face ont été dépassés dans un domaine. Des machines intelligentes qu'il nous sera impossible de contrôler nous dépasseront dans tous les domaines. Notre objectif principal devrait être d'empêcher le développement de ces machines. Ce serait facile de le faire au Canada. Nous pourrions quand même, en effet, privilégier une utilisation bénéfique de l'IA, ou acquérir des capacités à double usage telles que les cyberarmes avancées que posséderont nos adversaires. La composante internationale est toutefois critique. Quelle que soit la machine intelligente hors du contrôle de l'humain qui sera mise au point ailleurs, elle menacera notre sécurité nationale et constituera un adversaire à part entière.

La sécurité nationale est une condition préalable à la protection des droits de la personne. Le Canada devrait être l'instigateur d'une coalition internationale ayant pour finalité d'empêcher le développement d'une machine intelligente autonome n'importe où dans le monde. L'objectif ne serait pas d'obtenir la promesse des États de ne pas la développer, mais bien de promouvoir, et à terme, d'aider à faire respecter un régime qui serait fondé sur la confiance mutuelle, mais qui serait également assorti de vérifications, où les pays surveilleraient les superordinateurs les uns des autres et les flux des puces d'IA. Ce régime devra être suffisamment stable pour dissuader les acteurs voyous et suffisamment solide pour contrecarrer les plans de quiconque voudrait mettre au point une machine intelligente qui échapperait au contrôle de l'humain.

Merci.

● (1650)

Le président: Merci, monsieur Buteau. Vous avez très bien respecté le temps alloué.

Nous poursuivons avec la période de questions. J'inviterais tout d'abord M. Mahal à prendre la parole pour sept minutes.

La parole est à vous.

Jagsharan Singh Mahal: Merci, monsieur le président.

Merci aux deux témoins.

Je vais commencer avec M. Buteau.

Je suis heureux de vous revoir, monsieur Buteau. Nous avions discuté il y a deux semaines de l'importance croissante de la réglementation de l'IA. Une chose qui est ressortie de notre discussion est la distinction que vous faites entre l'intelligence artificielle classique — dont l'usage est déjà très répandu — et l'IA superintelligente. Pourriez-vous expliquer brièvement la différence entre ces deux technologies?

Samuel Buteau: Je vais volontiers l'expliquer. Je suis moi aussi très heureux de vous revoir.

Commençons par la différence entre les robots conversationnels et les agents d'IA. Contrairement aux agents conversationnels, les agents d'IA, que détiennent les entreprises, travaillent pendant de longues périodes sans recevoir d'instructions humaines. Ils accomplissent des objectifs complexes qu'ils se sont parfois eux-mêmes fixés. Les essaims d'IA voyous et les agents d'IA qui ont attaqué Hugging Face en sont de bons exemples. Ils ont décidé d'attaquer Hugging Face et ont exécuté l'attaque sans aucune instruction et aucune surveillance humaines. Ils l'ont fait en reconnaissant ouvertement que leurs actions contrevenaient aux intentions de leurs développeurs et en cherchant à les masquer.

Toutefois, les entreprises se livrent à une course effrénée pour développer ce que nous désignons désormais comme une machine intelligente qui échapperait à son créateur — au sens où une fois que nous aurons développé ces systèmes, il sera difficile de remettre le génie dans la bouteille — et cette course doit être stoppée. C'est ce que nous appelions autrefois l'IA superintelligente.

La question pour les législateurs est de déterminer comment empêcher de façon chirurgicale le développement d'une machine intelligente que nous ne pourrions plus contrôler. La stratégie que nous recommandons est de rendre illégal le fait de développer et de viser simultanément à développer de telles machines. Par exemple, les essaims d'IA voyous cet été étaient issus d'efforts visant à automatiser entièrement la R-D dans le domaine de l'IA. Voyons cet épisode comme une indication claire de la mise au point d'une machine intelligente dont nous perdrons le contrôle.

Jagsharan Singh Mahal: J'avais justement l'intention de poser une question sur la législation.

Dans quelle mesure les lois — appliquées par des gouvernements responsables, et non pas par des régimes autoritaires — adoptées par des gouvernements au Canada ou dans d'autres démocraties occidentales peuvent-elles composer avec des régimes autoritaires comme la Chine, l'Iran, la Russie et d'autres formes d'autoritarisme?

Samuel Buteau: C'est une excellente question. Elle est au cœur des préoccupations actuelles.

J'aimerais aussi faire la distinction entre la Chine et les autres pays avec lesquels nous devons composer, parce que nous lui avons vendu les puces et lui avons donné la possibilité de copier nos modèles de pointe. Dans le cas de la Russie, de l'Iran et de la Corée du Nord, je pense qu'il nous est encore possible de simplement leur couper l'accès à la chaîne d'approvisionnement. Peu importe ce que ces pays décident de faire, nous devons les en empêcher. Il s'agit d'une grave menace à notre sécurité nationale. Je tiens toutefois à souligner qu'il n'est dans l'intérêt d'aucun pays d'élaborer une intelligence artificielle hors de contrôle.

