CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

ENCADREMENT DES PLATEFORMES DE MÉDIAS SOCIAUX : ASSURER LA PROTECTION DE LA VIE PRIVÉE ET LA SÉCURITÉ EN LIGNE

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

John Brassard, président

DÉCEMBRE 2024
44e LÉGISLATURE, 1re SESSION

ENCADREMENT DES PLATEFORMES DE MÉDIAS SOCIAUX : ASSURER LA PROTECTION DE LA VIE PRIVÉE ET LA SÉCURITÉ EN LIGNE

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le président
John Brassard

DÉCEMBRE 2024

44e LÉGISLATURE, 1re SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

PRÉSIDENT

John Brassard

VICE-PRÉSIDENTS

Darren Fisher

René Villemure

MEMBRES

Parm Bains

Michael Barrett

Frank Caputo

Michael Cooper

Matthew Green

Anthony Housefather

Iqra Khalid

Brenda Shanahan

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

L'hon. Carolyn Bennett

Maxime Blanchette-Joncas

Alexandre Boulerice

Larry Brock

Pam Damoff

Eric Duncan

Ali Ehsassi

Nathaniel Erskine-Smith

L'hon. Mona Fortier

Marilyn Gladu

Jacques Gourde

Lisa Hepfner
Mike Kelloway
Damien C. Kurek
Vivane Lapointe
Bryan May
Glen Motz
Kyle Seeback
Francesco Sorbara
Karen Vecchio

GREFFIÈRE DU COMITÉ

Nancy Vohl

BIBLIOTHÈQUE DU PARLEMENT

Recherche et éducation

Alexandra Savoie, analyste
Maxime-Olivier Thibodeau, analyste

LE COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

a l'honneur de présenter son

SEIXIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(3)h) du Règlement, le Comité a étudié l'utilisation des plateformes de médias sociaux pour la collecte de données et le partage non éthique ou illicite de renseignements personnels avec des entités étrangères et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

SOMMAIRE

Les plateformes de médias sociaux font partie de l'écosystème d'information depuis maintenant plusieurs années. Une proportion importante de la population les utilise, dont des enfants et adolescents, qui partagent volontiers leurs renseignements personnels en ligne.

Ce rapport s'attaque à une question importante : comment peut-on mieux encadrer les plateformes de médias sociaux pour assurer la protection des renseignements personnels que la population canadienne fournit à ces plateformes, l'utilisation appropriée de ces renseignements, ainsi que la sécurité en ligne pour tous?

Le rapport fait d'abord un survol des pratiques des plateformes de médias sociaux, en se penchant entre autres sur leur modèle d'affaires et leurs pratiques en matière de collecte, d'utilisation et de partage de renseignements personnels, particulièrement en ce qui concerne les mineurs. Il reflète le contraste entre la façon dont les universitaires, experts et représentants de ces plateformes de médias sociaux décrivent et évaluent ces pratiques. Le rapport aborde également les mesures que ces plateformes mettent en œuvre pour assurer la sécurité des données qu'elles recueillent, pour lutter contre les menaces externes et pour contrer les tentatives d'ingérence étrangère.

Une attention particulière est par ailleurs accordée aux pratiques de TikTok, la plateforme de médias sociaux mentionnée expressément dans la motion qui a mené à l'étude du Comité. Par exemple, le Comité s'est intéressé à l'interdiction de cette application sur les appareils du gouvernement du Canada.

Enfin, le rapport résume les mesures, législatives ou autres, proposées par les témoins pour assurer un meilleur encadrement des plateformes de médias sociaux. Il aborde aussi l'éducation et la sensibilisation, deux éléments considérés comme étant primordiaux par plusieurs témoins pour contrer les efforts d'acteurs malveillants qui utilisent les plateformes de médias sociaux à des fins néfastes.

À la lumière des témoignages entendus, du mémoire qu'il a reçu et de documents additionnels fournis par certains témoins, le Comité formule 8 recommandations.

LISTE DES RECOMMANDATIONS

À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.

Recommandation 1

Recommandation 2

Recommandation 3

Recommandation 4

ENCADREMENT DES PLATEFORMES DE MÉDIAS SOCIAUX : ASSURER LA PROTECTION DE LA VIE PRIVÉE ET LA SÉCURITÉ EN LIGNE

INTRODUCTION

Le 31 janvier 2023, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (le Comité) a adopté la motion suivante :

> Que, conformément à l'article 108(3)h) du Règlement, le Comité entreprenne une étude de l'utilisation des plateformes de médias sociaux telles que TikTok et sa société mère, ByteDance Ltd., mais sans s'y limiter, et de leur participation ou utilisation de renseignements privés de Canadiens dans le but de recueillir des données et de partager de façon illicite ou contraire à l'éthique des renseignements personnels avec des entités étrangères; que le Comité étudie si ces données et renseignements privés de Canadiens sont protégés et stockés de façon adéquate; que le Comité invite des témoins pertinents du Centre canadien de la sécurité des télécommunications, des cadres clés de ByteDance Ltd., des experts en cybersécurité et des organismes de surveillance; que le Comité consacre au moins trois réunions avec les témoins à cette étude; et que le Comité fasse rapport de ses conclusions à la Chambre.

Interprétant cette motion de façon large, le Comité s'est aussi intéressé à d'autres aspects des plateformes de médias sociaux, comme leur modèle d'affaires, leurs pratiques en matière de protection des renseignements personnels, particulièrement en ce qui concerne les mineurs, et la modération de contenu. L'étude découlant de cette motion s'est étalée du 18 octobre au 13 décembre 2023. Le Comité a tenu six réunions publiques, a entendu 24 témoins et a reçu un mémoire.

Le rapport est divisé en 4 chapitres. Le premier chapitre traite principalement des pratiques des plateformes de médias sociaux, telles qu'elles ont été décrites par des experts et universitaires et par les représentants des plateformes. Le deuxième chapitre discute entre autres du partage potentiel de renseignements personnels recueillis par des plateformes de médias sociaux avec des acteurs étrangers. Le chapitre 3 se penche sur certaines mesures, législatives, réglementaires ou autres, qui permettraient au Canada de mieux encadrer les plateformes de médias sociaux. Enfin, le chapitre 4

aborde l'éducation et la sensibilisation. Les recommandations du Comité sont insérées dans les chapitres pertinents.

CHAPITRE 1 : PRATIQUES DES PLATEFORMES DE MÉDIAS SOCIAUX ET ENJEUX LIÉS

Survol général des pratiques

Comme l'a expliqué Brett Caraway, professeur agrégé de l'économie des médias à l'Université de Toronto, de nombreuses données sont recueillies par les entreprises de médias sociaux les plus importantes, comme Facebook, Google, Instagram et TikTok. Elles recueillent tous les renseignements personnels de leurs utilisateurs et suivent également toutes leurs données transactionnelles et les données relatives à leurs interactions. Par exemple, Facebook a du succès parce qu'elle est capable d'exploiter les liens sociaux de ses utilisateurs à grande échelle et Google a du succès car elle peut exploiter l'intention d'achat de ses utilisateurs à grande échelle, selon lui.

M. Caraway a dit que l'intérêt public et les intérêts privés divergent trop souvent dans le marché des plateformes numériques. Il a expliqué que les utilisateurs, les annonceurs et l'exploitant de la plateforme ont chacun leur propre ensemble d'incitatifs. Il a donné l'exemple d'Instagram, qui a pour incitatif financier de maximiser le nombre d'utilisateurs et leur niveau de participation, ce qui rend la plateforme plus attrayante pour les annonceurs. Les annonceurs veulent le plus de renseignements possible sur les utilisateurs afin de minimiser l'incertitude. Les utilisateurs, pour leur part, veulent simplement profiter des fonctionnalités de la plateforme avec le moins de perturbations possible, selon lui.

M. Caraway a expliqué que chaque fois qu'une recherche est effectuée sur Google, qu'une vidéo est regardée sur TikTok, qu'une publication est aimée sur Facebook ou qu'un gazouillis est partagé sur X, l'information est recueillie, des enchères ont lieu et des messages commerciaux sont livrés. Il a fait part de ses préoccupations concernant les répercussions négatives qu'ont ces plateformes sur la sphère publique, même lorsqu'elles fonctionnent exactement comme prévu. Le modèle d'affaires des plateformes garantit pratiquement la propagation de la désinformation, les efforts pour influencer les comportements et l'érosion de la vie privée, selon lui.

Dans la même veine, Anatoliy Gruzd, professeur et titulaire de la Chaire de recherche du Canada sur les technologies numériques de protection des renseignements personnels à la Toronto Metropolitan University, a indiqué que les personnes qui partagent des renseignements personnels sur des plateformes de médias sociaux ou un

site Web sont suivies, une pratique qu'il qualifie d'omniprésente dans tous les domaines et dans toute l'industrie.

Concernant les risques découlant de l'utilisation des plateformes de médias sociaux, Emily Laidlaw, professeure agrégée et titulaire de la Chaire de recherche du Canada en droit de la cybersécurité à l'Université de Calgary, a argué que la protection de la vie privée n'est qu'une partie de l'équation. Elle a donné l'exemple de Discord, une plateforme qui n'utilise pas d'outils pour détecter le contenu montrant l'exploitation sexuelle d'enfants, ne surveille pas le contenu diffusé en direct et n'offre pas d'outil pour faire des signalements. Selon elle, cet exemple dénote un problème de conception de la sécurité qui s'ajoute à un problème de protection de la vie privée. Malheureusement, de nombreuses plateformes populaires font seulement le minimum pour gérer les risques associés à leurs produits, selon M^{me} Laidlaw.

Faisant écho à certains propos d'autres témoins, Joe Masoodi, analyste principal des politiques chez The Dais, un institut de politique publique et de leadership à l'Université métropolitaine de Toronto, a expliqué que les plateformes de médias sociaux recueillent, transfèrent et stockent une grande variété de renseignements personnels et sensibles, y compris des renseignements d'identification personnelle, des messages privés, des données relatives à l'emplacement d'une personne, des données financières et des données biométriques.

Selon M. Masoodi, les plateformes de médias sociaux ont été conçues pour maintenir les personnes en ligne et les inciter à s'engager afin de recueillir le plus de données possible à leur sujet. Les plateformes regroupent ensuite ces données pour créer des profils détaillés et faire des déductions sur les personnes, notamment sur leurs opinions politiques, leur orientation sexuelle, leur religion, leurs revenus, leur santé ou des détails sur leur famille. M. Masoodi a argué que cela décrit les pratiques de TikTok, mais aussi de la plupart des grandes plateformes en ligne.

De l'avis de M. Masoodi, il n'existe actuellement aucune protection adéquate sur la manière dont les données personnelles des Canadiens sont transférées et stockées, en particulier à l'étranger, malgré les risques importants que représente l'utilisation potentiellement abusive de ces données. Il a argué que cette absence de protection adéquate menace la souveraineté du Canada et la sécurité numérique et la vie privée de sa population.

Parmi les risques encourus, M. Masoodi a mentionné l'accès aux données personnelles des Canadiens par les agences de sécurité nationale et d'application de la loi de certains

pays qui ne disposent pas de protections juridiques suffisantes, comme la Chine[1]. À ce risque s'ajoute la possibilité que les entreprises technologiques fassent l'objet de rachats, de fusions ou de faillites qui pourraient modifier l'endroit et la manière dont les données personnelles sont stockées et la protection de la vie privée offerte par ces entreprises. Des acteurs malveillants pourraient également tirer parti de données dont les garanties sont insuffisantes, selon M. Masoodi.

En ce qui concerne le transfert transfrontalier de données, Sam Andrey, directeur général de The Dais, a mentionné un rapport intitulé « Home Ice Advantage », co-rédigé avec M. Masoodi et leur ancien collègue, Yuan Stevens, qui s'est penché sur la sécurité transfrontalière des données des plateformes de médias sociaux. Les mesures qui permettraient de mieux encadrer les transferts transfrontaliers de données sont discutées davantage au chapitre 3 du présent rapport[2].

Cette vue d'ensemble donne un aperçu des nombreuses questions soulevées par les témoins en ce qui concerne la manière dont les plateformes de médias sociaux fonctionnent, recueillent, utilisent, stockent et partagent les données, qui affecte les utilisateurs de ces plateformes. Le présent chapitre fournit plus de détails sur les pratiques des plateformes de médias sociaux. Les témoignages entendus par le Comité mettent en évidence le contraste entre la manière dont les universitaires et les parties prenantes évaluent ces pratiques et l'évaluation qu'en font les plateformes.

Un modèle d'affaires basé sur les revenus publicitaires et l'économie de l'attention

Philippe Dufresne, le commissaire à la protection de la vie privée du Canada, a rappelé l'expression « si c'est gratuit, c'est que vous êtes le produit » pour expliquer l'importance que les Canadiens comprennent que, même s'ils ont l'impression de recevoir un produit ou un service gratuit, ils cèdent un élément fondamental de leur identité aux entreprises qui recueillent leurs renseignements personnels. Dans le même ordre d'idées, M. Caraway a rappelé que, même si certains services semblent gratuits, dans un modèle financé par la

1 Un autre exemple est la possibilité pour les autorités d'application de la loi des États-Unis, en vertu du *Foreign Intelligence Surveillance Act*, de contraindre un fournisseur de services de communication, soumis à la législation américaine, à communiquer des données sous son contrôle. Voir : Stevens, Y., Masoodi, M.J. & Andrey, S, *Home Ice Advantage : Securing Data Sovereignty for Canadians on Social Media*, Cybersecure Policy Exchange, 2020, p. 13 [DISPONIBLE EN ANGLAIS SEULEMENT]. En ce qui concerne les cybermenaces étrangères, comme indiqué plus loin dans le présent rapport, les témoins ont identifié des pays autres que la Chine qui mènent de telles activités, notamment la Russie, l'Iran, la Corée du Nord et le Mexique.

2 Stevens, Y., Masoodi, M.J. & Andrey, S, *Home Ice Advantage: Securing Data Sovereignty for Canadians on Social Media*, Cybersecure Policy Exchange, 2020 [DISPONIBLE EN ANGLAIS SEULEMENT].

publicité, les utilisateurs paieront pour ces services plus tard au moment d'acheter des biens ou des services. M. Gruzd a abondé dans le même sens.

M. Caraway a affirmé que le modèle d'affaires pousse les annonceurs à toujours demander plus de données et, par conséquent, les exploitants de plateformes à en recueillir davantage. En effet, dans le modèle d'affaires des plateformes, il n'existe aucune réelle limite supérieure à l'exploitation de l'attention humaine, selon lui. Il a rappelé que la fonction économique de la publicité est d'accaparer notre attention, qui est par nature limitée, au détriment d'intérêts concurrents. M. Caraway a argué que la façon dont nous choisissons d'accorder notre attention est importante, autant d'un point de vue individuel que sociétal : « Notre attention façonne notre identité, qui nous pourrions devenir et où nous pourrions aller. »

À cet égard, M^me^ Laidlaw a noté qu'une grande partie de la transparence dont font preuve les entreprises actuellement relève davantage d'un exercice de marketing que d'un portrait franc de certaines de leurs pratiques, particulièrement en ce qui concerne la publicité visant les enfants.

Collecte, utilisation et partage de données

Sharon Polsky, la présidente du Conseil du Canada de l'accès et la vie privée, a souligné que de nombreuses entreprises récupèrent des données qu'elles considèrent publiques parce qu'elles se trouvent en ligne. Selon elle, il est trop facile pour une organisation d'utiliser les renseignements personnels recueillis en ligne pour influencer l'opinion de la population à l'égard des politiques publiques, du gouvernement, des législateurs, des enseignants et des institutions. Il s'agit d'une menace pour la démocratie, les libertés civiles et les droits de la personne, selon elle.

Concernant le fait que les entreprises de médias sociaux savent ou non que leurs données sont détournées ou qu'elles permettent une mauvaise utilisation de leurs données par des tiers, M^me^ Laidlaw a avancé que c'est un peu des deux : les entreprises ne donnent pas un portrait complet de la situation, mais elles ne savent pas tout ce qui se passe non plus. Elle a affirmé que diverses applications qui indiquent être dotées de toutes les mesures de protection de l'enfance disponibles, n'offrent pas ces mesures de protection dans les faits. Elle n'a pas précisé à quelles applications elle faisait référence.

Contenu explicite et exploitation des enfants

Certains membres du Comité ont posé des questions concernant la propagation de contenu sexuellement explicite en ligne. Jeanette Patell, cheffe des affaires

gouvernementales et des politiques publiques du Canada pour Google et YouTube, et Rachel Curran, cheffe des politiques publiques pour le Canada chez Meta Platforms Inc. (Meta), ont affirmé que la pornographie et le contenu sexuellement explicite sont interdits sur YouTube et Facebook. Quant à lui, Wifredo Fernández, chef des affaires gouvernementales pour les États-Unis et le Canada chez X Corporation (X), a expliqué que les utilisateurs de moins de 18 ans – et ceux qui n'ont pas indiqué leur date de naissance dans leur profil – ne peuvent pas consulter le contenu explicite qui se retrouve sur X.

Les représentantes de Google et de Meta ont aussi expliqué de quelle façon le contenu sexuellement explicite est supprimé de leurs plateformes et comment les motifs de la suppression de contenu sont publiés. Par exemple, selon Google, comme M^me^ Patell l'a expliqué, le contenu interdit est d'abord détecté par les machines dans plus de 90 % des cas, ce qui permet à Google de s'attaquer à ce problème rapidement et à grande échelle.

M^me^ Curran a précisé que les restrictions sur la publication de contenu d'actes sexuels s'appliquent également aux contenus créés numériquement, sauf s'ils sont publiés à des fins éducatives ou satiriques.

M. Fernández a expliqué que X a limité la recherche de ce type de matériel au cours de la dernière année, a accru la formation des agents pour qu'ils déclarent les incidents à la ligne de signalement pour les cybermenaces et a automatisé son processus de signalement à la ligne de dénonciation du National Center for Missing and Exploited Children (NCMEC) aux États-Unis, qui agit comme centre d'information mondial pour les lignes de signalement de différentes administrations.

À cet égard, M^me^ Patell a noté que Google et YouTube fournissent des condensés numériques de contenu lié à l'exploitation sexuelle des enfants au NCMEC et à d'autres plateformes, dans le but que ce matériel ne soit pas retransmis ailleurs. M^me^ Curran a ajouté que Meta appuie l'élaboration d'un outil de gestion de cas pour les signalements en ligne faits au NCMEC.

M. Fernández a aussi mentionné que X a récemment annoncé un partenariat avec Thorn, une organisation qui lutte contre l'exploitation sexuelle des enfants, pour améliorer sa capacité de détection de contenu à caractère sexuel. Quant à Meta, M^me^ Curran a noté qu'elle a établi des partenariats avec d'autres experts de la lutte contre la traite des personnes et des organismes de protection de l'enfance, comme OneChild au Canada, Polaris et Stop the Traffik, en plus de Thorn.

M^me^ Curran a également noté que Meta a mis au point de nouvelles technologies pour empêcher l'utilisation de ses plateformes à des fins d'exploitation sexuelle des enfants. Meta aurait supprimé plus de 34 millions de publications d'exploitation juvénile de

Facebook et d'Instagram au quatrième trimestre de 2022 et plus de 98 % de ces cas ont été détectés avant d'être signalés. Pour détecter et prévenir la manipulation des enfants ou les interactions potentiellement inappropriées entre mineurs et adultes, Meta utilise une combinaison de technologies et de signaux comportementaux[3].

Le Comité note qu'en dépit des efforts déployés par les représentants des plateformes de médias sociaux, les contenus sexuellement explicites, dont certains concernent les enfants, semblent manifestement rester présents sur ces plateformes. En janvier 2024, par exemple, les directeurs généraux des cinq principales sociétés de médias sociaux, Meta, Snap, Discord, TikTok et X, ont comparu devant la commission judiciaire du Sénat américain pour discuter de la disponibilité de contenus préjudiciables pour les enfants sur ces plateformes, y compris de matériel pédopornographique[4].

Du côté des forces de l'ordre, Bryan Larkin, sous-commissaire, Services de police spécialisés de la Gendarmerie royale du Canada (GRC) a noté que la GRC entretient une relation continue avec toutes les plateformes de médias sociaux, par l'intermédiaire du Centre national de coordination contre la cybercriminalité. La GRC a aussi mis en place des protocoles, notamment en ce qui concerne l'exploitation des enfants et les préjudices causés aux jeunes.

Demandes légitimes d'« accès légal » de gouvernements et suppression de contenu

Les représentants de Google, Meta et X ont expliqué le processus selon lequel ils évaluent les demandes légitimes d'« accès légal » aux renseignements sur les utilisateurs ou de suppression de contenu provenant de différents gouvernements en fonction des lois américaines, des lois locales et des normes internationales – comme les Principes de liberté d'expression et de respect de la vie privée de la Global Network Initiative[5] – et comment ils publient cette information dans des rapports de transparence ou sur leur site Web. Les représentants de TikTok ont fourni une explication semblable dans leur réponse écrite[6].

3 Chambre de communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI), *Témoignages*, Rachel Curran (cheffe des politiques publiques pour le Canada, Meta Platforms Inc.).

4 États-Unis, Senate Committee on the Judiciary, *Protecting Children Online* [DISPONIBLE EN ANGLAIS SEULEMENT].

5 Google Canada, *Réponse écrite soumise au Comité ETHI*, p. 2 [HYPERLIEN NON DISPONIBLE].

6 TikTok, *Réponse écrite soumise au Comité ETHI*, p. 2 [HYPERLIEN NON DISPONIBLE].

M^me^ Patell a ajouté à cet égard que si une demande vise à obtenir trop d'information, selon l'équipe de Google concernée, cette dernière essaie de la circonscrire et s'oppose même à toute divulgation d'information, dans certains cas. De la même façon, Nathaniel Gleicher, chef des politiques de sécurité chez Meta, a expliqué que Meta rejette les demandes jugées trop larges.

Dans une réponse écrite aux questions posées par les membres du Comité aux représentants de Google lors de leur comparution, il est également mentionné que Google reçoit parfois des demandes de renseignements dans le cadre de situations d'urgence, comme en cas d'alerte à la bombe, de fusillade dans une école, d'enlèvement, de prévention du suicide ou de disparition de personnes. Dans ces situations, Google a affirmé qu'elle fournirait des renseignements à une agence gouvernementale, dans la mesure où cela empêcherait une personne de mourir ou de subir un préjudice physique grave[7].

M. Fernández a précisé que les organismes d'application de la loi ont accès à un portail où ils peuvent présenter des demandes légitimes pour obtenir des données des utilisateurs de X ou la suppression de contenu.

En ce qui concerne la suppression de contenu, Steve de Eyre, directeur des politiques publiques et des affaires gouvernementales pour le Canada chez TikTok, a noté que les politiques de TikTok et les lignes directrices communautaires publiées sur son site Web décrivent ce qui n'est pas autorisé sur la plateforme. Une équipe de plus de 40 000 professionnels de la sécurité travaillerait chaque jour pour modérer le contenu et supprimer ce qui contrevient aux lignes directrices de TikTok. Les modérateurs de contenu se trouveraient partout dans le monde, y compris au Canada. Il a indiqué qu'un utilisateur peut signaler une vidéo qui viole les lignes directrices de TikTok à l'entreprise, qui la supprimera.

Par exemple, M. de Eyre a noté que pendant le deuxième trimestre de 2023, TikTok a retiré 885 vidéos, ce qui représente moins de 1 % de toutes les vidéos téléversées au Canada, et dont 90 % ont été retirées par TikTok, sans signalement d'un utilisateur à l'égard du contenu[8].

Du côté des forces de l'ordre, M. Larkin a mentionné que la GRC fait le suivi des demandes légitimes d'accès aux renseignements personnels des utilisateurs de médias sociaux, des ordonnances de production et des mandats de perquisition pour obtenir

7 Google Canada, *Réponse écrite soumise au Comité ETHI*, p. 2 [HYPERLIEN NON DISPONIBLE].

8 Tik Tok, *Content violations and bans* [DISPONIBLE EN ANGLAIS SEULEMENT]. TikTok indique qu'elle a recours à une évaluation automatisée et humaine pour détecter les violations de ses lignes directrices communautaires, prendre des mesures à cet égard et supprimer du contenu.

des renseignements supplémentaires de la part des plateformes de médias sociaux. Il a précisé que la GRC a des ententes permanentes avec les services de sécurité de ces plateformes pour recevoir et récupérer les renseignements demandés, qui deviennent alors des éléments de preuve dans une enquête.

Utilisation de l'intelligence artificielle à des fins d'ingérence étrangère ou de désinformation

Lindsay Hundley, responsable des politiques d'influence chez Meta, a noté que le phénomène d'ingérence étrangère utilisant du contenu généré par l'IA n'est pas nouveau : Meta a décelé des opérations utilisant des images contrôlées sur ses plateformes à compter de 2019. Elle a expliqué que Meta se base sur le comportement pour déceler ce type de contenu généré par l'IA et que plus du deux tiers des opérations d'images contrôlées supprimées par Meta en 2022 en comportaient.

M^me^ Hundley a ajouté que, plus récemment, Meta a décelé des opérations utilisant les dernières techniques en matière d'IA générative, ce qui posera des défis à l'avenir. Selon elle, l'expérience de Meta a montré qu'une approche basée sur le comportement demeure utile pour relever les premiers signes d'opérations d'influence secrètes parce que ces opérations, en publiant ce type de contenu, laissent de nombreux signaux comportementaux derrière eux, que Meta peut encore détecter.

Samy Khoury, dirigeant principal du Centre canadien pour la cybersécurité (CCC) affilié au Centre de la sécurité des télécommunications (CST), a dit que le CCC se préoccupe de la mauvaise utilisation de l'IA, comme lorsqu'utilisée pour amplifier la désinformation, au moyen de fermes de robots, par exemple. Le CCC est aussi préoccupé par la fuite d'information au moyen de l'IA dans le cadre d'interactions en ligne. C'est pourquoi il fournit des conseils et orientations à la population canadienne sur la façon d'utiliser des outils d'IA existants et sur la manière dont certains États tentent d'exploiter les algorithmes à leur profit.

Par exemple, M. Khoury a noté que le CCC fait de la recherche à la fine pointe de la technologie en matière d'IA, offre des présentations et publie des articles. Il travaille aussi en étroite collaboration avec le CST pour que ce dernier fournisse des directives aux ministères sur la manière d'utiliser l'IA.

M^me^ Hundley a offert un exemple concret de l'utilisation de l'IA pour des opérations d'influence. Elle a raconté comment Meta a détecté et supprimé une grappe d'activités de commentaires d'une opération d'influence, appelée « camouflage de pourriel », qui ciblait, entre autres, des Canadiens. Elle a expliqué que le camouflage de pourriel est

une opération de longue haleine qui transcende les frontières et que Meta, avec d'autres, a mis en œuvre des mesures ciblées à l'échelle mondiale depuis 2019 afin de contrer ce type d'opération. Elle a aussi noté qu'en août 2023, Meta a supprimé des milliers de comptes et de pages après avoir associé différentes grappes d'activités à une opération unique liée à des individus ayant des liens avec les forces de l'ordre chinoises.

Selon M^me^ Hundley, l'activité de camouflage de pourriel en question transcende les frontières. On en a retrouvé la trace sur plus de 50 plateformes et forums sur Internet, dont Facebook, Instagram, X, YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, LiveJournal, Vimeo et des dizaines d'autres plus petites. Cela démontre que toute la société doit être impliquée dans la lutte contre l'ingérence étrangère, selon elle.

Google a également mentionné effectuer un suivi du camouflage de pourriel « Dragon », également connu sous le nom de « Dragonbridge », comme l'a expliqué Shane Huntley, directeur principal du Groupe d'analyse des menaces. Cependant, M^me^ Hundley et M. Huntley ont noté que ces campagnes, malgré leur ampleur, n'ont pas nécessairement d'effets néfastes réels. Ce type d'opération finit souvent par ne pas interagir avec des utilisateurs réels.

Utilisation de l'intelligence artificielle par les forces de l'ordre

Dans une réponse écrite aux questions posées par les membres du Comité aux représentants de la GRC lors de leur comparution, il est mentionné que, du point de vue de l'application de la loi, la GRC considère l'IA comme « une technologie à double usage, qui peut aider les organismes d'application de la loi, surtout dans le cadre d'enquêtes complexes et riches en données, mais qui peut également être utilisée par les auteurs de menaces criminelles au Canada pour victimiser les Canadiens et nuire aux intérêts du Canada[9] ».

Selon la GRC, l'IA pourrait avoir des répercussions importantes pour le Canada dans ses efforts de lutte contre l'ingérence étrangère, car elle est un facteur de démultiplication pour la désinformation et permet la création d'hypertrucages, qui dépasseront de plus en plus la capacité humaine de détection[10]. La réponse écrite de la GRC affirme que :

> La GRC évalue la menace de l'utilisation criminelle de l'IA comme facteur dans un éventail d'activités criminelles, de la fraude à l'ingérence étrangère. Le développement rapide de la technologie basée sur l'IA et sa facilité d'accès par les acteurs de la menace criminelle sont des sujets de préoccupation connus. L'utilisation de l'IA générative pour

9 Gendarmerie royale du Canada, *Réponse écrite soumise au Comité ETHI*, p. 1 [HYPERLIEN NON DISPONIBLE].

10 *Ibid.*

> la création, l'amplification et la diffusion de désinformation et de mésinformation servira probablement à semer la méfiance à l'égard des institutions occidentales. La facilité de la création et une possible diffusion prolifique dépasseront vraisemblablement de loin les capacités des contre-discours des canaux officiels[11].

La GRC a ajouté dans sa réponse écrite qu'elle dispose d'une technologie qui peut être utile à toute enquête sur des infractions où l'IA aurait été exploitée à des fins malveillantes, incluant les hypertrucages, et dans n'importe quel contexte, y compris l'ingérence étrangère.

Ingérence étrangère en contexte électoral

En contexte électoral, M. Khoury a expliqué que le rôle du CCC est de collaborer avec Élections Canada pour s'assurer que les infrastructures électorales sont bien protégées, ce qu'il a fait durant les dernières élections fédérales. Il a précisé que ce rôle n'inclut pas d'examiner le contenu publié en ligne, le mandat du CCC étant plutôt de protéger la sécurité des infrastructures.

Brigitte Gauvin, la commissaire adjointe par intérim de la GRC, Police fédérale, Sécurité nationale, a précisé que la GRC a un mandat partagé avec le Bureau du commissaire aux élections fédérales en ce qui concerne les allégations d'ingérence étrangère durant les élections. Elle a expliqué que la GRC dispose d'une variété de moyens pour avertir les individus visés.

À cet égard, M. Fernández a mentionné la politique d'intégrité civique de X, qui cible quatre infractions potentielles : les renseignements trompeurs qui pourraient induire les électeurs en erreur sur la façon de participer à une élection, les renseignements trompeurs qui pourraient intimider les électeurs pour les empêcher de voter, les renseignements qui pourraient empêcher les gens de voter et l'usurpation d'identité. M. Fernández a également mentionné la fonctionnalité appelée « Notes de la communauté », qui permet aux utilisateurs de X d'ajouter du contexte au contenu qui pourrait être trompeur, selon eux, et d'ainsi aider d'autres lecteurs.

Selon M. de Eyre, l'entreprise a établi un partenariat avec Élections Canada pour concevoir un centre électoral bilingue intégré à l'application TikTok où les Canadiens pouvaient trouver de l'information fiable, par exemple sur l'endroit où ils pouvaient aller voter. Il a également mentionné que TikTok est signataire de la Déclaration du Canada sur l'intégrité électorale en ligne.

11 *Ibid.*

Les questions entourant les plateformes de médias sociaux et les acteurs étrangers sont développées davantage au chapitre 2. Les quatre sections suivantes contiennent des éléments de preuve fournis par les représentants des quatre plateformes de médias sociaux qui ont comparu devant le Comité au sujet de leurs pratiques. Comme nous l'avons déjà indiqué au chapitre 1, et comme nous le verrons au chapitre 3, qui discute des mesures législatives et autres qui pourraient être adoptées pour mieux protéger la vie privée et la sécurité en ligne, de nombreux témoins ne seraient probablement pas d'accord avec certaines déclarations faites par les représentants des plateformes concernant leurs pratiques, notamment l'idée qu'elles ne recueillent pas de données excessives.

Pratiques de TikTok : position des plateformes

Selon M. de Eyre, des millions de Canadiens et plus d'un milliard de personnes dans le monde utilisent TikTok.

Cette statistique semble être confirmée par le dernier rapport de Social Media Lab sur l'état des médias sociaux, qui montre que la majorité des neuf plateformes les plus utilisées par les Canadiens sont nord-américaines et américaines et que TikTok est la plateforme qui connaît la plus forte croissance[12].

Collecte et utilisation de données par TikTok

Selon M. de Eyre, TikTok recueille des informations que les utilisateurs choisissent de lui fournir. Les renseignements recueillis par TikTok incluent :

- Le numéro de téléphone ou le courriel (p. ex., pour créer un compte);
- La date de naissance (p. ex., pour proposer une expérience adaptée à l'âge de l'utilisateur);
- Les informations de paiements pour les comptes qui utilisent des fonctions payantes (p. ex., les cadeaux virtuels);

12 ETHI, *Témoignages*, Anatoliy Gruzd (professeur et titulaire de la Chaire de recherche du Canada sur les technologies numériques de protection des renseignements personnels, Toronto Metropolitan University); Philip Mai and Anatoliy Gruzd, *The State of Social Media in Canada 2022*, Social Media Lab, Toronto Metropolitan University, septembre 2022.

- Les mentions « j'aime », les partages et l'historique de navigation pour affiner la pertinence du contenu proposé;

- Les informations sur l'appareil, qui incluent par exemple des renseignements sur l'appareil utilisé, comme son modèle, son système d'exploitation et ses paramètres tel le fuseau horaire et la langue, afin d'exécuter des fonctions de sécurité (p. ex., la réduction des pourriels) et de permettre aux annonceurs d'optimiser et mesurer l'efficacité de leurs campagnes publicitaires;

- L'emplacement approximatif de l'utilisateur afin d'afficher du contenu et des publicités pertinents selon la région dans laquelle se trouve cet utilisateur[13].

Dans une réponse écrite aux questions posées par les membres du Comité lors de leur comparution, les représentants de TikTok ont également confirmé qu'elle recueille l'adresse IP de ses utilisateurs. Il y est aussi précisé que TikTok considère toute personne qui visite sa plateforme, qu'elle soit connectée à l'aide d'un compte ou non, comme un utilisateur. Tiktok recueillerait des utilisateurs non connectés à un compte TikTok certains renseignements techniques, comme la langue de leur appareil et son adresse IP[14].

M. Gruzd a confirmé ce fait. Il a noté qu'après avoir récemment installé l'application TikTok sur son téléphone, sans créer de compte, il a commencé à recevoir des demandes d'information de l'application comme la durée de vie de sa pile et l'identifiant de son appareil.