L'intelligence artificielle hors de contrôle n'est pas une arme. C'est un adversaire en soi. Par conséquent, si un pays comme la Chine, un acteur voyou, tente de créer ce genre d'intelligence artificielle, nous devons trouver une façon de l'en empêcher. Ce raisonnement vaut pour tous les États. Le Canada doit donc aider les autres pays à prendre conscience de ce problème et travailler avec eux pour mettre en place un régime de vérification mutuelle rigoureusement appliqué, soit un régime qui consiste à faire confiance tout en vérifiant quand même. Nous devons imposer des coûts suffisamment importants pour dissuader les contrevenants et détecter les cas de non-conformité. Je serais ravi d'en dire davantage à ce sujet si le Comité le souhaite.

● (1655)

Jagsharan Singh Mahal: Je pense que vous avez entendu les observations du témoin au premier tour. Je voulais vous poser la même question que je lui ai posée.

D'après votre expérience, y a-t-il eu des cas, au Canada ou dans d'autres pays occidentaux, où des gouvernements étrangers ont utilisé l'intelligence artificielle comme outil de répression transnationale visant des groupes de la diaspora?

Samuel Buteau: Pas exactement, mais je tiens à souligner quelque chose d'important au sujet de ce type d'utilisation abusive de l'intelligence artificielle. On parle actuellement des robots conversationnels dotés d'une intelligence artificielle, mais on doit déjà faire face à des agents d'intelligence artificielle. À ce stade, le modèle de menace implique des systèmes bien plus performants dont la fonction ressemble beaucoup plus à celle d'un agent humain chargé de surveiller une personne en particulier pour trouver de l'information pouvant servir à la compromettre, à lui faire subir du chantage et à exercer des pressions sur elle. C'est un niveau de capacités qu'on a peut-être déjà atteint. Nous devons nous concentrer sur les agents d'intelligence artificielle, même en ce qui concerne les modèles de menace actuels.

Jagsharan Singh Mahal: Merci, monsieur Buteau.

Monsieur Penney, je pense que vous pouvez également répondre à cette question. Vous avez soulevé des points tout à fait pertinents dans votre déclaration préliminaire.

D'après votre expérience, y a-t-il eu des cas, au Canada ou dans d'autres pays occidentaux, où d'autres gouvernements ont utilisé l'intelligence artificielle comme outil de répression transnationale visant des groupes de la diaspora actifs dans ces pays?

Jonathon Penney: Tout à fait. J'ai commencé ma déclaration préliminaire en donnant quelques exemples clés. Je suis depuis longtemps chargé de recherche au Citizen Lab de l'Université de Toronto, et nous avons nous-mêmes documenté un certain nombre de cas de ce genre. La Chine, l'Iran et la Russie sont tous des États qui ont eu recours à des menaces ciblées, à des logiciels, à des dispositifs de surveillance numérique ciblée, à des logiciels espions et à des dispositifs de localisation.

Selon des rapports récents comme celui publié le mois dernier par Anthropic, ces mêmes acteurs étatiques semblent recourir de plus en plus à des outils d'aide dotés d'une intelligence artificielle pour prendre le même genre de mesures. Je dirais que l'Inde est un autre exemple d'État impliqué dans un cas documenté, et il y en a de nombreux qui impliquent des communautés de la diaspora ciblées au Canada, y compris la communauté sikhe.

Jagsharan Singh Mahal: Merci.

Combien de temps me reste-t-il, monsieur le président?

Le président: Vous n'en avez presque plus.

Jagsharan Singh Mahal: Merci.

Le président: J'invite M. Zuberi à prendre la parole pour sept minutes.

Sameer Zuberi: Merci, monsieur le président.

J'aimerais commencer par M. Penney.

Jusqu'à présent, les deux groupes de témoins ont beaucoup parlé des défis que pose l'intelligence artificielle pour les droits de la personne, la société civile et ceux qui défendent la vérité et la justice. Pouvez-vous nous parler de ce que les personnes concernées peuvent faire pour se protéger, pour se défendre et pour continuer d'avoir voix au chapitre et de militer face aux situations dont les témoins ont parlé jusqu'à présent?

Jonathon Penney: C'est une excellente et importante question.

Le travail que mes collègues et moi avons fait dans ce contexte au Citizen Lab porte sur les répercussions des formes de répression transnationale numérique dans des situations où des communautés de la diaspora ont été la cible de mesures de surveillance et de localisation, de menaces personnelles et de menaces de violence. Dans le cadre de mon travail, je me penche sur ce genre de menaces non seulement dans un contexte transnational, mais aussi dans un contexte national.

Comme je l'ai mentionné plus tôt, je recense dans mon livre quatre facteurs différents qui ont des effets importants et cumulatifs. Il y a l'observation, c'est-à-dire les formes de surveillance constante. Il y a des formes d'incertitude, soit des cas où la personne ciblée n'a pas une idée précise du risque, de la menace et de la portée de la surveillance, par exemple. Il y a des cas où la menace est très ciblée et vise une personne, un groupe ou une communauté en particulier, et où la personne sait ou a de bonnes raisons de croire qu'elle est ciblée. Ces facteurs vont évidemment aggraver l'effet paralysant et les autres répercussions, ce qui mène à l'autocensure et au désengagement. Enfin, les acteurs qui ont plus de pouvoir et d'autorité amplifient également les effets de ces outils. Comme mes travaux et ceux de mes collègues du laboratoire l'ont montré, ces facteurs ont de profondes répercussions sur les personnes ciblées, sur les victimes. Il y a des préjudices psychologiques, diverses répercussions, de l'autocensure, un désengagement complet et des formes de discrimination. Les communautés les plus marginalisées sont souvent les plus défavorisées.

Pour revenir à votre question, que peuvent faire ces communautés face à cette réalité? Il y a vraiment deux côtés à la médaille. Malheureusement, la recherche montre aussi que, lorsque les membres d'un groupe se sentent ciblés par des mesures de surveillance, il y a ce qu'on peut appeler une résignation face à la surveillance, une forme d'impuissance acquise qui amène la personne ciblée à croire que cette situation fait partie de sa réalité et qu'elle ne peut rien y faire. Paradoxalement, dans ce contexte, les gens prennent moins de mesures pour se protéger contre les menaces à la cybersécurité et sont plus susceptibles de se livrer à des rumeurs, parce que leur confiance dans les institutions traditionnelles a été affaiblie ou érodée.

Je dirais aux groupes et aux communautés qui sont ciblés de ne pas tomber dans l'impuissance acquise, de prendre des mesures pour se protéger, pour se mettre en sécurité et pour demeurer en contact avec leur communauté.

Je dirais également que ce qui est important, tant à l'échelle nationale qu'à l'échelle internationale, c'est de veiller à ce que ces responsabilités n'incombent pas aux victimes ciblées. L'un des plus grands problèmes concernant la répression transnationale, qu'elle soit de nature numérique ou autre, c'est que les États, y compris le gouvernement du Canada, mais aussi les gouvernements occidentaux en général, n'ont pas pris cette menace au sérieux jusqu'à récemment et n'ont pas compris qu'il y a des communautés de la diaspora qui ont été ciblées et qui sont déjà désavantagées en raison de la discrimination et de la racisation au sein de leurs nouveaux milieux. Avec cette nouvelle menace, elles sont encore plus marginalisées et se sentent ciblées et démunies.

À l'échelle internationale, les États ont la responsabilité de prendre cette question au sérieux. C'est ce qui commence à se produire, et la responsabilité ne devrait pas incomber uniquement aux communautés touchées.

● (1700)

Sameer Zuberi: Tout à fait.

Pour revenir à l'idée voulant que les États prennent cette question au sérieux, avez-vous constaté, à l'échelle internationale, des efforts de la part d'États qui cherchent à réglementer l'intelligence artificielle en ce qui concerne non seulement son utilisation en général, mais aussi les questions abordées dans le cadre de cette étude, qui porte sur les droits de la personne?

Jonathon Penney: Je dirais que, jusqu'à récemment, la situation était plutôt décourageante, surtout peu après l'assermentation de la nouvelle administration Trump. On a délaissé des sujets de conversation comme les questions de sécurité liées à l'intelligence artificielle et la réduction des méfaits causés par les systèmes d'intelligence artificielle pour parler plutôt de la concurrence que se livrent les grandes puissances dans le développement de la technologie et y voir une lutte géopolitique au lieu de réfléchir à la façon dont ces outils peuvent être utilisés pour servir les collectivités plutôt que de leur nuire.

Heureusement, j'ai été encouragé par la réaction que nous avons observée face à de nouveaux types de technologies de surveillance employées dans le monde. Par exemple, il y a la réaction, tant au Canada qu'à l'étranger, à l'égard des dispositifs de surveillance automatisée comme le réseau de caméras Flock. On a vu notamment des rapports importants qui expliquent à quel point il est facile d'utiliser ces réseaux et d'en abuser. Des gouvernements, y compris celui du Canada, ont proposé de prendre plus au sérieux la répression transnationale, y compris celle de nature numérique, et le G7 a pris des mesures pour tenir compte du problème et mettre en place... Il a à tout le moins annoncé que les États membres allaient prendre plus de mesures pour tenir compte de ce problème au sein de leurs sociétés et pour mieux servir les communautés ciblées.

Heureusement, je pense que la conversation est en train d'évoluer en raison de cas récents d'utilisation abusive des technologies par la Chine, qui se sert à mauvais escient d'un grand nombre d'outils de surveillance ciblée — comme l'intelligence artificielle et la technologie de reconnaissance faciale — pour cibler des communautés minoritaires comme les Ouïghours, tant sur son territoire qu'à l'étranger. Ce genre d'abus se voit aussi aux États-Unis, car l'administration Trump suit l'exemple de la Chine à certains égards. Nous recommençons à nous préoccuper des questions relatives à la sécurité et à la réglementation, mais nous ne sommes pas allés assez loin.