Au sujet de l'emplacement d'un utilisateur, David Lieber, chef des Politiques publiques en matière de vie privée pour les Amériques chez TikTok, a expliqué que l'entreprise ne recueille pas d'information de localisation précise, mais plutôt l'emplacement approximatif de l'utilisateur, en utilisant l'adresse IP, par exemple pour déterminer dans quelle province ou quelle ville se trouve cette personne.

Les représentants de TikTok ont également indiqué qu'elle recueille le contenu des messages sur sa plateforme pour alimenter la fonction de messagerie directe, mais qu'elle ne recueille pas les messages provenant d'autres applications.

---

13 TikTok, *Réponse écrite soumise au Comité ETHI*, p. 1 et pp. 5-6 [HYPERLIEN NON DISPONIBLE]. TikTok, *Privacy Policy* [DISPONIBLE EN ANGLAIS SEULEMENT]. Une description plus détaillée de tous les types d'informations collectées par TikTok se trouve dans la politique de confidentialité.

14 TikTok, *Réponse écrite soumise au Comité ETHI*, p. 2 [HYPERLIEN NON DISPONIBLE].

> TikTok peut accéder au contenu de la messagerie directe de l'application même, par exemple, pour promouvoir la sûreté et la sécurité de la plateforme, ce qui peut comprendre l'examen de ce contenu et des métadonnées pour des violations de ses conditions de service ou des lignes directrices de la communauté, ou encore des menaces pour la sûreté et la sécurité de sa communauté et du public en général[15].

Selon ses représentants, TikTok ne se livre à aucune collecte agressive de données. Elle recueille les informations que ses utilisateurs choisissent de lui fournir et celles qui permettent à l'application de fonctionner en toute sécurité et d'améliorer l'expérience des utilisateurs.

En ce qui concerne la collecte de données biométriques par TikTok, M. Lieber a confirmé qu'elle n'utilise pas de telles données pour identifier ses utilisateurs. TikTok a confirmé qu'elle ne collecte ni n'utilise de données biométriques pour « déduire » des caractéristiques d'utilisateurs comme l'âge, le sexe et les centres d'intérêt. Cependant, elle utilise des renseignements relatifs à l'image et à la voix à d'autres fins que l'identification, par exemple lorsqu'un utilisateur décide d'utiliser un effet visuel ou un filtre[16].

Dans sa réponse écrite, TikTok explique aussi qu'elle n'identifie personne et ne déduit pas de renseignements de nature délicate en fonction de ce qu'un utilisateur visionne sur sa plateforme[17]. M. de Eyre a expliqué le fonctionnement de l'algorithme de TikTok de la manière suivante :

> Essentiellement, l'algorithme TikTok fonctionne en analysant votre réaction aux vidéos. Votre réaction à une vidéo est positive: vous l'aimez, vous la commentez ou vous la partagez? Regardez-vous toute la vidéo? La regardez-vous de nouveau? Votre réaction peut être négative: vous passez à une autre vidéo au bout de quelques secondes? À partir de là, nous pouvons déterminer les types de vidéos que vous aimez et examiner d'autres utilisateurs semblables qui ont interagi de la même façon avec cette vidéo, puis vous recommander du contenu supplémentaire. Cela permet vraiment aux Canadiens de trouver et de se faire recommander du contenu qui risque de leur plaire[18].

Dans sa réponse écrite, TikTok a expliqué que des contenus sont recommandés en classant les vidéos en fonction d'une combinaison de facteurs centrés sur les activités

15 *Ibid*., p. 6.

16 *Ibid*.

17 *Ibid*., p. 3.

18 Voir aussi : ETHI, *Témoignages*, Steve de Eyre (directeur, Politiques publiques et affaires gouvernementales, Canada, TikTok).

des utilisateurs. La fonction « Pourquoi cette vidéo » permettrait de mieux comprendre pourquoi une vidéo particulière est apparue dans le fil « Pour toi » d'un utilisateur[19].

Les utilisateurs de TikTok peuvent également influencer le contenu qu'ils voient, par exemple en utilisant la fonction « Pas intéressé(e) » pour voir moins de contenu d'un certain type. Un nouvel outil permet aussi de filtrer les vidéos contenant des mots-clés et des mots-clics qu'un utilisateur ne souhaite pas voir apparaître dans son fil « Pour toi ». Cette fonction fait partie de sa gamme d'outils de « Connexion Famille », la fonction de contrôle parental de TikTok[20].

En ce qui concerne les mineurs, M. de Eyre a dit que TikTok a élaboré des politiques inspirées par les recherches de pointe menées par des organismes à but non lucratif sur l'expérience en ligne des jeunes afin de leur offrir une expérience adaptée à leur âge. Par exemple, l'étiquetage du contenu adapté en fonction de l'âge a été intégré au système, ce qui fait en sorte que certains types de vidéos sont étiquetés et ne sont pas recommandés pour un utilisateur de moins de 18 ans. Pour recommander du contenu à ses utilisateurs, TikTok recueille aussi des renseignements sur ce qu'ils regardent et le temps passé à regarder la vidéo, cette donnée étant un facteur important pour déterminer si un contenu est pertinent et intéressant pour un utilisateur donné[21].

Partage et stockage des données recueillies par TikTok

M. Lieber a confirmé que les données recueillies par TikTok sont stockées sur ses serveurs aux États-Unis, à Singapour et en Malaisie. Selon M. de Eyre, les activités de TikTok au Canada sont assujetties aux lois canadiennes sur la protection des renseignements personnels, malgré le fait que les données soient stockées à l'extérieur du pays.

À cet égard, M. Dufresne a rappelé que la loi canadienne en matière de renseignements personnels s'applique si des Canadiens sont touchés. Un certain nombre de facteurs font en sorte que le CPVP a compétence, même si l'information est stockée ailleurs. Lorsqu'il y a un lien suffisant, la loi s'applique au traitement des renseignements personnels[22].

---

19 TikTok, *Réponse écrite soumise au Comité ETHI*, pp. 4-5 [HYPERLIEN NON DISPONIBLE].

20 *Ibid*., p. 5.

21 *Ibid*., p. 6.

22 Voir : *A.T. c. Globe24h.com*, 2017 CF 114 (CanLII). La Cour fédérale a déterminé que la *Loi sur la protection des renseignements personnels et les documents électroniques* avait une portée extraterritoriale parce qu'il existait un lien réel et important avec le Canada.

Revenant sur le témoignage de M. Lieber concernant l'endroit où sont situés les serveurs de TikTok, M. Andrey a toutefois argué qu'il s'agit d'un portrait incomplet de la situation parce qu'il est possible d'accéder aux serveurs de TikTok à distance, à partir de n'importe quel pays du monde.

Matt Malone, professeur adjoint, faculté de droit de Thompson Rivers University, a quant à lui expliqué que, selon la loi chinoise, particulièrement la *Loi nationale sur le renseignement*, les entreprises qui exercent des activités en Chine doivent coopérer avec la Chine. Une disposition de cette loi prévoit également son application extraterritoriale. Selon M. Malone, le fait que l'État chinois soit propriétaire à 1 % de TikTok et de ByteDance lui permet d'exercer son contrôle sur ces entreprises, ce qui signifie que les problèmes identifiés concernant le transfert de données ne sont pas près de disparaître. Les inquiétudes liées au contrôle de l'entreprise sont abordées davantage dans le chapitre 2.

En ce qui concerne le partage de données, M. Lieber a noté que certaines d'entre elles peuvent être partagées avec des partenaires publicitaires de TikTok. Les identifiants mobiles permettent d'établir le lien entre un utilisateur de TikTok et une action posée par cet utilisateur sur le site Web d'un annonceur. Il a indiqué que ces partenaires ont accès aux données uniquement pour comprendre, par exemple, comment leurs campagnes publicitaires sur TikTok ont fonctionné et obtenir des statistiques comme le nombre de personnes qui ont regardé une annonce.

En ce qui concerne le partage de données avec ByteDance, les représentants de TikTok ont noté que la collecte de renseignements d'utilisateurs canadiens se fait de façon conforme à la politique de confidentialité de l'entreprise. Certaines entités de ByteDance fournissent des services qui soutiennent le fonctionnement de la plateforme TikTok et ont donc accès à distance aux données d'utilisateurs canadiens. Selon ses représentants, TikTok s'assure que seules les personnes qui en ont vraiment besoin ont accès à ces données en recourant à des moyens de contrôle robustes et des mesures de protection comme le cryptage et un processus d'approbation en plusieurs étapes fondé sur les principes du besoin de connaître et du moindre privilège[23].

M. Lieber a en fait expliqué que TikTok suit le principe d'accès minimal, c'est-à-dire que tout employé qui souhaite avoir accès aux données de ses utilisateurs doit présenter une demande et obtenir une approbation à l'issue d'un examen rigoureux. Il a rajouté que TikTok a des politiques de classification des données qui prévoient des degrés croissants de confidentialité, les données des utilisateurs étant les plus confidentielles.

23 TikTok, *Réponse écrite soumise au Comité ETHI*, p. 1 [HYPERLIEN NON DISPONIBLE].

Sécurité des données

En ce qui concerne la sécurité des données des utilisateurs canadiens, M. Lieber a noté que TikTok a une politique de confidentialité, qu'elle publie des renseignements sur les données qu'elle recueille, sur leur utilisation, la façon dont elles pourraient être divulguées et dans quelles conditions. TikTok offre aussi à ses utilisateurs des réglages détaillés qu'ils peuvent utiliser pour protéger leurs renseignements, selon lui. TikTok a aussi noté que l'entreprise a une certification ISO 27001, l'une des normes de sécurité de l'information les plus reconnues à l'échelle mondiale, y compris aux États-Unis[24].

Dans sa réponse écrite, TikTok a expliqué qu'elle applique un programme rigoureux de gestion des tiers pour garantir que ses partenaires respectent les mêmes normes de sécurité qu'elle[25]. TikTok a aussi précisé que, comme c'est le cas pour d'autres plateformes, sa politique de confidentialité indique qu'elle ne peut garantir la sécurité des renseignements transmis par la plateforme.

Pratiques concernant les mineurs

Selon M. de Eyre, TikTok a développé des mesures visant à protéger les adolescents, par exemple en restreignant l'âge auquel une personne peut créer un compte. M. Lieber a indiqué qu'un des mécanismes de contrôle utilisé par TikTok pour empêcher l'ouverture de compte par des personnes de moins de 13 ans est qu'elle ne fournit aucune indication concernant l'âge d'admissibilité, ce qui fait en sorte que les nouveaux utilisateurs ne savent pas qu'en fournissant leur âge, ils indiquent à TikTok s'ils ont l'âge requis pour ouvrir un compte.

M. Lieber a indiqué que pendant le deuxième trimestre de 2023, TikTok a supprimé à l'échelle internationale 18 millions de comptes parce qu'elle estimait que l'utilisateur avait peut-être moins de 13 ans.

Dans sa réponse écrite, TikTok a précisé que sa plateforme est destinée aux utilisateurs de 13 ans ou plus (14 ans au Québec), qu'elle offre des paramètres de confidentialité adaptés à l'âge et qu'elle intègre certaines protections par défaut. Par exemple, les comptes des jeunes de 13 à 15 ans sont privés par défaut. La messagerie directe est désactivée pour les utilisateurs de moins de 16 ans. Les comptes d'utilisateurs de moins de 18 ans ne peuvent pas utiliser la fonction de diffusion en direct, et chaque compte

24 Organisation internationale de normalisation, ISO/IEC 27001:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences.

25 TikTok, *Réponse écrite soumise au Comité ETHI*, p. 2 [HYPERLIEN NON DISPONIBLE].

appartenant à un utilisateur de moins de 18 ans est soumis par défaut à une limite de temps d'écran de 60 minutes par jour[26].

Cependant, ces paramètres peuvent simplement être modifiés, comme M. Caraway l'a indiqué, et un utilisateur peut continuer à utiliser l'application en saisissant un code d'accès après que les 60 minutes se sont écoulées.

TikTok a mentionné d'autres mesures de protection, comme le contrôle parental, qui peut être activé en liant le compte TikTok du parent à celui de son adolescent. Ce contrôle parental inclut la gestion du temps d'écran, la programmation des notifications et la limitation de l'affichage dans le fil d'actualité de l'enfant de contenu qui pourrait ne pas être adapté à son âge[27].

En ce qui concerne l'éducation des jeunes, M. de Eyre a indiqué que TikTok s'associe à des organismes canadiens sans but lucratif comme HabiloMédias, Jeunesse, j'écoute, Tel-jeune et Digital Moment pour appuyer le travail d'éducation de la population canadienne et créer des ressources pour la sécurité en ligne, le bien-être et la littératie numérique[28].

Dans sa réponse écrite, TikTok mentionne que lorsque certains mots-clés sont recherchés, les recherches sont redirigées vers des ressources de soutien et que certains mots-clics nuisibles sont bloqués[29].

En ce qui concerne la sensibilisation des adolescents sur les données qu'ils communiquent, M. de Eyre a réitéré que plusieurs paramètres existent sur TikTok pour protéger les mineurs et qu'au Canada, TikTok s'efforce de collaborer avec des organismes à but non lucratif dans ses efforts de sensibilisation des jeunes à des sujets comme la partialité algorithmique.

Contredisant les propos de TikTok, M. Malone a affirmé que TikTok – comme de nombreux autres médias sociaux – est responsable de violations des droits de la personne, qu'elle a des pratiques répréhensibles de collecte de données et de contrôle du discours, et qu'elle a permis l'accès à des données malgré l'assurance du contraire.

Selon M. Malone, TikTok – comme d'autres médias sociaux – est un « vecteur de préjudice en ligne » pour les jeunes. À l'appui de cette affirmation, il a donné comme exemple le modèle économique de TikTok axé sur la publicité ciblée, qui porte atteinte à

26 *Ibid*., p. 3.

27 *Ibid*.

28 Voir aussi : ETHI, Témoignages, de Eyre; ETHI, *Témoignages*, David Lieber (chef, Politiques publiques en matière de vie privée pour les Amériques, TikTok).

29 TikTok, *Réponse écrite soumise au Comité ETHI*, pp. 3-4 [HYPERLIEN NON DISPONIBLE].

la vie privée et exacerbe la crise de la santé mentale qui touche les jeunes, ainsi que les fonctions de sécurité de l'application pour les enfants qui sont toutes faciles à contourner. M. Malone a affirmé avoir vu – grâce à diverses demandes d'accès à l'information – plusieurs séances d'information internes où des représentants du gouvernement canadien ont relevé ces problèmes.

Pratiques de Meta : position des plateformes

L'affaire Cambridge Analytica

Le Commissariat à la protection de la vie privée du Canada a publié en 2019 un rapport d'enquête conjointe avec le Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique au sujet de Facebook dans l'affaire Cambridge Analytica. À l'issue de cette enquête conjointe, le Commissariat a fait des recommandations, car il n'a pas le pouvoir d'émettre une ordonnance. Le Commissariat a donc saisi la Cour fédérale et demandé qu'elle émette l'ordonnance qu'il recommandait. Ce processus est une procédure « de novo »[30]. Le commissaire a expliqué que la Cour fédérale a rejeté la demande du Commissariat, qui a interjeté appel sur les deux questions fondamentales soulevées devant la Cour : le consentement et les mesures de sécurité.

Revenant sur l'affaire Cambridge Analytica, M^me^ Curran a réitéré la position de Facebook, c'est-à-dire qu'il n'y avait aucune preuve que les renseignements d'utilisateurs canadiens avaient été communiqués à Cambridge Analytica, en soulignant que Meta ne vend pas les données de ses utilisateurs. Elle a rappelé que la Cour fédérale avait conclu dans cette affaire qu'il n'y avait pas suffisamment de preuves que les données d'utilisateurs canadiens avaient été communiquées et que les pratiques de communication des données de Facebook avaient été adéquatement divulguées.

Le 9 septembre 2024, la Cour d'appel fédérale a rendu une décision unanime, *Privacy Commissionner of Canada v. Facebook Inc* 2024 FCA 140 [EN ANGLAIS], qui renverse la décision de la Cour fédérale et conclut que les pratiques de Facebook entre 2013 et 2015 ont contrevenu à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) en n'obtenant pas le consentement éclairé de ses utilisateurs et en ne protégeant pas leurs données personnelles adéquatement. La Cour d'appel fédérale a demandé aux parties de faire rapport dans les 90 jours suivant la date de la décision pour indiquer si une entente sur les termes de l'ordonnance réparatoire a été

30 Commissariat à la protection de la vie privée du Canada (CPVP), *Enquête conjointe du Commissariat à la protection de la vie privée du Canada et du Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique au sujet de Facebook, Inc.*, Rapport de conclusions, 25 avril 2019; *Canada (Commissaire à la protection de la vie privée) c. Facebook, Inc.*, 2023 CF 533 (CanLII).

conclue. Le commissaire à la protection de la vie privée du Canada a déclaré qu'il s'attend à ce que Facebook présente maintenant de quelle façon elle s'assurera de respecter la décision de la Cour[31]. En date d'adoption du présent rapport, Meta n'avait pas indiqué si elle entend demander l'autorisation à la Cour suprême du Canada de faire appel de cette décision. Elle a 60 jours pour le faire après que la décision a été rendue[32].

Le Comité s'est penché sur l'affaire Cambridge Analytica à l'époque où le CPVP et le Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique enquêtaient sur Facebook. Le Comité avait d'abord publié un rapport provisoire, intitulé *Aborder les vulnérabilités de la vie privée numérique et les menaces potentielles au processus électoral démocratique canadien*. Un rapport final avait suivi, intitulé *Démocratie menacée : risques et solutions à l'ère de la désinformation et du monopole des données*. Ces deux rapports contenaient des recommandations de modifications législatives concernant notamment les plateformes de médias sociaux, le financement étranger et l'influence étrangère dans les élections au Canada ainsi que les pouvoirs du commissaire à la protection de la vie privée[33].

Protection de la vie privée

M^me^ Curran a argué que Meta a entièrement révisé ses pratiques de protection de la vie privée au cours des dernières années et que les considérations relatives à la protection de la vie privée sont désormais intégrées à l'ensemble de ses produits et services dès le début de la conception.

En ce qui concerne les nouveaux outils et fonctionnalités conçus par Meta au cours des dernières années pour les adolescents et leurs familles, M^me^ Curran a donné l'exemple des comptes d'adolescents qui sont réglés en mode « privé » lorsqu'ils s'inscrivent à Instagram ou à Facebook. Selon elle, Meta empêche les adultes qui ne sont pas suivis par des adolescents de leur envoyer des messages et limite la quantité de contenu qui pourrait être de nature délicate qu'ils peuvent voir dans les options « Explorer »,

31 CPVP, *Déclaration du Commissaire à la protection de la vie privée du Canada qui salue la décision de la Cour d'appel fédérale concernant Facebook*, 9 septembre 2024.

32 *Loi sur la Cour suprême*, articles 40 et 58(1).

33 Voir également : ETHI, *Grand comité international sur les mégadonnées, la protection des renseignements personnels et la démocratie*, juin 2019. Le Grand comité international était composé des membres du Comité et de parlementaires provenant de 10 autres pays et a tenu des réunions au cours desquelles il a entendu de nombreux témoins, dont des experts, universitaires, responsables de la réglementation et des représentants de plateformes numériques.

« Rechercher » ou « Reels ». M[me] Curran a ajouté que Meta interdit le contenu qui fait la promotion du suicide, de l'automutilation ou des troubles de l'alimentation.

Lutte contre les menaces externes

M. Gleicher a dit que Meta travaille à déceler et déjouer les menaces étrangères, notamment les opérations de piratage et de cyberespionnage, ainsi que les opérations d'influence, qu'il a appelées « comportements inauthentiques coordonnés » ou CIC, que Meta définit comme tout « effort coordonné visant à manipuler le débat public en vue d'atteindre un objectif stratégique, dans lequel les faux comptes sont au cœur de l'opération ».

M. Gleicher a expliqué qu'on parle de CIC lorsque des utilisateurs s'organisent et utilisent de faux comptes pour dissimuler leur identité et leurs activités. Il a expliqué que les normes de Meta interdisent les comportements inauthentiques, tels que se représenter faussement, utiliser de faux comptes ou gonfler artificiellement la popularité du contenu. Selon M. Gleicher, cette politique vise à protéger la sécurité des comptes des utilisateurs de Meta et de ses services, et à créer un espace où les individus peuvent faire confiance aux personnes et aux communautés avec lesquelles ils interagissent.

Selon M. Gleicher, les auteurs des menaces cherchent à s'immiscer dans le débat public et à le manipuler, à exploiter les fractures sociétales, à promouvoir la fraude, à influencer les élections et à viser une mobilisation sociale véritable. M. Gleicher a expliqué que les équipes de Meta responsables de la sécurité ont élaboré des politiques, des outils de détection automatisés et des cadres d'application des règles pour lutter contre les acteurs frauduleux étrangers et nationaux. Selon lui, ces investissements ont permis à Meta de contrer des millions de tentatives de création de faux comptes chaque jour, et d'en déceler et d'en supprimer des millions d'autres. Il a donné l'exemple de près de deux milliards de faux comptes désactivés par Meta en 2023, dont plus de 99 % ont été décelés en amont de tout signalement.

M. Gleicher a dit que Meta enquête de manière proactive pour dépister les campagnes de cyberespionnage et qu'elle fait rapport de ces activités de façon régulière dans ses rapports trimestriels, qui décrivent les mesures d'application prises. Meta communique aussi les renseignements sur toute activité décelée à d'autres acteurs de l'industrie pour leur permettre de prendre les mesures qui s'imposent.

Selon M. Gleicher, Meta a notamment constaté que ces campagnes de cyberespionnage sont des efforts d'envergure qui ciblent Internet dans son ensemble et sont souvent menées en parallèle avec des activités hors plateforme. M. Gleicher a ajouté que des

détails sur les régions ou les pays qui ont été particulièrement ciblés sont inclus dans les rapports trimestriels et que Meta publie également des renseignements sur les personnes ou les organisations responsables de l'opération lorsqu'elle détient des preuves à cet égard.

M^me^ Hundley, a expliqué que l'entreprise utilise une approche axée sur le comportement pour déceler les opérations d'influence secrètes, plutôt qu'une approche basée sur le contenu partagé par des acteurs mal intentionnés. Selon elle, Meta démantèle des réseaux comme ceux-ci, sans égard à qui se trouve derrière, à ce qu'ils publient, ou au fait qu'ils soient étrangers ou nationaux.

À titre d'exemple, M^me^ Hundley a expliqué que Meta a démantelé plus de 200 opérations d'influence secrètes, provenant de 68 pays dans au moins 42 langues. Elle a noté que Meta publie régulièrement ce type d'informations dans ses rapports sur les menaces et que le partage de ces informations a permis à ses équipes, ainsi qu'aux journalistes d'enquête, représentants gouvernementaux et autres membres de l'industrie de mieux comprendre et exposer les risques de sécurité sur Internet, notamment avant la tenue d'élections cruciales.

M^me^ Hundley a expliqué que, selon le dernier rapport de Meta, la Chine est maintenant au troisième rang des pays responsables de CIC étrangers qu'elle a réussi à désamorcer, après la Russie et l'Iran. Elle a noté qu'en 2023, Meta a démantelé cinq réseaux de CIC basés en Chine, ce qui est davantage que tout autre pays. Selon M^me^ Hundley, ces campagnes de CIC publiaient généralement du contenu lié aux intérêts chinois dans différentes régions du monde, par exemple en louant la Chine, en défendant son bilan au chapitre des droits de la personne au Tibet et au Xinjiang, ou en critiquant les détracteurs du gouvernement chinois, dont des journalistes et des chercheurs.

Comme indiqué ci-dessus, M^me^ Hundley a argué que la lutte contre les opérations d'influence étrangère est un effort qui concerne l'ensemble de la société. Selon elle, aucune plateforme de médias sociaux ne peut résoudre à elle seule le problème de l'ingérence étrangère, ce pourquoi Meta travaille avec ses pairs de l'industrie, des chercheurs indépendants, des journalistes d'enquête, le gouvernement et les forces de l'ordre.

Pratiques de X : position des plateformes

M. Fernández a expliqué que les utilisateurs de X peuvent choisir de créer un compte pseudonyme afin de protéger leur identité ou de contrôler qui peut voir leurs messages. Il a affirmé que X est guidée par le principe selon lequel les données ne devraient être utilisées qu'aux fins pour lesquelles elles ont été recueillies.

Selon M. Fernández, les paramètres du compte X permettent aux utilisateurs de faire divers choix au sujet de la protection de leurs données, notamment en limitant les données recueillies par X, en déterminant s'ils veulent voir de la publicité fondée sur leurs intérêts et en contrôlant la façon dont X personnalise leur expérience. Selon lui, X permet également aux utilisateurs d'accéder à des renseignements sur les annonceurs qui les ont inclus dans des auditoires personnalisés pour leur montrer des annonces, des données démographiques et des données d'intérêt sur leurs comptes auprès de partenaires publicitaires, et des renseignements que X a pu déduire à leur sujet.

M. Fernández a argué que la protection de la vie privée dès la conception est une priorité pour chaque produit conçu par X. Selon lui, X effectue des examens exhaustifs de la protection de la vie privée pour toutes les nouvelles caractéristiques et tous les nouveaux outils qu'elle déploie. X effectue aussi des évaluations supplémentaires des facteurs relatifs à la protection des données pour les produits qui peuvent présenter des risques accrus pour ses utilisateurs.

M. Fernández a ajouté que X a pris des mesures pour limiter la collecte non autorisée de données sur sa plateforme. À titre d'exemple, il a mentionné le recours à des équipes spécialisées qui surveillent, identifient et atténuent les activités de collecte de données dans une gamme de vecteurs et de plateformes; l'introduction de limites de taux pour limiter la capacité d'un acteur malveillant à extraire des données; l'élargissement des offres de vérification par l'utilisateur pour évaluer si un demandeur de compte donné est une vraie personne, et non un robot; et la mise à jour des conditions de service de X, qui mentionnent expressément que l'extraction est une utilisation abusive de ce service.

M. Fernández a expliqué que le fait d'utiliser X transmet à l'entreprise des renseignements personnels sur les utilisateurs, comme le type d'appareil utilisé et l'adresse IP. Selon M. Fernández, les utilisateurs peuvent choisir les renseignements supplémentaires qu'ils veulent communiquer à X, comme leur adresse de courriel, leur numéro de téléphone, les coordonnées de l'annuaire et leur profil public. Il a argué que X utilise notamment cette information pour assurer la sécurité des comptes et montrer aux utilisateurs des messages plus pertinents à suivre, comme des événements et des publicités.

M. Fernández a reconnu que X fait des affaires en grande partie grâce à la publicité, mais a avancé que certaines différences fondamentales la distinguent des nombreuses entreprises qui ont un modèle d'affaires semblable. En général, selon M. Fernández, plutôt que de se concentrer sur qui sont les utilisateurs, les données de X portent davantage sur ce qui les intéresse : ce qu'ils republient, ce qu'ils aiment et qui ils suivent; de l'information qui est publique.

Collecte de données biométriques

Josh Harris, conseiller principal en matière de protection de la vie privée et des données chez X a mentionné que les données biométriques dont il est question dans la nouvelle politique sur la protection de la vie privée de X sont des renseignements qui pourraient se trouver sur la carte d'identité d'une personne. Étant donné qu'il s'agit de renseignements plus sensibles que d'autres, plus de restrictions s'appliquent à leur conservation. Il a précisé que ces données ne sont pas utilisées par X pour entraîner des systèmes d'IA ou toute autre technologie. Selon M. Harris, X se sert des données biométriques pour prouver l'identité, lorsque le consentement parental est requis pour qu'une personne crée un compte, par exemple.

Dans une réponse écrite aux questions posées par les membres du Comité aux représentants de X lors de leur comparution, M. Fernández a confirmé que X peut recueillir des données biométriques à partir de pièces d'identité avec photo délivrées par le gouvernement à des fins de sécurité et aux fins de vérifications générales. Selon lui, X recueille ces données pour ses enquêtes et pour l'application de ses politiques, y compris lorsque le consentement d'un parent ou d'un tuteur légal est requis, ou lorsqu'un cas d'usurpation d'identité est signalé. Il existe aussi un processus volontaire de vérification de l'identité pour certaines fonctions de la plateforme X. La réponse écrite de X affirme qu'à l'heure actuelle, X n'a pas l'intention d'étendre la collecte de données biométriques au-delà de ces catégories[34].

Pratiques de Google : position des plateformes

Protection de la vie privée

Selon Mme Patell, Google conçoit des produits et services qui sont sécurisés par défaut et dont la conception est axée sur la protection de la vie privée. Elle a affirmé que Google dit clairement au public que la majorité de ses revenus proviennent de la publicité. Selon elle, Google s'est engagée auprès de ses utilisateurs à les mettre au courant de « la façon dont leurs renseignements servent à guider leur expérience, à leur donner des outils favorisant la transparence et, au bout du compte, à leur permettre de contrôler la façon dont leurs renseignements sont utilisés ».

Selon Mme Patell, l'information recueillie par Google contribue au bon fonctionnement et à l'efficacité de ses produits, les rend plus sûrs, les rend plus utiles et permet de détecter les fraudes et d'en diminuer le nombre. Elle a expliqué que Google offre des

34 X Corporation, *Réponse écrite soumise au Comité ETHI*, 22 décembre 2023, p. 2 [HYPERLIEN NON DISPONIBLE].

paramètres qui permettent aux utilisateurs de choisir la façon dont leurs renseignements sont recueillis et utilisés. Les utilisateurs peuvent procéder à ce que Google appelle une « vérification de la sécurité » et ils peuvent voir comment l'information est utilisée sur la page « Mes préférences publicitaires ». Les utilisateurs peuvent également supprimer l'information ou désactiver des éléments comme les annonces personnalisées.

M^me^ Patell a expliqué que Google fournit de l'information aux utilisateurs concernant la suppression de l'information ou la désactivation de certains éléments et a mis en place une fonction de suppression automatique pour les nouveaux comptes, qui fait en sorte que l'information est supprimée automatiquement au bout de 18 mois.

En ce qui concerne les politiques en matière de contenu sur YouTube, M^me^ Patell a expliqué que les conditions d'utilisation s'appliquent à tout le contenu sur la plateforme : commentaires, liens externes, la vidéo elle-même, etc. Elle a noté que Google compte plus de 20 000 personnes formées pour examiner les questions de confiance et sécurité qui évaluent si chaque élément du contenu se retrouvant sur la plateforme répond aux normes établies dans les conditions d'utilisation.

M^me^ Patell a affirmé que Google protège la vie privée de ses utilisateurs « au moyen d'une infrastructure de sécurité de pointe, de pratiques responsables en matière de données et d'outils de protection de la vie privée faciles à utiliser » qui mettent ses utilisateurs en contrôle. Elle a noté que des outils comme la vérification de la protection de la vie privée et la vérification de la sécurité envoient des rappels aux utilisateurs et des recommandations personnalisées en matière de protection de la vie privée et de sécurité, y compris des mesures qu'ils devraient prendre pour sécuriser immédiatement leur compte Google. Selon elle, ces deux fonctions de vérification permettent aux utilisateurs de personnaliser, étape par étape, les contrôles de sécurité et de confidentialité selon leurs préférences personnelles.

M^me^ Patell a également mentionné le programme de protection avancé de Google, qui est accessible à tous mais qui est conçu pour les personnes et les organisations — comme les élus, les campagnes politiques, les défenseurs des droits de la personne et les journalistes — qui sont plus à risque d'être la cible d'attaques en ligne.

M^me^ Patell a expliqué que le traitement des données des utilisateurs de Google inclut la protection des données de tiers et que Google a comme politique de ne jamais vendre les renseignements personnels de ses utilisateurs à qui que ce soit.

En ce qui concerne la protection des mineurs, M^me^ Patell a noté que YouTube est conçue pour des utilisateurs de 13 ans et plus et que la fourniture d'une date de naissance est

requise pour ouvrir un compte. Elle a expliqué que si un utilisateur indique qu'il n'a pas l'âge requis, sa tentative est bloquée et il ne peut recommencer. Il est alors redirigé vers le processus de contrôle parental de YouTube.

Lutte contre les menaces externes

Selon M^me^ Patell, Google investit considérablement dans des équipes et des opérations mondiales pour prévenir les abus sur ses plateformes, comme le groupe d'analyse des menaces, dont Shane Huntley est le directeur principal. Celui-ci a expliqué que l'équipe mondiale d'analystes et d'experts en sécurité de Google travaille en étroite collaboration avec des équipes de produits pour analyser et contrer les menaces dirigées contre Google et ses utilisateurs, y compris les menaces provenant d'acteurs étatiques, de cybercriminels professionnels et d'opérations de collecte d'information.

M. Huntley a noté que chaque jour, le groupe d'analyse des menaces surveille plus de 270 groupes d'attaquants ciblés ou émanant d'un gouvernement provenant de plus de 50 pays. Il a également noté que Google publie un bulletin trimestriel sur les mesures prises contre les comptes qui semblent liés à des campagnes d'influence coordonnées. Il a donné l'exemple du troisième trimestre de 2023, dont le bulletin mentionne des campagnes d'influence bloquées par Google provenant de la Russie, de l'Iran, de la Chine et du Mexique.

M. Huntley a expliqué que le groupe qu'il dirige se concentre particulièrement sur la perturbation des opérations d'influence coordonnées sur YouTube. Il a mentionné que depuis janvier 2023, Google a supprimé plus de 2 400 chaînes YouTube liées à la Russie et plus de 60 000 chaînes liées à la Chine. Selon M. Huntley, ces mesures s'ajoutent aux lignes directrices communautaires, qui sont appliquées par YouTube de façon continue et qui ont entraîné le retrait de plus de huit millions de vidéos dans le monde au troisième trimestre de 2023.

M. Huntley a affirmé qu'à mesure que Google découvre et perturbe des opérations, elle prend des mesures pour protéger ses utilisateurs, diffuser l'information publiquement et partager ses conclusions avec des partenaires de l'industrie et du gouvernement « pour soutenir l'ensemble de l'écosystème ». Google émet également des avertissements à ses utilisateurs lorsqu'ils semblent avoir été ciblés par une attaque soutenue par un gouvernement.

CHAPITRE 2 : PLATEFORMES DE MÉDIAS SOCIAUX ET ACTEURS ÉTRANGERS

Utilisation des plateformes de médias sociaux par des entités étrangères

Cherie Henderson, directrice adjointe, Exigences, pour le Service canadien du renseignement de sécurité (SCRS), a indiqué que des acteurs étatiques étrangers mènent des activités d'ingérence en utilisant tous les moyens à leur disposition, y compris les plateformes de médias sociaux. Par exemple, la Russie et la Chine utilisent les médias sociaux et leurs algorithmes subjectifs pour amplifier les chambres d'écho et manipuler le contenu affiché auprès du public afin de propager de la désinformation.