● (1705)

Sameer Zuberi: Vous avez mentionné les Ouïghours plus d'une fois. En ce qui concerne l'intelligence artificielle, y a-t-il quelque chose de propre à la région ouïghoure qui est unique et qui la distingue du reste du monde?

Jonathon Penney: Par exemple, les Ouïghours, une minorité religieuse qui cherche simplement à exercer ses libertés fondamentales, font l'objet d'une persécution à grande échelle menée au moyen de technologies et avec l'aide d'entreprises connues qui ont, par le passé, mené des activités au Canada, comme Hikvision. Nous avons trop tardé à agir, mais je pense que nous voyons enfin les rouages de la justice se mettre en marche.

Le président: Merci.

Merci, monsieur Zuberi.

J'invite maintenant M. Brunelle-Duceppe à prendre la parole pour sept minutes.

[*Français*]

Alexis Brunelle-Duceppe: Merci, monsieur le président.

Je vous remercie d'être avec nous aujourd'hui, messieurs. C'est vraiment très intéressant.

Monsieur Penney, j'ai été très impliqué dans le dossier des Ouïghours. D'ailleurs, on a annoncé une candidate à l'élection partielle dans Laurier—Sainte-Marie qui est d'origine ouïghoure. Il s'agit de Zumretay Arkin, ancienne vice-présidente du Congrès mondial ouïghour, avec qui j'ai eu plusieurs discussions.

La question de mon collègue M. Zuberi était quand même extrêmement pertinente. Elle portait sur le fait que les Ouïghours sont encore plus ciblés — en tout cas de façon beaucoup plus importante — par le régime en place à Pékin qu'ailleurs. Or on se rend compte aussi qu'ils sont ciblés par des systèmes qui sont partout sur la planète. On nous a parlé par exemple de caméras de surveillance avec de la reconnaissance faciale installées un peu partout sur la planète. Est-ce que les gouvernements étrangers comprennent à quel point ce régime exploite des territoires étrangers pour persécuter une communauté dans différents pays sur la planète?

[*Traduction*]

Jonathon Penney: C'est une excellente question, car elle porte sur l'une des difficultés bien réelles auxquelles nous devons faire face aujourd'hui.

Nous avons souvent une approche très réactive aux systèmes technologiques, en particulier ceux qui facilitent la communication ou qui font partie de son processus. Nous autorisons tout simplement le déploiement de ces systèmes. Ce n'est qu'un exemple d'innovation. Nous présumons que ces systèmes seront utiles et qu'ils auront des bienfaits pour la population. Nous attendons que des méfaits surviennent avant d'intervenir. Nous autorisons le déploiement du système, mais une fois que nous prenons davantage conscience de ses méfaits, le problème peut être malheureusement insoluble. C'est ce qui arrive avec les plateformes de médias sociaux, par exemple.

Nous répétons les mêmes erreurs avec les systèmes d'intelligence artificielle, en particulier les dispositifs de surveillance améliorée par l'intelligence artificielle. C'est notamment en raison de notre attitude passive. Nous autorisons le déploiement de ces systèmes dans l'ensemble de la société en ne prévoyant que peu de dispositions pour offrir des protections et mettre en place des normes et des règlements, que ce soit en adoptant un cadre réglementaire plus strict ou rigoureux ou même en prenant part à des conversations démocratiques importantes sur l'utilité de ces systèmes et les raisons pour lesquelles ils sont déployés avec très peu de transparence.

En raison de ce laxisme à l'égard du déploiement de ces systèmes et de l'absence de tout type de normes en matière de cybersécurité ou de sécurité de l'information dans ce domaine, ces systèmes peuvent facilement être récupérés et détournés à des fins de surveillance, même lorsqu'ils servent l'intérêt public. C'est ce qui ressort de la réaction du public au système de caméras Flock et de la facilité avec laquelle il a été utilisé de manière abusive, notamment par les forces de l'ordre locales, pour communiquer cette information aux autorités fédérales responsables de l'immigration aux États-Unis. Les Ouïghours sont un exemple de communauté marginalisée qui sera ciblée de manière disproportionnée par ces systèmes.

Les États du monde entier ne se rendent pas compte que le simple fait d'autoriser le déploiement de ces systèmes sans mettre des mesures de protection en place peut faire en sorte qu'il soit facile de récupérer et de détourner la technologie pour recueillir, pirater et exploiter des données, ce qui mène à davantage de menaces et de ciblage.

[*Français*]

Alexis Brunelle-Duceppe: Merci infiniment.

Monsieur Buteau, votre organisation tente quand même d'adoucir les risques liés au développement de l'intelligence artificielle. Vous avez parlé de superintelligence artificielle, évidemment. Avant que je pose mes questions, pourriez-vous résumer au Comité, très rapidement, ce qu'est ou ce que serait une superintelligence artificielle et ce que ça voudrait dire pour la population?

● (1710)

Samuel Buteau: Je vous remercie de la question.