M^me^ Henderson a expliqué que les auteurs de menace s'intéressent aux plateformes de médias sociaux pour les données qu'elles génèrent et recueillent, y compris des données personnelles comme les albums photos, les messages et les listes de contacts. Ces données, lorsqu'elles sont réunies en volumes importants, permettent de cerner des tendances et d'en apprendre plus sur diverses populations, sur l'opinion publique et sur des réseaux individuels[35]. Il faut donc que la population canadienne sache de quels facteurs elle doit tenir compte sur le plan de la vie privée lorsqu'elle décide de transmettre ses renseignements personnels en ligne, en particulier à des entreprises qui se trouvent en dehors du Canada et de pays alliés.

M^me^ Henderson a rajouté que les États autoritaires comme la Chine se servent de mégadonnées pour mener des activités d'ingérence étrangère. Ils ne respectent pas les obligations légales ou éthiques en place dans d'autres pays, comme le Canada. Selon elle, les nouvelles technologies ne feront qu'aider la Chine dans ses activités malveillantes. M^me^ Henderson a noté que la loi chinoise de 2017 sur le renseignement national qui oblige les particuliers, les organisations et les institutions, y compris les plateformes de médias sociaux qui offrent leurs services en Chine, à fournir des informations de masse au gouvernement, aide les services de sécurité et de renseignement chinois à mener leurs activités.

M. Khoury a confirmé que dans son évaluation non classifiée des cybermenaces nationales de 2023-2024, le CCC a évalué que les États étrangers utilisent les médias

35 ETHI, *Témoignages*, Cherie Henderson (directrice adjointe, Exigences, Service canadien du renseignement de la sécurité).

sociaux pour cibler des Canadiens[36]. M. Khoury a rajouté qu'il est fort probable que certains pays utilisent des applications de messagerie et de médias sociaux étrangers populaires auprès de la diaspora au Canada et à travers le monde pour surveiller les communications. Il a noté que certains pays peuvent profiter de conditions d'utilisation permissives et de leurs propres pouvoirs législatifs pour forcer le partage de données.

Mme Henderson a souligné que les États hostiles peuvent récolter les renseignements personnels publiés ouvertement sur les médiaux sociaux par des individus, en précisant que ce n'est pas seulement la Chine qui mène de telles activités. Selon elle, il ne faut pas perdre de vue toutes les activités hostiles menées contre les Canadiens en mettant l'accent sur un seul acteur. Elle a mentionné que les États hostiles, comme la Russie, l'Iran et la Corée du Nord, peuvent traiter des données volumineuses et faire de la surveillance s'ils le souhaitent.

Mme Henderson a noté qu'en 2023, le ministre de la Sécurité publique a émis une directive ministérielle qui prévoit que si le SCRS apprend que des agents étrangers hostiles mènent des activités nuisibles contre des politiciens, il doit examiner l'information, déterminer la gravité de la menace qu'elle représente puis communiquer avec les différents acteurs politiques concernés pour leur fournir des conseils.

Mme Henderson a expliqué que l'ingérence étrangère se produit tous les jours, pas seulement lors d'une élection. Le SCRS surveille ce qui se passe au quotidien, pour déceler une quelconque forme d'ingérence étrangère par un acteur étatique hostile. Il ne surveille pas, cependant, les médias sociaux. La menace d'ingérence étrangère sur les médias sociaux doit être réelle avant que le SCRS intervienne. Trouver le point d'origine d'une attaque prend souvent beaucoup de temps au SCRS, selon Mme Henderson. Elle a par ailleurs rappelé l'importance de préserver la liberté d'expression et a rappelé qu'il faut toujours considérer, lorsqu'une menace provient de l'étranger, l'incidence de cette menace sur la souveraineté du Canada et sur la sécurité nationale.

Peter Madou, directeur général, Évaluation des renseignements, pour le SCRS, a dit que l'organisation fournit des conseils sur l'ingérence étrangère au gouvernement de manière générale. Il a rappelé que le SCRS enquête sur les auteurs de menace; pas sur les plateformes de médias sociaux. Il a souligné que la détection de contre-discours sur les plateformes de médias sociaux est un phénomène courant, mais il est plus complexe de lier ce type de discours précisément à un auteur de menace hostile. Il est donc difficile d'identifier la fréquence à laquelle une telle menace a lieu.

36 Centre canadien pour la cybersécurité, *Évaluation non classifiée des cybermenaces nationales de 2023-2024*.

M^me^ Henderson a aussi indiqué que, compte tenu de la quantité de renseignements personnels partagés sur les médias sociaux, les acteurs étrangers hostiles peuvent se faire une très bonne idée de qui vous êtes et de la manière dont ils peuvent vous influencer. En surveillant les réseaux sociaux, les acteurs étrangers peuvent aussi observer certaines tendances dans des régions données, comme pour qui les gens votent ou de quoi ils s'inquiètent. Néanmoins, elle a souligné qu'en cessant de partager des renseignements personnels ou en faisant attention à ce qui est partagé, il est possible de protéger sa présence sur les médias sociaux.

M. Larkin a souligné que la GRC accorde la plus haute priorité à l'exploitation des données personnelles des citoyens canadiens par des protagonistes à l'étranger, ainsi qu'à la perpétration de crimes dans l'espace numérique. Il a expliqué que l'ingérence étrangère touche plusieurs aspects de notre vie, allant des fondements de la démocratie canadienne et de sa prospérité économique aux valeurs et droits fondamentaux qui nous définissent en tant que société.

M. Larkin a expliqué que des acteurs étrangers cherchent à atteindre leurs objectifs de multiples façons, dont le harcèlement et l'intimidation de personnes et de communautés partout au Canada. Ces acteurs étrangers ont le soutien d'un État. Les gouvernements étrangers utilisent les données recueillies sur les plateformes de médias sociaux pour établir le profil de certaines personnes et mener des campagnes de mésinformation et de désinformation au Canada ou identifier et réprimer des dissidents politiques qui cherchent refuge au Canada.

M. Larkin a indiqué que la GRC a le mandat d'enquêter sur les crimes graves, la criminalité organisée et la sécurité nationale, ce qui inclut les cas d'ingérence étrangère en ligne. Son Centre national de coordination contre la cybercriminalité collabore avec tous les organismes d'application de la loi et d'autres partenaires comme le Centre antifraude du Canada pour réduire la menace posée par la cybercriminalité[37].

M. Larkin a noté qu'en 2022, 35 % des (plus de) 30 000 signalements de fraudes et d'escroqueries liées à la cybercriminalité étaient liés aux plateformes de médias sociaux. La GRC travaille en étroite collaboration avec les services de police dans tout le pays, qui sont souvent les premières entités d'application de la loi à être informées des activités cybercriminelles soutenues par un État qui ciblent des Canadiens.

Selon M. Larkin, il est essentiel que les Canadiens comprennent que tout ce qu'ils transmettent en ligne est recueilli et stocké sur des serveurs, souvent situés à l'extérieur

37 Le Centre antifraude du Canada est géré conjointement par la Gendarmerie royale du Canada, le Bureau de la concurrence du Canada et la Police provinciale de l'Ontario.

du Canada, où les droits relatifs à la protection des renseignements personnels pourraient ne pas avoir la même signification qu'ici. Il a rappelé que

> Dans certains pays, les lois sur la sécurité nationale obligent les entreprises de médias sociaux à transmettre les données personnelles recueillies auprès d'utilisateurs étrangers aux gouvernements locaux. Ces données sont ensuite utilisées pour harceler, contraindre ou menacer des voix dissidentes, des dirigeants politiques et nos communautés diversifiées à l'étranger, ou pour faciliter la cybercriminalité.

Mme Gauvin a également souligné que la Chine et d'autres acteurs étrangers utilisent divers moyens pour cibler les dissidents et mener des activités d'ingérence étrangère, dont les médias sociaux.

En ce qui concerne l'hébergement des données de citoyens canadiens sur des serveurs étrangers, M. Larkin a indiqué que le niveau de sécurité de ces renseignements dépend de plusieurs facteurs, dont le niveau de cryptage. Cependant, aucun système ne peut garantir la sécurité totale des données, selon lui[38].

M. Larkin a indiqué que l'amplification dans les médias sociaux des objets d'enquêtes criminelles pose un autre défi. Dans la majorité des enquêtes menées par la GRC, du délit mineur au délit violent ou d'exploitation, il y a une forme d'entité numérique liée à l'enquête. Cela est loin d'une enquête menée dans un quartier ou une cour d'école. La GRC voit maintenant des cas où des acteurs étrangers utilisent et amplifient le contenu qui se trouve sur les médias sociaux pour cibler des citoyens canadiens ou des citoyens étrangers qui vivent dans notre pays, ce qui représente un défi considérable pour la GRC.

M. Larkin a noté que la GRC utilise elle-même les médias sociaux dans le cadre d'enquêtes, pour obtenir des renseignements venant de sources ouvertes. Elle utilise aussi des logiciels pour affiner les recherches requises par son travail courant ou dans le cadre d'enquêtes criminelles.

Mme Gauvin a reconnu qu'il y a eu, au cours des dernières années, une augmentation de l'ingérence étrangère et que les médias sociaux servent de véhicules aux entités étrangères pour propulser leurs activités. Elle a expliqué que cette ingérence est beaucoup plus difficile à détecter.

Mme Gauvin a toutefois réitéré que la GRC n'enquête pas sur les médias sociaux et ne cherche pas à savoir s'il y a mésinformation, désinformation ou tentative d'influence sur la plateforme. Le programme de sécurité nationale de la GRC enquête sur les activités

38 ETHI, *Témoignages*, Bryan Larkin (sous-commissaire, Services de police spécialisés, Gendarmerie Royale du Canada).

criminelles. Si les activités criminelles ont trait à l'ingérence étrangère, une enquête aura lieu.

Sur la capacité pour la GRC d'intervenir dans un contexte ou du contenu ou une application a été créée sur un autre territoire, M[me] Gauvin a indiqué que « si on menace un Canadien, une Canadienne ou la sécurité publique canadienne ou la sécurité nationale du Canada, cela donne l'autorité d'agir à la GRC ».

Extraction de données par des acteurs étrangers

Concernant la possibilité que des gouvernements étrangers fassent l'extraction et recueillent les données de Canadiens à des fins malveillantes, M. Dufresne a noté que ses homologues des provinces et lui ont récemment publié une déclaration sur l'extraction des données[39]. Ils ont entre autres demandé aux organisations de médias sociaux de prendre des mesures pour protéger les renseignements et informer leurs utilisateurs, en plus de décrire des mesures que peuvent prendre les individus pour protéger leurs données.

M. Dufresne a noté que la déclaration fait état des risques liés à l'extraction des données, ce qui inclut « les cyberattaques, l'usurpation d'identité, le contrôle, le profilage, la surveillance des individus, l'utilisation non autorisée à des fins politiques ou de collecte de renseignements et le marketing direct non sollicité ou pourriels ». Les commissaires ont aussi établi des techniques d'atténuation des risques que les entreprises de médias sociaux peuvent et doivent mettre en œuvre pour protéger l'information contre les acteurs malveillants qui pourraient l'extraire.

À cet égard, M. Gruzd a argué qu'il y a lieu de s'inquiéter du risque que TikTok et d'autres plateformes soient exploitées par des acteurs malveillants à des fins de propagande et de radicalisation. Les préoccupations exprimées par M. Gruzd ne se limitent pas à une seule plateforme; elles représentent plutôt des défis plus vastes pour l'intégrité et la sécurité de notre environnement d'information. Il a affirmé que les acteurs étatiques utiliseront tous les outils disponibles et toutes les plateformes de médias sociaux populaires au Canada[40]. Selon lui, en mettant l'accent sur une seule plateforme, cela peut donner l'impression que les autres plateformes sont sûres alors

39 CPVP, *Déclaration commune sur l'extraction de données et la protection des renseignements personnels*, 24 août 2023.

40 ETHI, *Témoignages*, Gruzd.

qu'elles se livrent à des pratiques similaires de collecte et d'utilisation abusive de données, ou des acteurs étatiques peuvent les utiliser.

M. Gruzd a reconnu que les outils des médias sociaux ont été militarisés par divers acteurs étatiques et d'autres groupes d'intérêts, qui tentent d'orienter l'opinion publique. Il a rajouté que ces efforts sont parfois menés par de vastes réseaux de robots automatisés. Par exemple, des recherches menées avec des données fournies par Twitter ont permis de constater que des robots automatisés publiaient des contenus innocents sur des sites comme X, pour ensuite basculer vers des récits différents. Les acteurs étatiques exploitent les divisions et la polarisation, ouvertement ou secrètement.

M. Gruzd a rajouté qu'il y a différents types d'ingérence étrangère. Il y a des plateformes où un acteur étatique a un accès direct, comme VKontakte, qui fonctionnait à partir de la Russie et a dû être interdite en Ukraine puisqu'on a établi qu'elle était en fait gérée par l'État. Parfois, l'accès se fait par l'entremise d'applications des développeurs, ce qui représente une autre forme d'ingérence.

M. Gruzd a précisé que les acteurs étatiques visent souvent les groupes sympathisants, qui vont, par exemple, répéter le contenu qu'ils fournissent comme du contenu pro-Kremlin. Ils s'intéressent aux opinions politiques partisanes qui peuvent cadrer avec leurs objectifs. Le but est que du contenu touche quelqu'un qui détient du pouvoir, par exemple un influenceur sur TikTok, un politicien qui cherche à être élu, qui propage le discours souhaité.

Il est préoccupant que de nombreux Canadiens se tournent vers les médias sociaux pour se renseigner sur des conflits comme la guerre en Ukraine ou la guerre en Palestine, alors que les réactions sur ces plateformes sont motivées par le contenu produit par l'influenceur qui fournit l'information, comme l'a souligné M. Gruzd. Les sources d'information fiables ne peuvent tout simplement pas faire compétition avec le contenu produit par des influenceurs, selon lui. Bien que la liberté d'expression soit importante, il a rappelé qu'il est aussi important de veiller à ce que la population canadienne qui utilise ces plateformes ait accès à des renseignements crédibles.

TikTok : Collecte de données excessive et partage potentiel avec des acteurs étrangers

Enquêtes sur TikTok et amendes par des autorités dans d'autres pays

En février 2019, la Federal Trade Commission des États-Unis (FTC) a annoncé que l'application Musical.ly (aujourd'hui TikTok) acceptait de payer $US 5,7 millions pour

régler une plainte alléguant que l'entreprise avait recueilli illégalement les renseignements personnels d'enfants, enfreignant ainsi la *Children's Online Privacy Protection Act*, qui requiert le consentement parental pour recueillir les données d'enfants de moins de 13 ans. TikTok a plaidé qu'un règlement ne signifie pas qu'il y a eu admission d'une violation ou d'un manquement et que, depuis 2019, des paramètres par défaut, des mesures de protection des outils ont été mis en place par TikTok pour protéger les mineurs, y compris les adolescents canadiens[41].

En septembre 2023, le Commissariat à la protection des données irlandais (le DPC ou Commissariat irlandais) a imposé une amende de €345 millions à TikTok pour avoir contrevenu à divers articles du Règlement général sur la protection des données de l'union européenne (RGPD) concernant le traitement de données personnelles d'enfants[42]. M. Lieber a noté le désaccord de TikTok avec la décision du DPC et l'amende imposée et qu'elle a fait appel de cette décision. Il a expliqué que cette amende concerne les réglages des comptes de jeunes utilisateurs créés avant 2020. Il a ajouté qu'au moment où l'enquête a été lancée, TikTok avait déjà prévu des protocoles pour rendre les comptes d'adolescents privés par défaut et imposer d'autres réglages pour les mineurs.

En avril 2023, le Commissariat à l'information du Royaume-Uni a imposé une amende de £12,7 millions à TikTok pour non-respect de certaines dispositions du *Data Protection Act 2018* entre autres pour avoir fourni des services à des enfants de moins de 13 ans en traitant leurs renseignements personnels sans le consentement ni l'autorisation de leurs parents ou tuteurs et pour ne pas avoir fourni des informations adéquates et faciles à comprendre aux utilisateurs de TikTok sur la façon dont leurs données sont recueillies, utilisées et partagées. TikTok a noté son désaccord avec la décision du Commissariat à l'information du Royaume-Uni. Comme pour l'amende imposée par le Commissariat irlandais, la décision vise une période précédant 2020 et TikTok fait appel de la décision[43].

Enquête conjointe sur TikTok par des autorités canadiennes

M. Dufresne a rappelé qu'il a déposé une plainte contre TikTok en février 2023, en sa qualité de commissaire. L'enquête conjointe est menée avec ses homologues provinciaux du Québec, de l'Alberta et de la Colombie-Britannique. M. Dufresne a indiqué pendant sa comparution en octobre 2023 qu'ils espéraient terminer leur enquête d'ici la fin du mois de mars 2024. Aucun rapport d'enquête n'a été publié pour l'instant. Le

41 TikTok, *Réponse écrite soumise au Comité ETHI*, p. 8 [HYPERLIEN NON DISPONIBLE].

42 Irish Data Protection Commission, *Irish Data Protection Commission announces €345 million fine of TikTok*, 15 septembre 2023 [DISPONIBLE EN ANGLAIS SEULEMENT].

43 TikTok, *Réponse écrite soumise au Comité ETHI*, p. 8 [HYPERLIEN NON DISPONIBLE].

commissaire a précisé que l'enquête conjointe cible les méthodes de gestion des données de TikTok, dont notamment le consentement à une utilisation à des fins appropriées, particulièrement dans le cas des enfants et des jeunes, qui en sont les principaux utilisateurs.

M. Dufresne a expliqué que les commissaires examinent aussi la question de savoir si une personne raisonnable estimerait que les fins pour lesquelles TikTok traite les renseignements personnels, en particulier les renseignements des enfants, sont appropriées dans les circonstances, c'est-à-dire qu'il s'agit de « fins acceptables » selon le terme utilisé dans la LPRPDE. L'enquête permettra aussi de déterminer si TikTok respecte ses obligations sur le plan de la transparence, en particulier lorsqu'elle recueille les renseignements personnels de ses utilisateurs[44].

Le commissaire ne pouvait entrer dans les détails de l'enquête, qui est en cours. M. Dufresne a néanmoins précisé que l'enquête a été lancée à la suite de recours collectifs aux États-Unis et au Canada, ainsi que de nombreux reportages dans les médias concernant la collecte, l'utilisation et la communication de renseignements personnels par TikTok. Il a aussi abordé les principes de protection de la vie privée qui sous-tendent l'approche du CPVP à l'égard du monde numérique et du point de vue du droit à la vie privée des enfants.

Michael Maguire, directeur pour la LPRPDE au sein de la Direction de la conformité du CPVP, a confirmé que l'enquête porte sur ByteDance en tant que propriétaire de TikTok. M. Dufresne a aussi rappelé qu'en vertu de la LPRPDE, une organisation est responsable des renseignements personnels « qu'elle a sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement ». Ce faisant, l'organisation « doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie ». Le projet de loi C-27, qui sera abordé au chapitre 3, contient une obligation semblable, à l'article 11 de la Loi sur la protection de la vie privée des consommateurs proposée[45].

M. Dufresne a noté que dans le cas du partage de données, il faut vérifier si celui-ci est approprié, s'il respecte les limites juridiques et s'il donne lieu à des préoccupations en matière de sécurité. Il a expliqué que le CPVP dispose de nombreux outils pour évaluer

44 ETHI, *Témoignages*, Philippe Dufresne (commissaire à la protection de la vie privée, Commissariat à la protection de la vie privée du Canada).

45 Projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois (Projet de loi C-27).

les pratiques d'une organisation, par exemple, les visites au site et les demandes de documentation. Le CPVP a aussi un laboratoire où on examine les outils techniques qui lui permettront de mener des enquêtes dans le domaine numérique et d'obtenir les renseignements recherchés. M. Maguire a rappelé que le CPVP peut aussi mener des auditions sous serment et peut se rendre sur les lieux pour exiger la production de documents.

Selon la réponse écrite de TikTok, la confidentialité et la sécurité de ses utilisateurs, en particulier des jeunes, sont toujours une priorité absolue pour TikTok et elle coopère avec les autorités canadiennes chargées de la protection des données dans le cadre de cette enquête[46].

Examen de sécurité nationale de TikTok

Le 6 septembre 2023, le gouvernement du Canada a émis un ordre d'examen de la sécurité nationale de TikTok[47]. Le bureau du ministre de l'Innovation, des Sciences et de l'Industrie a déclaré que l'examen n'a pas été divulgué - et que l'ordonnance du cabinet n'est pas accessible - parce que les informations sont protégées et confidentielles en vertu de la *Loi sur Investissement Canada*[48]. Le bureau du ministre a également indiqué que TikTok ferait l'objet d'un « examen approfondi » en vertu de la *Loi*, par le biais d'une nouvelle politique sur les investissements étrangers dans le secteur des médias numériques interactifs, qui a été publiée par le gouvernement au début du mois de mars 2024[49]. Cet énoncé de politique indique que « certains acteurs hostiles parrainés ou influencés par un État pourraient chercher à tirer parti des investissements étrangers dans le secteur des médias numériques interactifs afin de propager la désinformation ou de manipuler l'information d'une manière portant atteinte à la sécurité nationale du Canada[50] ».

Dans une lettre qu'a fait parvenir Innovation, Sciences et Développement économique du Canada au Comité le 12 avril 2024, il est indiqué qu'un examen de sécurité nationale peut durer plus de 200 jours. Il est également indiqué que pour les examens qui font

46 TikTok, *Réponse écrite soumise au Comité ETHI*, p. 8 [HYPERLIEN NON DISPONIBLE].

47 Anja Karadeglija, « Federal government reveals it ordered national security review of TikTok », *CBC News*, 14 mars 2024 [DISPONIBLE EN ANGLAIS SEULEMENT].

48 Voir la partie IV.1 de la *Loi sur Investissement Canada*, « Investissements préjudiciables à la sécurité nationale » (art. 25.1 à 25.6).

49 Gouvernement du Canada, *Énoncé de politique sur l'examen des investissements étrangers dans le secteur des médias numériques interactifs*, 1 mars 2024.

50 *Ibid*.

l'objet d'une ordonnance finale par le gouverneur en conseil, un avis de la décision est publié dans une liste mensuelle mise à la disposition du public et des médias. Au moment de l'adoption du présent rapport, aucun avis public n'avait encore été publié à l'égard de l'examen de sécurité national de TikTok.

Interdiction d'utiliser TikTok à l'échelle internationale

Il est totalement interdit d'utiliser TikTok dans certains pays, comme l'Inde, l'Indonésie et le Pakistan[51]. Dans d'autres pays, l'interdiction est limitée aux appareils du gouvernement : au Canada, aux États-Unis, dans les pays membres de l'Union européenne, au Royaume-Uni – en plus de son parlement – en Australie et au parlement de Nouvelle-Zélande, par exemple[52].

Le 23 février 2023, la Commission européenne – la branche exécutive de l'Union européenne – a suspendu l'utilisation de TikTok sur les appareils de son personnel afin de se protéger « contre les cybermenaces et les agissements qui pourraient être ensuite exploités à des fins de cyberattaques ciblant l'institution[53] ». La Commission a précisé qu'elle fera également un suivi constant de l'évolution de la sécurité d'autres plateformes de médias sociaux[54].

Le 27 février 2023, le gouvernement canadien a annoncé qu'il interdisait, à compter du 28 février, l'utilisation de TikTok sur les appareils mobiles fournis par le gouvernement[55]. Il a fondé cette décision sur un examen de TikTok effectué par la dirigeante principale de l'information du Canada, qui a déterminé que cette application présentait un niveau de risque inacceptable pour la vie privée et la sécurité[56].

---

51 Sénat français, *Rapport fait au nom de la commission d'enquête (1) sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence*, 4 juillet 2023, p. 9.

52 Royaume-Uni, Bureau du Cabinet, *TikTok banned on UK government devices as part of wider app review*, communiqué, 16 mars 2023 [DISPONIBLE EN ANGLAIS SEULEMENT]; Australie, Porfolio du Procureur général, *TikTok ban on Government Services*, communiqué, 4 avril 2023 [DISPONIBLE EN ANGLAIS SEULEMENT]; Sapna Maheshwari et Amanda Holpuch, *Why Countries Are Trying to Ban TikTok*, The New York Times, 16 août 2023 [DISPONIBLE EN ANGLAIS SEULEMENT].

53 Commission européenne, *La Commission renforce sa cybersécurité et suspend l'utilisation de TikTok sur les appareils de son personnel*, Communiqué de presse, 23 février 2023.

54 *Ibid.*

55 Gouvernement du Canada, *Déclaration de la ministre Fortier annonçant l'interdiction d'utiliser l'application TikTok sur les appareils mobiles du gouvernement*, 27 février 2023.

56 *Ibid.*

Le 27 février 2023, la Maison blanche a elle aussi donné 30 jours aux agences fédérales pour enlever l'application des appareils et des systèmes informatiques du gouvernement des États-Unis[57]. TikTok était déjà interdite depuis trois ans sur les appareils du gouvernement des États-Unis utilisés par les militaires[58].

M. Lieber a par ailleurs confirmé que les négociations se poursuivent entre TikTok et le Comité d'investissements étrangers aux États-Unis concernant un accord visant à résoudre les inquiétudes liées à la sécurité nationale que pose la plateforme aux États-Unis. Il a mentionné qu'entretemps, TikTok a mis en place son Projet Texas, qui tente de répondre aux préoccupations exprimées par le gouvernement des États-Unis, notamment sur l'accès aux données des utilisateurs par le gouvernement chinois et la façon dont la plateforme pourrait être manipulée ou utilisée[59].

En avril 2024, la *Protecting Americans from Foreign Adversary Controlled Applications Act* a été adoptée aux États-Unis par le passage d'un projet de loi concernant des crédits supplémentaires pour l'exercice 2024 destinés à plusieurs agences fédérales américaines afin qu'elles puissent aider l'Ukraine, Israël et les alliés des États-Unis dans la région indopacifique. Cette loi exige que dans les 270 jours de son adoption, TikTok soit vendue à un propriétaire qui n'est pas originaire de la Chine, faute de quoi l'application sera bannie aux États-Unis. L'échéance pour cette vente est le 19 janvier 2025.

Interdiction d'utiliser TikTok sur les appareils du gouvernement canadien

Catherine Luelo, qui a comparu alors qu'elle était toujours sous-ministre et dirigeante principale de l'information du Canada, a dit n'avoir eu aucune pression politique pour interdire l'application[60]. Elle a noté que le gouvernement a récemment interdit WeChat et Kaspersky Lab, en plus de TikTok.

M^{me} Luelo a rappelé que son poste lui confie la responsabilité de veiller à ce que le gouvernement ait des règles et des lignes directrices explicites concernant l'utilisation des appareils du gouvernement. C'est dans cette optique qu'elle a pris la décision

57 David Shepardson, *White House sets deadline for purging TikTok from federal devices*, Reuters, 28 février 2023 [DISPONIBLE EN ANGLAIS SEULEMENT].

58 Stephen Castle, « U.K. Bans TikTok on Government Devices », *The New York Times*, 16 mars 2023 [DISPONIBLE EN ANGLAIS SEULEMENT].

59 TikTok, U.S. Data Security, *About Project Texas* [DISPONIBLE EN ANGLAIS SEULEMENT].

60 ETHI, *Témoignages*, Catherine Luelo (ancienne sous-ministre et dirigeante principale de l'information du Canada).

concernant TikTok. Elle a expliqué que lorsque des décisions sont prises sur ce qui constitue une utilisation acceptable des appareils du gouvernement, on tient compte d'une série d'éléments, comme la protection de la vie privée, l'usage acceptable dans un environnement professionnel et le coût.

Selon M^me^ Luelo, il faut continuer à resserrer l'environnement entourant l'utilisation des appareils du gouvernement, qui serait assez ouvert à l'heure actuelle. Environ 90 % des appareils du gouvernement autorisent le téléchargement de tout ce que l'utilisateur souhaite et permettent un usage professionnel et un usage personnel sur le même appareil. Elle a conseillé au gouvernement que ses appareils ne soient utilisés que pour les affaires du gouvernement.

M^me^ Luelo a toutefois convenu que dans certains cas, il peut y avoir une raison acceptable d'utiliser une plateforme de médias sociaux à des fins professionnelles, par exemple pour transmettre des renseignements à des catégories de personnes qui utilisent ces plateformes pour obtenir de l'information. Elle a donné l'exemple d'utilisation de plateformes de médias sociaux pour atteindre des groupes démographiques au sujet du vaccin contre la COVID pendant la pandémie. Pour M^me^ Luelo, un risque est acceptable « lorsque la valeur de l'action l'emporte sur le risque d'un inconvénient éventuel ».

M. Khoury a expliqué que pour donner des avis et des conseils sur ce qui est téléchargé sur des appareils gouvernementaux, le CCC étudie un certain nombre de choses, comme les contrôles de sécurité et l'identité du créateur de l'application. Il a noté que les menaces étrangères sont éclairées par diverses sources, dont certaines sont publiques et d'autres sont classifiées. Il a rajouté que les préoccupations du CCC sont les suivantes : Qui a accès aux données? Où les données sont-elles conservées? À quel point est-il facile pour le pays d'accueil d'obtenir l'accès aux données? Dans le cas de TikTok, si les données sont hébergées en Chine, ce serait une préoccupation, compte tenu des lois chinoises qui permettent l'accès aux données des utilisateurs.

En ce qui concerne la décision d'interdire TikTok sur les appareils gouvernementaux, M. Khoury a précisé que le CCC faisait partie de la table ronde avec le Secrétariat du Conseil du Trésor, mais que la décision d'interdire l'application appartient à la dirigeante principale de l'information[61].

Dans le même ordre d'idées, M. Dufresne a rappelé que le gouvernement du Canada s'est basé sur son propre examen de la situation pour prendre cette décision, à la lumière des avis formulés par la dirigeante principale de l'information et les différents spécialistes

61 ETHI, *Témoignages*, Sami Khoury (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications).

de l question. Il a confirmé ne pas avoir participé aux évaluations menées par le gouvernement qui ont mené à cette interdiction. Il a soutenu que les gouvernements ont une responsabilité en matière de sécurité nationale et en matière de sécurité de l'information des fonctionnaires.

Pour sa part, M. Gruzd a souligné que l'interdiction d'une seule application peut se révéler inefficace. Une telle interdiction pourrait selon lui miner la confiance dans le gouvernement, légitimer la censure et créer un environnement propice à la mésinformation. Selon lui, à défaut d'une preuve concrète d'ingérence étrangère, interdire l'utilisation d'une plateforme mine nos processus démocratiques, en créant une perception de politisation du sujet.

Dans la même veine, M. Malone, a trouvé que la déclaration sur les préoccupations relatives à la protection de la vie privée et à la sécurité qui avait accompagné l'interdiction d'utiliser TikTok sur les appareils du gouvernement a laissé plusieurs questions sans réponse. Il a souligné que TikTok n'est pas la seule application qui conserve les données de ses utilisateurs dans les instances étrangères et les divulgue potentiellement à des régimes étrangers.

M. Malone a affirmé que le Secrétariat du Conseil du Trésor lui a confirmé qu'aucune des applications suivantes n'est interdite de téléchargement et d'utilisation sur les appareils émis par le gouvernement : VKontakte affiliée à la Russie, Mail.ru, Facebook, Instagram, Tinder, Snapchat, Bumble, Grindr, Truth Social, Gab et Discord. M. Malone a rappelé que Discord a été impliquée dans les fuites de documents du Pentagone de 2022-2023 et ne dispose pas de mesures de protection de la sécurité des enfants, selon M^{me} Laidlaw.

M. Malone a recommandé que le gouvernement interdise toutes les applications de médias sociaux sur les appareils fournis par le gouvernement, à moins qu'il n'y ait une justification commerciale solide de ne pas les interdire, dans le but d'offrir une meilleure protection de la vie privée et de la sécurité. Il a également recommandé que le gouvernement cesse d'acheter de la publicité sur tous les services de médias sociaux.

M. Malone estime aussi qu'il est contraire à l'éthique de faire de la publicité auprès des entreprises de médias sociaux au regard des préoccupations soulevées au sujet de la collecte de données et de l'ingérence étrangère illicite. Il a noté qu'en 2022, par exemple, le gouvernement canadien a dépensé 141 millions de dollars en publicité, incluant près de 2 millions de dollars de publicité sur TikTok.

En ce qui concerne le type de renseignements communiqués sur les appareils fournis par le gouvernement, M. Malone a fait valoir que même si l'utilisation individuelle de certaines applications est inoffensive, les renseignements recueillis pourraient servir de

façon regroupée. Il a expliqué que certains éléments, comme les données de localisation, peuvent révéler des renseignements sensibles comme l'emplacement des politiciens ou des membres des Forces armées canadiennes.

Considérant les préoccupations soulevées par les témoins à l'égard de la manière dont les appareils gouvernementaux sont utilisés, le Comité fait la recommandation suivante :

Recommandation 1

Que le gouvernement du Canada réévalue ses normes numériques concernant le téléchargement et l'utilisation de toutes les applications de médias sociaux sur les appareils fournis par le gouvernement afin de s'assurer qu'elles sont principalement utilisées pour les affaires du gouvernement.

Position de TikTok concernant l'interdiction d'utiliser son application

En ce qui concerne son interdiction sur les appareils gouvernementaux au Canada, M. de Eyre a mentionné que TikTok a communiqué avec le Secrétariat du Conseil du Trésor et le Bureau de la dirigeante principale de l'information, pour tenter de mieux comprendre les critères qui ont été utilisés pour interdire seulement TikTok, alors que d'autres plateformes fonctionnent de la même façon qu'elle. Il a reconnu qu'il n'est probablement pas nécessaire d'avoir des applications de médias sociaux, de divertissement ou de jeu sur l'appareil d'un employé du gouvernement, mais que ces règles devraient s'appliquer à toutes les plateformes.

Concernant le fait que plusieurs pays dont l'Inde, l'Indonésie et le Pakistan ont interdit TikTok dans leur pays et que d'autres pays, comme l'Australie, la Nouvelle-Zélande et l'ensemble de l'Union européenne, en ont restreint l'utilisation sur les appareils du gouvernement, TikTok a plaidé dans sa réponse écrite que ces interdictions sont mal informées et non méritées[62].

Ces interdictions ne reposent sur aucune conclusion déterminante concernant une violation de la confidentialité ou un problème de confidentialité, selon les représentants de TikTok. À leur avis, le fait d'interdire une seule entreprise ne représente pas la bonne approche pour renforcer la protection et la sécurité des utilisateurs. Par exemple, la réponse écrite de TikTok fait valoir que l'interdiction d'utiliser la plateforme sur les appareils gouvernementaux au Canada risque d'avoir un impact négatif sur la population canadienne, car elle empêche d'utiliser des canaux que le gouvernement, les institutions

62 TikTok, *Réponse écrite soumise au Comité ETHI*, p. 7 [HYPERLIEN NON DISPONIBLE].

publiques et d'autres voix faisant autorité utilisaient pour atteindre la population canadienne et elle paralyse le discours public[63].