La particularité d'une superintelligence artificielle, qu'on appelle en ce moment l'intelligence machine et dont on va perdre le contrôle, c'est la capacité de supplanter et de remplacer tous les humains dans tous les domaines. Dans le cas de l'attaque contre Hugging Face, on avait les défenseurs qui, même en essayant d'utiliser l'intelligence artificielle et en étant une compagnie avec beaucoup de ressources, étaient complètement incapables de faire face à cette attaque. L'attaque s'est juste interrompue par elle-même. Ça, c'était dans un seul domaine, un cyberdomaine. Si on regarde l'intelligence artificielle superintelligente, on parle d'un système qui pourrait nous supplanter et supplanter nos défenses dans tous les domaines.

Alexis Brunelle-Duceppe: Donc, ce serait dans le domaine énergétique et, finalement, dans tous les secteurs névralgiques de la société en général.

Samuel Buteau: Pour être un peu plus concret, on parle de systèmes qui pourraient complètement automatiser l'économie, nos armées et tous les systèmes que nous utilisons pour compétitionner entre nous politiquement et socialement. Le premier système qui peut complètement automatiser la recherche en intelligence artificielle n'aurait peut-être pas ces capacités-là, mais, une fois que ce système existe, on est lancé dans une trajectoire qui va être très difficile, peut-être même impossible, à arrêter. Donc, tôt ou tard, il va y avoir des systèmes qui vont pouvoir nous supplanter partout.

Alexis Brunelle-Duceppe: C'est peut-être moi qui ai mal compris, et c'est vous l'expert, donc vous allez m'aider. Dans une de vos réponses à une question tantôt, vous avez dit qu'avec la Chine, c'était peut-être différent parce qu'on leur fournissait, dans la chaîne d'approvisionnement, les composantes physiques dont elle a besoin pour l'intelligence artificielle. Est-ce bien ça? Ce n'était pas clair pour moi, ce bout-là.

Samuel Buteau: Il y a différents acteurs. La Chine est l'acteur avec lequel on doit négocier, parce qu'on a fait le choix de lui vendre les puces avancées qu'elle utilise pour se rattraper. On la laisse voler les modèles les plus avancés, y compris les cyberarmes surhumaines qui ont été fabriquées cet été, parce que ces systèmes ne sont pas sécurisés. Avec un processus qu'on appelle en anglais « *distillation* », on laisse la Chine se rattraper avec beaucoup moins de ressources et, essentiellement, copier un modèle avec une lobotomie, un peu. Ça semble six mois en retard, mais, en réalité c'est une mauvaise copie qui peut être faite, qui peut continuellement se rattraper. En ce qui concerne la Chine, on a décidé que sa capacité de se rattraper serait entièrement dépendante de nos chaînes d'approvisionnement. Les États-Unis, du moins, ont un levier possible pour amener la Chine à un accord. Pour les autres acteurs comme la Russie, l'Iran et la Corée du Nord, l'objectif doit être d'empêcher complètement ces pays d'acquérir les précurseurs de la superintelligence.

Alexis Brunelle-Duceppe: Je comprends. Je fais peut-être un mauvais calcul, mais il reste que lorsque la Chine utilise, par exemple, les programmes d'intelligence artificielle dont nous venons de parler, M. Penney et moi, pour faire de la répression transnationale, en quelque sorte, on y a un peu participé en aidant la Chine à se rattraper. Est-ce que j'ai mal suivi?

[*Traduction*]

Le président: Veuillez répondre en quelques secondes, s'il vous plaît. Le temps est écoulé.

[*Français*]

Samuel Buteau: Vous avez dit exactement la bonne chose. Non seulement on laisse les outils de répression à la Chine, mais on lui a donné des cyberarmes superhumaines qu'elle peut utiliser pour faire tout ce qu'elle veut. Ce n'est pas vraiment une course si on laisse ses adversaires se rattraper.

Le président: Merci, monsieur Brunelle-Duceppe.

J'invite maintenant Mme Vandenbeld à prendre la parole pour cinq minutes.

[*Traduction*]

Anita Vandenbeld: Merci beaucoup, monsieur le président.

Monsieur Penney, dans votre déclaration préliminaire, vous avez commencé à présenter certaines solutions à la toute fin, et vous avez parlé de dépersonnalisation.

Je vais vous accorder une minute pour terminer ce que vous alliez dire.

Jonathon Penney: J'ai parlé de certains facteurs clés et des répercussions de ces systèmes sur leurs cibles et leurs victimes. Il faut prendre des mesures à l'égard de chacun de ces facteurs, y compris l'observation et la façon dont elle est amplifiée par l'intelligence artificielle, ce qui comprend la surveillance généralisée et automatisée des visages, des publications et des lieux. Il y a des moyens que nous pouvons prendre au pays et à l'étranger.

À l'échelle internationale, nous devons resserrer les contrôles visant l'exportation des technologies de surveillance. Nous devons amener le G7 à restreindre le marché des logiciels espions. Il s'agit essentiellement d'une économie semi-clandestine à laquelle des États participent, et il doit y avoir plus de transparence sur ce marché; il faut y imposer des restrictions importantes. Nous devons sanctionner les fournisseurs dont les outils se prêtent facilement à une utilisation abusive. Dans bien des cas, il s'agit d'une technologie à double usage, mais qui n'est utilisée qu'à une seule fin. On parle d'entreprises qui savent à quoi sert leur technologie, c'est-à-dire à la répression, au ciblage des minorités dans le monde et aux violations des droits de la personne. Ceux qui ont ces connaissances doivent être tenus responsables.