Questions concernant le contrôle de l'entreprise TikTok

M. de Eyre a insisté sur le fait que le gouvernement chinois ne possède ni ne contrôle ByteDance, la société mère de TikTok, dont 60 % des parts sont détenues par des investisseurs institutionnels mondiaux, 20 % par ses fondateurs et 20 % par des employés. Il a noté que trois des cinq membres du conseil d'administration de ByteDance viennent des États-Unis. Il a reconnu que ByteDance a été créée en Chine, mais a insisté sur le fait qu'il s'agit d'une multinationale ayant des bureaux partout dans le monde.

M. de Eyre a rappelé que TikTok n'est pas disponible en Chine continentale et que l'entreprise n'est pas une société d'État, mais une entreprise privée. Il a également rappelé que ByteDance est aussi une entreprise privée, qui rend des comptes à son conseil d'administration. Il a reconnu que Douyin, un produit semblable à TikTok destiné au marché chinois, appartient aussi à ByteDance, tout en soulignant que Douyin est une application distincte. Il a aussi noté que les sièges sociaux de TikTok sont à Los Angeles et Singapour, que son avocat général est aux États-Unis et que le responsable mondial de la confiance et de la sécurité est à Dublin. M. de Eyre a rajouté que TikTok a des milliers d'employés dans le monde, dont 150 à son bureau canadien de Toronto.

M. de Eyre a confirmé qu'une entité opérationnelle chinoise s'occupe exclusivement du marché chinois tout en précisant que cette entité n'a rien à voir avec TikTok, n'a aucun contrôle sur elle, ses employés ne peuvent pas accéder aux données d'utilisateurs de TikTok et elle ne se situe pas au-dessus de TikTok dans l'organigramme.

En ce qui concerne le partage de données avec le Parti communiste chinois, M. Lieber a affirmé ce qui suit :

> Notre position est claire: nous ne transmettrons pas de données sur les utilisateurs au gouvernement chinois s'il en fait la demande. Il n'a fait aucune demande dans ce sens, et le gouvernement chinois n'a pas revendiqué ses droits à l'égard des données des utilisateurs de TikTok. L'application TikTok n'est pas autorisée en Chine. Comme nous l'avons indiqué précédemment, nous avons un bureau ainsi que des employés sur le territoire canadien. Nous avons des utilisateurs au Canada et nous sommes assujettis aux lois canadiennes. Nous publions également un rapport semestriel sur la transparence dans lequel nous indiquons le nombre de demandes de la part des

63 *Ibid*.

> gouvernements du monde. Si jamais nous recevions une demande du gouvernement chinois, nous l'indiquerions sans faute dans notre rapport sur la transparence.

M. Lieber a dit ignorer si le gouvernement chinois a la capacité technologique d'accéder aux données d'utilisateurs directement, sans l'entremise d'une demande. Il a toutefois argué qu'il serait irresponsable pour tout employé du secteur de la technologie d'offrir des garanties catégoriques sur les capacités éventuelles des gouvernements de mener leurs activités, y compris des activités de piratage.

M. Lieber a aussi indiqué que la politique de confidentialité de TikTok contient une disposition traitant de la communication d'information au sein de son groupe d'entreprises, notant qu'il y a des fonctions qui sont exécutées par d'autres entités de la famille d'entreprises à laquelle TikTok appartient, par exemple pour résoudre un problème avec un compte. Il a toutefois rappelé que ByteDance a des filiales dans toutes les régions du monde et qu'il serait possible d'invoquer des arguments liés à la compétence pour justifier que la loi chinoise ne s'applique pas dans les régions du monde où il n'y a pas d'utilisateurs chinois.

Cependant, M. Andrey a expliqué que TikTok a fait l'objet d'un examen particulier de la part de The Dais, compte tenu de sa structure d'entreprise. Selon lui, avant 2019, la politique de confidentialité de TikTok était transparente en déclarant qu'elle communiquait les renseignements de ses utilisateurs « avec tout membre ou associé de [son] groupe » en Chine. Cette référence à un lieu précis a ensuite été supprimée, mais la disposition relative à la divulgation demeure. M. Andrey a expliqué que la même disposition apparait également dans la politique de protection de la vie privée de l'application WeChat – qui est utilisée par 6 % de la population canadienne – et que c'est le cas pour beaucoup d'autres.

M. Malone a quant à lui rappelé que TikTok s'est fait prendre à utiliser toutes sortes de méthodes inquiétantes en ce qui concerne les données des utilisateurs, comme le fait d'accéder à l'emplacement physique de journalistes qui utilisent l'application, afin de retrouver leurs sources. Il a aussi rappelé que TikTok a transféré les données de ses utilisateurs des États-Unis vers la Chine, alors qu'elle garantissait qu'elle ne le faisait pas. M. Malone a mentionné certains rapports internes du gouvernement canadien, émanant notamment du Secrétariat de l'évaluation du renseignement du Bureau du Conseil privé, qui cernent d'autres problèmes liés au type de données et à la collecte de données faite au moyen de TikTok.

M. Malone a aussi confié au Comité qu'il a eu l'occasion d'examiner un document du gouvernement fédéral intitulé *Economic Security and Technology: TikTok Takeover*, qui provient de l'unité du renseignement sur les cybermenaces de la Défense nationale,

dans lequel sont abordées des préoccupations liées à TikTok comme des opérations de surveillance et de renseignement, des violations de la vie privée, la collecte de données, l'ingérence politique, le contrôle du discours et la censure des exportations par le Parti communiste chinois. Selon M. Malone, le document aborde également des préoccupations relatives à de nombreuses autres entreprises de médias sociaux, comme Snapchat et LinkedIn.

CHAPITRE 3 : ENCADREMENT DES PLATEFORMES DE MÉDIAS SOCIAUX

Protection de la vie privée

À l'heure actuelle, la loi fédérale sur la protection des renseignements personnels qui concerne le secteur privé est la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Cette loi s'applique aux entreprises de compétence fédérale et à celles qui mènent des activités commerciales dans les provinces qui n'ont pas adopté de loi substantiellement similaire[64]. La LPRPDE a été adoptée en 2000.

En juin 2022, le gouvernement du Canada a présenté le projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois[65]. La Loi sur la protection de la vie privée des consommateurs (LPVPC) remplacerait la partie 1 de la LPRPDE.

En avril 2023, le projet de loi C-27 a franchi l'étape de la deuxième lecture à la Chambre et a été renvoyé au Comité permanent de l'industrie et de la technologie de la Chambre des communes[66]. Plusieurs témoins ont fait référence au projet de loi C-27 dans le cadre de la présente étude. Ces commentaires sont reflétés dans le présent chapitre. Cependant, les

64 Les trois provinces qui ont adopté des lois substantiellement similaires sont l'Alberta, la Colombie-Britannique et le Québec.

65 Projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois (Projet de loi C-27). Voir aussi : Sabrina Charland, Alexandra Savoie et Ryan van den Berg, *Résumé législatif du projet de loi C-27 : Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, publication nº 44-1-C27-F, Bibliothèque du Parlement, 12 juillet 2022.

66 Chambre des communes, *Journaux*, 44e législature, 1re session, 24 avril 2023.

recommandations du rapport portent sur des modifications à la LPRPDE, considérant qu'il s'agit de la loi en vigueur au moment de l'adoption de ce rapport. Le projet de loi C-27, s'il était adopté, pourrait combler certaines lacunes du régime législatif actuel soulevées par les témoins.

Consentement valide

La question du consentement valide a été soulevée à plusieurs reprises durant l'étude. Selon M. Dufresne, le projet de loi C-27 renforcerait le consentement valide en disant explicitement qu'il doit être donné avec des renseignements que l'individu concerné peut comprendre[67]. Toutefois, M[me] Polsky a affirmé que la LPVPC n'exige que la communication de certains éléments d'information en langage clair, sans niveau de détail suffisant. Le Conseil du Canada de l'Accès et la vie Privée (le CCAP), que M[me] Polsky préside, estime que la LPVPC confond notification et consentement[68]. Selon elle, les règles du consentement proposées dans le projet de loi C-27 et même celles au Québec, qui ont été modifiées par la Loi 25, laissent encore trop de marge de manœuvre aux organisations[69].

Au sujet des politiques de confidentialité des organisations, M. Dufresne a indiqué que le CPVP offre les conseils suivants : « faire en sorte que ce soit convivial; ne pas se contenter d'une action ponctuelle; veiller à ce qu'il y ait parfois un suivi; et rendre le tout le plus compréhensible possible ». Il a aussi suggéré d'adapter la façon d'obtenir le consentement lorsqu'il s'agit d'enfants, par exemple en recourant à une vidéo plutôt qu'à une politique écrite. Il a rappelé qu'il faut des données pour innover, mais que l'on peut aussi utiliser l'innovation pour protéger les données et aider au consentement et à l'explicabilité.

---

67 Projet de loi C-27, Loi sur la protection de la vie privée des consommateurs (LPVPC), art. 15. Le paragraphe 15(3) de la LPVPC prévoit que le consentement est valide si l'organisation a fourni certains renseignements à l'individu concerné. Le paragraphe 15(4) précise que ces renseignements doivent être fournis en langage clair. Voir aussi : Commissariat à la protection de la vie privée du Canada (CPVP), *Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-27, la Loi de 2020 sur la mise en œuvre de la Charte du numérique*.

68 Le paragraphe 6.1 de la LPRPDE prévoit actuellement que le consentement de l'individu concerné n'est valable que « s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti ». Voir aussi : ETHI, *Mémoire*, Conseil du Canada de l'Accès et la vie Privée (CCAP), para. 48. Ce mémoire présente les commentaires et recommandations du CCAP à l'égard du projet de loi C-27.

69 Assemblée nationale du Québec, Projet de loi n° 64 (2021, chapitre 25), *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25). Cette loi a modifié la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec.

Un exemple d'innovation soulevé par M.Gruzd est l'initiative « Terms of Service; Didn't Read ». Cette initiative permet à des juristes et des technologues d'évaluer les conditions d'utilisation de divers fournisseurs d'outils technologiques, y compris les plateformes de médias sociaux. Ils attribuent une note à ces conditions que les gens peuvent consulter en ligne[70]. M. Gruzd a souligné que toutes les grandes plateformes de médias sociaux, y compris TikTok, se voient attribuer la pire note par cette initiative. Pourtant, M. Harris a dit croire que les utilisateurs de X ont la capacité de comprendre, en lisant sa politique de confidentialité, ce à quoi ils consentent, y compris en ce qui concerne la collecte de données biométriques[71]. Le Comité note que les conditions de service de TikTok sont longues et rédigées en langage juridique. Sa politique de confidentialité est également longue[72].

D'autres témoins ont discuté des politiques de confidentialité. Par exemple, M. Caraway a critiqué la complexité des contrats de licence d'utilisateur, qui ne peuvent être compris que par des experts et peuvent changer quotidiennement, mettant ainsi en question ce que représente un consentement dans ce contexte. M. Khoury a reconnu qu'il serait bénéfique que les conditions d'utilisation auxquelles ils consentent soient expliquées dans un langage que les utilisateurs d'une application comprennent et qui leur permettent de savoir exactement ce qu'ils acceptent de partager et avec qui.

Le problème, selon M^me^ Polsky, est que les plateformes de médias sociaux reconnaissent que peu de gens lisent leurs politiques de confidentialité. À ses yeux, elles recueillent donc des données en sachant pertinemment que personne ne lit les politiques sur la protection des renseignements personnels; donc sans consentement éclairé. À son avis, les consommateurs canadiens devraient pouvoir consulter un index indiquant quelles entreprises se conforment aux lois canadiennes sur la protection des renseignements personnels pour mieux choisir à quelles entreprises ils décident de fournir leurs données.

Le CCAP et Sam Andrey ont critiqué les exceptions au consentement de la LPVPC relatives aux « activités d'affaires » et à « l'intérêt légitime ». Ces exceptions prévoient qu'une organisation peut recueillir ou utiliser les renseignements personnels d'un

70 ETHI, *Témoignages*, Gruzd. Une extension installée sur un navigateur Web affiche la note accordée aux conditions d'utilisation d'une plateforme ou d'un site Web et détaille ses lacunes, par exemple si la plateforme a accès aux messages privés des utilisateurs ou ne supprime pas réellement leurs données.

71 ETHI, *Témoignages*, Josh Harris (conseiller principal en matière de protection de la vie privée et des données, X Corporation).

72 TikTok, *Terms of Service* [DISPONIBLE EN ANGLAIS SEULEMENT]; TikTok, *Privacy Policy* [DISPONIBLE EN ANGLAIS SEULEMENT].

individu à son insu et sans son consentement dans le cadre d'activités d'affaires ou lorsqu'elle a des « intérêts légitimes » pour le faire[73].

M. Malone a de son côté souligné qu'il est difficile de parler de consentement valide et éclairé lorsqu'un déséquilibre des pouvoirs aussi grand existe entre un utilisateur individuel qui clique sur le bouton « accepter » d'une longue politique de confidentialité et une entreprise qui a une valeur sur le marché qui dépasse la taille de celle d'un pays du G7.

En fait, pour M. Malone, le consentement éclairé, sur lequel reposent les lois canadiennes sur la protection des renseignements personnels « ne sert pas les fins pour lesquelles nous avons vraiment besoin de lois sur la protection des données et la protection de la vie privée au pays ». Selon lui, il faudrait plutôt changer de paradigme pour que la possession, la conservation, l'utilisation et la communication de renseignements personnels deviennent une responsabilité plutôt qu'une façon rentable de gérer une entreprise.

Obligations juridiques des organisations

M. Dufresne a rappelé qu'il y a souvent un incitatif économique pour que les plateformes numériques utilisent les données de ses utilisateurs. Les États et les organismes de réglementation doivent donc créer des incitatifs pour protéger les renseignements personnels. Selon lui, deux types d'incitatifs devraient exister : un incitatif positif, qui reconnaît les bons comportements et donne des récompenses liées à la réputation; et un incitatif négatif, qui utilise la contrainte juridique.

Pour M. Dufresne une réglementation adéquate imposerait aux plateformes une obligation proactive : de publier leur plan de protection de la vie privée; de faire des vérifications, et de minimiser l'utilisation des données. Il ajouterait une obligation de bien expliquer l'utilisation qu'une organisation fait des données qu'elle recueille. Le non-respect de ces obligations devrait mener à des vérifications, des enquêtes, des ordonnances et des amendes.

M. Dufresne a aussi rappelé que la LPRPDE est plus ancienne que les médias sociaux. À son avis, à mesure que la technologie progresse, des obligations proactives plus fortes sont requises. Par exemple, on devrait obliger les organisations à faire des évaluations de

73 LPVPC, art. 18. La liste des activités visées par l'exception relative aux « activités d'affaires » se trouve au paragraphe 18(2) de la LPVPC. Ce qui constitue un « intérêt légitime » est précisé au paragraphe 18(3). Pour se prévaloir des exceptions de l'article 18, une organisation doit satisfaire certains critères ou conditions préalables; Voir aussi : CCAP, *Mémoire*, paras. 47-56, 59-63, 72-73.

base et à les divulguer au CPVP. Il faudrait aussi imposer une plus grande obligation de transparence, notamment en ce qui a trait à l'utilisation de l'IA.

Minimisation des données

Concernant la minimisation des données, M. Gruzd a noté que des éléments du projet de loi C-27 pourraient permettre aux citoyens canadiens de demander que leurs données soient supprimées[74]. Il a toutefois noté qu'il est trop fréquent que les plateformes recueillent par défaut plus de données que nécessaire. Selon lui, il faut donc passer de la responsabilité individuelle à l'élaboration de stratégies qui obligent les entreprises à protéger les renseignements personnels dès la conception et par défaut.

Selon M. Caraway, considérant l'impératif économique de maximiser la collecte de données, des critères juridiques devraient limiter la collecte de données. Il a rappelé à nouveau que lorsqu'on a accès sans entrave à des ressources limitées, il y a une propension à la surutilisation et à l'exploitation de ces ressources.

Comme solution à la collecte excessive de données, M^me^ Laidlaw a pour sa part proposé de définir des zones interdites, c'est-à-dire des formes de collecte de données qui devraient être considérées comme totalement inappropriées et être interdites.

M^me^ Laidlaw a expliqué que les utilisateurs semblent accepter la collecte de toutes sortes de données personnelles, car ils veulent utiliser une application[75]. Selon elle, les gens ne devraient pas pouvoir donner leur consentement à ce genre de collecte de données puisqu'ils ne comprennent pas vraiment ce qu'ils acceptent, comme la vente de leurs données personnelles à des courtiers en données. Une fois les données entre les mains des courtiers en données, il devient impossible de savoir ce qu'il en advient.

M^me^ Polsky est aussi d'avis qu'il faut lutter contre la position prise par les géants du Web, qui insistent sur le fait que les utilisateurs désirent qu'ils recueillent autant de renseignements personnels pour créer un profil de nous. Comme peu de gens comprennent vraiment ce que ces entreprises font avec leurs données, elle n'est pas d'accord avec leur position.

Concernant la capacité pour un utilisateur de savoir ce qui arrive aux données qu'il fournit à une plateforme en ligne après qu'elles ont été partagées avec une tierce partie

74 LPVPC, art. 55 (droit de retrait). Un individu peut demander le retrait de ses renseignements personnels, sauf lorsqu'une exception s'applique. Aucune exception ne peut être utilisée pour refuser le retrait des renseignements personnels de mineurs.