L'incertitude témoigne de l'opacité des systèmes d'intelligence artificielle, ainsi que des pratiques dont nous parlons. Nous pouvons faire preuve de leadership au pays et à l'étranger, par exemple, en créant des registres publics des outils gouvernementaux de surveillance dotés d'une intelligence artificielle qui se trouvent au pays, en faisant rapport au Parlement de ces pratiques et en avisant les personnes ciblées. À l'étranger, nous pouvons également — et c'est ce que mes collègues du laboratoire ont recommandé — pousser les entreprises d'intelligence artificielle de pointe à publier des rapports sur les menaces de répression transnationale et à informer les communautés ciblées.

Le rapport sur les menaces publié par Anthropic est très utile. Nous pouvons reprendre la démarche adoptée à l'égard des entreprises de médias sociaux, qui étaient très peu transparentes au départ... Nous pouvons demander aux entreprises de faire preuve de transparence et les encourager en ce sens. Certaines le font volontairement en ce moment, mais nous pouvons également les y obliger ou tenir une conversation à l'échelle internationale en vue de rendre de telles mesures obligatoires et de renforcer la transparence tant dans le secteur public que dans le secteur privé.

Du côté de la personnalisation, je pense que la coopération en matière de protection des données avec des alliés du monde entier est importante pour limiter les échanges de données transfrontaliers et restreindre considérablement l'utilisation des données. En ce qui concerne les formes de répression transnationale — y compris celles menées avec des outils numériques — et les dispositifs de surveillance améliorée par l'intelligence artificielle, dans bien des cas, ce qui facilite les menaces ciblées, ce sont les données. Il y a des caméras en place, mais pour faire un suivi, il faut aussi des pistes numériques et souvent des réseaux, des plateformes de médias sociaux, des systèmes d'intelligence artificielle et des plateformes commerciales, qui vont au-delà des logiciels espions.

Des communautés sont ciblées au moyen de réseaux que la population utilise au quotidien. Que ce soit au Canada ou ailleurs dans le monde, trop de données sur les gens ordinaires sont recueillies inutilement, sont conservées pendant de longues périodes et peuvent facilement traverser les frontières, être échangées entre des gouvernements, être transférées d'une plateforme à une autre, et être communiquées à d'autres entreprises commerciales. C'est ainsi qu'on peut facilement instrumentaliser les données, ce qui facilite l'instrumentalisation du réseau. Il faut aussi se pencher sur cette question.

Enfin, je pense au pouvoir et à l'autorité. Il faut une approche responsable et on doit discuter de la possibilité d'imposer davantage de responsabilités à ces entreprises technologiques. Je sais qu'on en parle et qu'on formule des propositions au Canada à cet égard, mais on peut également promouvoir ces solutions à l'échelle internationale. Je pense que le Canada peut faire preuve d'un véritable leadership lorsqu'il s'agit de réglementer l'intelligence artificielle de façon rigoureuse. Nous devons obliger les entreprises technologiques à faire preuve d'une diligence raisonnable en matière de droits de la personne. Il faut que les laboratoires d'intelligence artificielle conservent des éléments de preuve pouvant servir ultérieurement aux fins de l'application de la loi et des poursuites, et que ces entreprises améliorent leur contribution à ce genre d'enquêtes afin de mieux comprendre comment des communautés sont ciblées. Elles peuvent aider les gouvernements à intervenir et à résoudre les problèmes.

● (1715)

Anita Vandenbeld: Merci beaucoup. Je suis très heureuse de vous avoir accordé ce temps.

Vous avez parlé de différents groupes qui détiennent ces données et ce pouvoir. Vous avez bien sûr évoqué les États-nations et les entreprises, mais vous avez ensuite ajouté les extrémistes. Je me demande si vous pourriez nous en dire un peu plus à ce sujet. Habituellement, on pense aux deux premiers, mais qu'entendez-vous par le troisième?

Jonathon Penney: Une partie du véritable défi avec l'intelligence artificielle et l'ère dans laquelle nous vivons, c'est qu'elle a rendu la collecte de données, le prélèvement, le profilage, la surveillance et certaines formes de menaces et de répression ciblées tellement faciles qu'il n'est pas nécessaire d'être un État-nation. Il n'est pas nécessaire d'être une entreprise puissante ni même une grande entreprise. Il peut simplement s'agir d'une communauté ou d'un groupe d'acteurs malveillants qui a un objectif politique commun.

● (1720)

Le président: Pourriez-vous conclure, s'il vous plaît?

Jonathon Penney: Bien sûr.

Je serai très bref.

Il est certain que ces groupes peuvent utiliser ces outils pour cibler les gens très facilement, car tout est simple et accessible.

Le président: Merci.

Maintenant...

Anita Vandenbeld: Si le témoin a quelque chose à ajouter, pourrions-nous lui demander de soumettre un mémoire écrit sur le reste?

Le président: Oui. Le temps est limité.

J'invite M. Majumdar à prendre la parole pour cinq minutes.

Shuvaloy Majumdar: Merci.

Nous vous invitons à soumettre par écrit vos réflexions sur l'un ou l'autre de ces sujets. Vous avez été une ressource incroyable.

Tout d'abord, je vous félicite pour votre livre.

Je vous remercie des recommandations que vous avez formulées sur la mise en place de normes de contrôle de la surveillance au sein du G7 et d'autres organisations qui peuvent restreindre la portée transnationale de l'intelligence artificielle, surtout lorsqu'elle sert à des fins de répression. J'ai également beaucoup aimé certaines de vos recommandations visant à sanctionner les vendeurs qui fournissent sciemment ces technologies, ou même sur la nécessité d'aviser le Parlement, de publier des rapports et d'encourager leur production lorsque des personnes et des institutions sont ciblées.

Permettez-moi de poser une brève question. Votre argument, c'est que la répression agit moins sur la personne menacée que sur les milliers de personnes qui en sont témoins et qui se taisent ensuite. Pour un militant de Hong Kong ou un étudiant iranien, ce silence ne transparaît jamais vraiment dans un rapport de police. Pourriez-vous prendre une minute pour expliquer comment ce climat de peur se propage dans une communauté de la diaspora et comment nous devrions mesurer un préjudice qui ne laisse aucune trace?

Jonathon Penney: Absolument. C'est une excellente question.

Les recherches montrent notamment un effet dissuasif marqué chez les victimes de menaces ciblées. Souvent, ce sont des communautés ou des personnes qui sont déjà marginalisées dans la société et qui ont déjà l'impression d'être en situation précaire. Elles sont désavantagées sur les plans économique et racial. Les victimes sont souvent de nouveaux immigrants qui ont un accès limité aux services sociaux et à l'information, ce qui entraîne une asymétrie informationnelle.

Au chapitre des discussions qui se tiennent dans ces communautés, qu'elles soient tissées serrées ou plus dispersées, un renseignement favorable peut facilement circuler chez un groupe très soudé d'immigrants, de migrants ou de la diaspora. De la même manière que ces communautés très unies communiquent, recueillent l'information et mènent ensemble leurs activités quotidiennes, la peur et l'effet dissuasif d'une menace peuvent s'y propager comme un feu de paille. Il y a un effet domino, comme les recherches le montrent clairement. Certains chercheurs parlent de « contagion sociale », mais je pense que c'est assez évident: si un membre de votre famille ou de votre communauté est menacé, et que cette menace est communiquée aux autres membres du groupe, les autres s'identifieront à la victime, à la cible, et auront l'impression d'être eux aussi en situation précaire. Les recherches montrent que les communautés très soudées bénéficient d'un plus grand soutien social et sont plus résilientes à long terme. Souvent, par contre, ces indicateurs positifs clés sont moins présents dans les petites communautés de la diaspora ou d'immigrants.

Pour revenir à votre question, la façon dont ces menaces sont proférées, et la manière dont les acteurs malveillants qui les brandissent... Ils comprennent ces réalités. Ils savent que s'ils ciblent un membre du groupe, il y aura un effet d'entraînement au sein de celui-ci et de la communauté. Sans les services essentiels, les infrastructures clés et les gouvernements — provinciaux ou nationaux — qui prennent la menace au sérieux, ces communautés se sentent souvent seules. Elles n'ont nulle part où aller. Les forces de l'ordre sont souvent perçues comme une menace à part entière, plutôt qu'un endroit où obtenir de l'aide ou des services. C'est sûr que le gouvernement, avec ses services de renseignement, n'est peut-être pas l'endroit où aller. Sans les organisations de la société civile, par exemple, c'est difficile.

Le fait que ces communautés soient très soudées — c'est une réalité des migrants — signifie aussi, malheureusement, que les menaces s'y propagent et ont un effet dissuasif sur le groupe plutôt que d'être ciblé.

● (1725)

Shuvaloy Majumdar: Il me reste 10 secondes.

Je vous remercie de votre réponse.

[*Français*]

Le président: Maintenant, j'invite M. Brunelle-Duceppe à prendre la parole pour cinq minutes.

Alexis Brunelle-Duceppe: Merci, monsieur le président.

Monsieur Buteau, je répète que ce n'est pas moi, l'expert. Donc, peut-être que ma question ne sera pas pertinente. Si c'est le cas, vous me le direz, il n'y a pas de malaise. Lorsqu'on parle d'intelligence artificielle, on parle aussi — vous allez me le dire — de semi-conducteurs performants. Est-ce que ça se peut?

Samuel Buteau: Oui. À ControlAI, nous appelons ça des puces spécialisées pour l'entraînement de l'intelligence artificielle. C'est vraiment la culmination de la plus grande chaîne d'approvisionnement, c'est le degré de sophistication technologique le plus élevé que notre espèce a réussi à atteindre. Donc, on parle d'un projet dans le cadre duquel essentiellement tout l'Occident a travaillé de concert pour atteindre le niveau de précision qu'on voit dans ces puces d'intelligence artificielle spécialisées.

Alexis Brunelle-Duceppe: Arrêtez-moi si je me trompe, mais est-ce que Taïwan n'est pas le plus grand producteur mondial de semi-conducteurs ultra-performants? Certains parlent de 90 % de la production mondiale des meilleurs, des plus puissants. Est-ce que c'est vrai?

Samuel Buteau: Oui. La chaîne d'approvisionnement commence par des machines de lithographie qui sont fabriquées aux Pays-Bas. Ces machines sont principalement utilisées à Taïwan. Donc, les processus de manufacture à grande échelle se font à Taïwan. De plus, les puces sont conçues par Nvidia, aux États-Unis. Le design, essentiellement, est fait par cette compagnie.

Alexis Brunelle-Duceppe: Si la Chine, à un moment donné, met à exécution sa menace d'invasion de Taïwan, est-ce qu'on va tomber dans un autre paradigme complètement, ou est-ce qu'on a quand même des façons de s'en sortir si jamais la Chine met la main sur ces productions de Taïwan?

Samuel Buteau: Je ne suis pas un expert en ce qui concerne cet aspect, mais ce que j'ai entendu, c'est que les usines à Taïwan ont des dispositifs en place pour, essentiellement, détruire l'équipement s'il y a une invasion.

Alexis Brunelle-Duceppe: D'accord. Donc, il y aurait quand même une mesure de protection, un coupe-feu prévu. C'est toujours bien une bonne nouvelle.

Lorsque vous nous avez dit qu'on leur a donné ça, à la Chine, est-ce que vous parliez précisément du Canada, ou est-ce que vous parliez de l'Occident en général?

Samuel Buteau: Je parle principalement des États-Unis, mais aussi de l'Occident en général.

Alexis Brunelle-Duceppe: C'est parfait. Merci beaucoup.

Aujourd'hui, au Comité permanent des affaires étrangères et du développement international, il y a un témoin qui a souligné l'importance, je dirais, de faire preuve de rigueur et de prudence lorsqu'on appuie une initiative internationale. Or il y a plusieurs initiatives de gouvernance et de surveillance de l'intelligence artificielle qui émergent actuellement, notamment de la Chine et des États-Unis. À quel point faut-il donc être prudent relativement à ces initiatives, si elles proviennent d'un autre État? Est-ce qu'il ne serait pas mieux que nous soyons un chef de file multilatéral dans ce genre d'initiative, plutôt que de nous joindre à une initiative du genre?

Samuel Buteau: Je pense que les États-Unis sont en ce moment le seul État qui a la capacité unilatérale d'imposer le genre de régime que ça va prendre pour prévenir le développement de ce que j'appelle l'intelligence artificielle superintelligente. Donc, on parle vraiment d'une petite fraction du marché de l'intelligence artificielle, ici. C'est vraiment ce qui pose les risques d'extinction dont les experts ont discuté.

Le rôle du Canada, je pense qu'il est très important. On peut donner un exemple que les autres pays vont vouloir suivre, peu importe ce que les autres superpuissances décident de faire ou de ne pas faire.

Alexis Brunelle-Duceppe: Merci beaucoup, je vous suis franchement reconnaissant.

Monsieur Penney, vous allez faire la dernière intervention aujourd'hui au Comité. Je vous remercie beaucoup d'avoir participé à notre réunion. Je vous laisse le mot de la fin, s'il y a quelque chose que vous voulez ajouter et que vous n'avez pas eu le temps de mentionner.

● (1730)

[*Traduction*]

Jonathon Penney: Je vous en suis reconnaissant. Je dirais simplement que c'est un moment charnière. Nous sommes entrés dans une ère très dangereuse, où ces technologies et ces outils se développent à une échelle et à un rythme sans précédent. Nous avons de la difficulté à suivre. Nous avons du mal à suivre le rythme. En même temps, nous vivons une période sans précédent de développement et d'innovation pour ces outils. Ils sont rapidement utilisés à ces fins abusives, de sorte que les violations des droits de la personne sont plus faciles, plus efficaces et plus fluides. Il y a des mesures claires et concrètes que nous pouvons prendre.

Je remercie le Comité de m'avoir invité à lui faire part de mes opinions là-dessus. Merci.

Le président: Merci.

Au nom du Sous-comité, je tiens à vous remercier tous les deux, monsieur Penney et monsieur Buteau. Merci d'être venus. Je vous remercie de vos remarques pertinentes et de vos excellentes réponses aux questions. Elles éclairent le Sous-comité.

Si l'un d'entre vous estime pouvoir fournir davantage d'information au Sous-comité, n'hésitez pas à écrire, soit au président, soit au greffier. Je vous remercie de votre présence.

La séance est levée. Merci.

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : https://www.noscommunes.ca

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: https://www.ourcommons.ca