75 ETHI, *Témoignages*, Brett Caraway (professeur agrégé de l'économie des médias, University of Toronto).

comme un courtier en données, Mme Laidlaw a mentionné que la *California's Online Privacy Protection Act* prévoit « essentiellement qu'il faut être en mesure de suivre ces données et à qui elles sont destinées ». Cette loi, selon elle, est plus efficace que la loi canadienne en ce qui concerne la capacité d'un individu de savoir ce qui arrive avec ses données personnelles en ligne[76].

Pouvoir d'ordonnance et sanctions administratives pécuniaires

M. Dufresne a rappelé qu'en vertu de la LPRPDE, le commissaire à la protection de la vie privée ne peut faire que des recommandations non contraignantes. Les plateformes peuvent donc décider si elles donnent suite aux recommandations du CPVP[77]. Il a fait remarquer que si une organisation amasse des millions de dollars en utilisant des données et qu'il n'y a pas de sanction pécuniaire lors d'un manquement à la loi, elle peut être tentée de le refaire. Le fait que le commissaire ne puisse pas émettre d'ordonnance ni de sanction pécuniaire administrative est, selon lui, une lacune importante du régime législatif actuel.

Mme Polsky est d'avis que les organismes de réglementation des lois sur la protection des renseignements personnels n'ont pas assez de pouvoirs ni assez de financement[78].

Le Comité note que le projet de loi C-27 donnerait au commissaire à la protection de la vie privée le pouvoir de rendre des ordonnances. Il lui donnerait aussi le pouvoir de recommander au Tribunal de la protection des renseignements personnels et des données, nouvellement créé, d'imposer une sanction administrative pécuniaire. Le commissaire n'aurait pas le pouvoir d'imposer lui-même une sanction administrative pécuniaire en vertu du projet de loi C-27[79].

---

76 California, *California's Online Privacy Protection Act* [DISPONIBLE EN ANGLAIS SEULEMENT]. La loi exige que les sites Web commerciaux ou services en ligne affichent leur politique de confidentialité, qui doit indiquer si des tiers peuvent recueillir les renseignements personnels des consommateurs pour assurer le suivi d'une personne sur plusieurs sites Web afin de dresser un profil de son comportement et de ses intérêts. Elle doit aussi indiquer comment le site Web ou service en ligne répond aux demandes « ne pas suivre » des navigateurs Web.

77 Voir aussi : ETHI, *Témoignages*, Dufresne.

78 Voir aussi : CCAP, *Mémoire*, paras. 56 et 70, 109-112.

79 Projet de loi C-27, LPVPC, arts. 93-95. L'article 95 de la LPVPC permet au Tribunal de la protection des renseignements personnels et des données (le Tribunal) d'imposer des sanctions administratives pécuniaires pour le non-respect de certains articles de la LPVPC.

Amendes

En ce qui concerne les amendes, M. Caraway a dit appuyer l'approche proposée par le projet de loi C-27, qui prévoit une amende pouvant aller jusqu'à 5 % des recettes globales brutes de l'organisation au cours de l'exercice financier précédent[80].

Mme Polsky irait plus loin. S'appuyant sur la *Sarbanes-Oxley Act 2022* des États-Unis, qui prévoit que la personne à la tête d'une organisation est responsable de tout ce qui figure à l'état financier de celle-ci, elle a recommandé que les amendes soient imposées aux dirigeants d'entreprises plutôt qu'uniquement à l'organisation[81]. Elle a toutefois reconnu qu'il pourrait être bénéfique d'avoir les deux : des amendes imposées à l'entreprise et des conséquences pour les dirigeants.

Codes de pratique et droit d'action privé

M. Dufresne a souligné que le projet de loi C-27 prévoit la création de codes de pratique et de programmes de certification[82]. Selon lui, cette pratique incitera les organismes à adhérer à une série de règles et le respect de ces règles aura un effet bénéfique sur le processus de plaintes[83]. Le CCAP a toutefois soulevé la possibilité que cette approche fasse en sorte qu'une organisation doive se soumettre à plus d'un code de pratique. Cela rendrait le respect des codes de pratique plus difficile[84].

80 Projet de loi C-27, LPVPC, art. 128. L'article 128 de la LPVPC prévoit une infraction si une organisation contrevient à certaines dispositions précises de la loi (art. 58, para. 60(1), arts. 69 et 75, et para. 127(1)) ou fait obstruction au travail du commissaire. Une infraction de la LPVPC peut mener à une amende, qui est imposée par la Cour, suivant une poursuite par le procureur général du Canada.

81 Les sanctions administratives pécuniaires et les amendes prévues dans la LPVPC sont imposées à l'organisation concernée et non à ses dirigeants. Les amendes en vertu de la LPRPDE sont imposées aux organisations.

82 Projet de loi C-27, LPVPC, art. 76. Une entité peut demander au commissaire à la protection de la vie privée d'approuver un code prévoyant des pratiques qui permettent de mettre en place une protection des renseignements personnels équivalente ou supérieure à tout ou partie de celle prévue sous le régime de la LPVPC.

83 Projet de loi C-27, LPVPC, art. 87. Une plainte peut être irrecevable si la question soulevée dans la plainte fait l'objet d'un programme de certification approuvé par le commissaire et que l'organisation visée est certifiée (alinéa 87(1)d) de la LPVPC).

84 CCAP, *Mémoire*, paras. 107-108.

M^me^ Polsky a critiqué le droit d'action privé prévu dans la LPVPC en raison du fait qu'il ne peut être exercé qu'après que le processus de plainte auprès du CPVP et le processus d'appel devant le Tribunal aient eu lieu[85]. La LPRPDE ne contient pas de droit d'action privé.

Transfert transfrontalier de données

Plusieurs témoins ont déploré l'absence d'une disposition explicite concernant les transferts transfrontaliers dans la LPRPDE et la LPVPC, qui la remplacerait.

M. Malone a noté que ni la LPRPDE ni le projet de loi C-27 ne contiennent une contrainte significative sur les transferts transfrontaliers de données vers des pays comme la Russie et la Chine. Il a affirmé qu'un transfert de données transfrontalier est permis en vertu des articles 11 et 19 de la LPVPC[86]. Il a aussi affirmé qu'une note interne obtenue par l'entremise d'une demande d'accès à l'information confirme que le gouvernement aurait volontairement évité d'intégrer des restrictions à l'égard des transferts transfrontaliers dans le projet de loi C-27 par respect pour les intérêts commerciaux des entreprises qui y sont assujetties[87].

Le CCAP a lui aussi soulevé des inquiétudes à l'égard des articles 11 et 19 de la LPVPC. Par exemple, selon le CCAP, l'article 19, qui permet le transfert de renseignements personnels à un fournisseur de services à l'insu et sans le consentement de l'individu concerné, rend le droit de retirer son consentement à l'article 17 sans objet. Il rend aussi l'exercice du droit de retrait prévu à l'article 55 plus difficile, puisque certains renseignements personnels de l'individu concerné pourraient avoir été partagés avec un fournisseur de services ou une autre partie à son insu[88].

Comme indiqué dans le chapitre 1, M. Masoodi a indiqué qu'aucune protection adéquate sur la manière dont les données personnelles des Canadiens sont transférées et stockées, en particulier à l'étranger, n'existe au Canada. Ainsi, selon lui, de solides

85 CCAP, *Mémoire*, paras. 121-122. Projet de loi C-27, LPVPC, art. 107.

86 Projet de loi C-27, LPVPC, para. 11(1). Ce paragraphe impose à l'organisation qui transfère des renseignements personnels à un fournisseur de services l'obligation de veiller, contractuellement ou autrement, à ce que celui-ci offre une protection équivalente à celle qu'elle est tenue d'offrir sous le régime de la LPVPC. Le fournisseur de services n'est pas assujetti à la LPVPC, sauf en ce qui concerne les articles 57 et 61 (mesures de sécurité). L'article 19 de la LPVPC permet à une organisation de transférer à des fournisseurs de services les renseignements personnels d'un individu à son insu ou sans son consentement.

87 Matt Malone, *Document de référence soumis au Comité ETHI* [HYPERLIEN NON DISPONIBLE].

88 CCAP, *Mémoire*, paras. 57-58 et 68-69, 92-93; Projet de loi C-27, LPVPC, para. 11(2), arts. 17, 19, para. 55(4), arts. 57 et 61.

mesures de protection de la vie privée doivent être mises en place, surtout en ce qui concerne les transferts de données transfrontaliers.

De façon similaire, M. Andrey a argué que dans sa forme actuelle, le projet de loi C-27 permet un échange plus facile de données entre entreprises en érodant les dispositions limitées qui existent en matière de consentement. Il a recommandé que des exigences plus précises soient ajoutées au projet de loi C-27 pour garantir des niveaux de protection équivalents pour les données personnelles qui sont transférées à l'extérieur du Canada. Il a recommandé des exigences comparables à celles du RGPD[89]. Il a aussi soulevé la possibilité d'interdire le transfert de données d'utilisation des mineurs vers des pays où la protection est insuffisante.

M. Malone a lui aussi noté que les exigences du RGPD sont plus strictes que les règles applicables au transfert de données au Canada et qu'elles prévoient un test d'équivalence robuste[90]. Toutefois, il a fait remarquer que, contrairement à l'Europe, les États-Unis n'ont pas de loi fédérale uniforme sur la protection des renseignements personnels. Ils exportent, par l'entremise de traités commerciaux et d'organismes de gouvernance dans le monde entier, une vision de la gouvernance des données et de la protection de la vie privée qui affecte ce que le Canada peut faire. M. Malone a par exemple souligné que l'Accord Canada-États-Unis-Mexique interdit de restreindre les flux de données transfrontaliers. L'Accord de Partenariat transpacifique global et progressiste contient une interdiction semblable.

M. Malone a aussi mentionné la possibilité de création de zones sécuritaires pour le flux des données, qui miseraient sur les alliances existantes en matière de sécurité, comme l'OTAN. Considérant l'engagement de défense mutuelle des alliés de l'OTAN, il est d'avis qu'il serait logique d'échanger nos données et nos renseignements personnels avec ces alliés dans une zone permettant le libre mouvement transfrontalier des données.

89 Le chapitre 5 du Règlement général sur la protection des données prévoit des exigences concernant le transfert de données à caractère personnel vers des pays tiers ou des organisations internationales (arts. 44-50). Voir aussi: Stevens, Y., Masoodi, M.J. & Andrey. S, *Home Ice Advantage: Securing Data Sovereignty for Canadians on Social Media*, Cybersecure Policy Exchange, 2020. Le rapport fait la même recommandation et ajoute que les plateformes de médias sociaux devraient être obligées d'obtenir le consentement explicite des utilisateurs canadiens pour transférer leurs données personnelles dans des États qui n'offrent pas un niveau de protection équivalent à celui du Canada.

90 Le Règlement général sur la protection des données permet, entre autres, le transfert de données entre deux pays lorsque le pays à l'extérieur de l'Union européenne fait l'objet d'une décision d'adéquation qui confirme qu'il offre un niveau de protection des renseignements personnels adéquat.

Application des lois au gouvernement et aux partis politiques

Selon M. Malone le Canada a besoin de lois sur la protection des renseignements personnels qui démontrent aux Canadiens que le gouvernement prend la chose au sérieux. Cela veut dire une loi robuste qui s'applique à la conduite du gouvernement. Cela veut aussi dire que « les partis politiques, qui sont souvent très prompts à dénoncer les atteintes à la vie privée perpétrées par les entreprises privées de médias sociaux » devraient être visés par la législation canadienne sur la protection des renseignements personnels. Selon lui, il serait plus facile de convaincre les jeunes, qui sont les plus grands utilisateurs de plateformes de médias sociaux, de l'importance de prendre les questions de protection de la vie privée au sérieux si ces lois s'appliquaient à la conduite du gouvernement et aux partis politiques.

Considérant ce qui précède, le Comité fait les recommandations suivantes.

Recommandation 2

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* afin d'imposer aux organisations qui y sont assujetties davantage d'obligations en matière de minimisation de données, y compris l'interdiction de mener certaines formes de collecte de données.

Recommandation 3

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* pour donner des pouvoirs d'ordonnance contraignants au commissaire à la protection de la vie privée du Canada et le pouvoir d'imposer des sanctions administratives pécuniaires sévères.

Recommandation 4

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* afin d'y inclure des règles explicites concernant les transferts de renseignements personnels de Canadiens à l'extérieur du pays pour garantir des niveaux de protection équivalents pour les données transférées à l'extérieur du Canada.

Protection de la vie privée des mineurs

Au sujet de la protection de la vie privée des mineurs en ligne, M. Dufresne a dit

> [g]randir à l'ère numérique présente de nouveaux défis importants pour la vie privée des jeunes. Alors que les enfants et les jeunes adultes adoptent de nouvelles technologies et vivent une grande partie de leur vie en ligne, nous avons besoin de solides mesures pour protéger leurs renseignements personnels et encadrer la façon dont ces renseignements personnels pourraient être recueillis, utilisés et communiqués. Les renseignements personnels des enfants et des jeunes sont de plus en plus utilisés afin de créer du contenu personnalisé et des profils de publicité visant à influencer leurs comportements.
>
> Les enfants ont le droit d'être des enfants, même dans le monde numérique. Comme l'indique l'UNICEF dans ses orientations stratégiques sur l'IA destinée aux enfants, les jeunes sont davantage touchés par les technologies numériques que les adultes. Les jeunes sont aussi moins à même de comprendre les conséquences à long terme d'un consentement à la collecte de leurs données. Les lois sur la protection des renseignements personnels devraient reconnaître les droits de l'enfant, et le droit d'être un enfant. Cela signifie qu'il faut interpréter les dispositions des lois relatives à la protection des renseignements personnels d'une manière qui est cohérente avec l'intérêt supérieur de l'enfant.

M. Dufresne a affirmé qu'il est essentiel pour le gouvernement et les organisations de prendre des mesures permettant d'assurer que les jeunes puissent bénéficier de la technologie et être actifs en ligne sans craindre d'être ciblés, manipulés ou de subir des préjudices. Il a mentionné la déclaration commune portant sur l'intérêt supérieur des enfants qu'ont émis ses homologues provinciaux et territoriaux et lui-même en août 2023. Elle énonce les attentes des commissaires en matière de protection des renseignements personnels et inclut des recommandations[91]. La déclaration commune contient aussi des recommandations pour que les organisations s'assurent de bien protéger les enfants et de voir à leur intérêt supérieur en traitant leurs données de la manière qui convient.

Les recommandations des commissaires incluent : fournir des outils de protection de la vie privée et des mécanismes de consentement adaptés aux jeunes et au degré de maturité de ceux-ci; rejeter les pratiques trompeuses qui influencent négativement les décisions relatives à la vie privée ou les poussent à adopter des comportements préjudiciables; et permettre la suppression et la désindexation des données recueillies lorsque les utilisateurs étaient des enfants[92].

M. Dufresne a ajouté que le CPVP a formulé un certain nombre de recommandations pour interdire les techniques comportementales d'incitation en ligne. Il a souligné que des études ont démontré que les médias sociaux créent une dépendance chez les enfants. Le

91 CPVP, *Mettre l'intérêt supérieur des jeunes à l'avant-plan en matière de vie privée et d'accès aux renseignements personnels*, octobre 2023.

92 *Ibid*.; ETHI, *Témoignages*, Dufresne.

modèle d'affaires des plateformes de médias sociaux consiste parfois à essayer de les encourager à rester branchés plus longtemps, parce que c'est ce qui génère des revenus.

Mme Laidlaw a de son côté qualifié les pratiques utilisées par certaines plateformes de médias sociaux auprès des enfants de manipulation de l'esprit. Elle pense que des interventions similaires à celles qui ont été faites dans le milieu publicitaire par le passé pour empêcher la diffusion de certaines publicités à certains moments de la journée ou pendant des émissions pour enfants devraient être prises pour protéger les enfants en ligne.

Cependant, en réponse à des questions concernant l'impact de Meta sur les mineurs, Mme Curran a affirmé que « les plus récentes recherches dont nous disposons n'appuient pas l'hypothèse selon laquelle la technologie numérique est responsable des tendances liées à la santé mentale et au bien-être des adolescents ». Elle a indiqué que d'autres facteurs, comme l'instabilité économique ou la dépendance aux substances, influent sur le bien-être et la santé mentale des adolescents[93]. Elle a aussi dit qu'il serait « erroné, voire irresponsable, de laisser entendre qu'un seul facteur est à l'origine de certaines tendances en santé mentale chez les adolescents ».

En ce qui concerne le projet de loi C-27, M. Dufresne a dit trouver encourageantes les déclarations du ministre de l'Innovation, des Sciences et de l'Industrie selon lesquelles le gouvernement est prêt à proposer des amendements au projet de loi pour renforcer la protection de la vie privée des enfants, en ajoutant notamment dans son préambule que le traitement des renseignements personnels doit protéger l'intérêt supérieur de l'enfant[94]. M. Caraway a toutefois noté que la protection des enfants doit être incluse dans les articles du projet de loi et non pas seulement dans son préambule.

M. Dufresne a aussi rappelé que des obligations plus importantes sur le plan de la vigilance et des moyens utilisés pour obtenir le consentement s'imposent pour les mineurs, en raison du fait que leurs renseignements personnels sont de nature sensible. Il a indiqué que les lignes directrices du CPVP concernant l'obtention d'un consentement valide en vertu de la LPRPDE précisent que le consentement parental devrait être requis dans certaines circonstances, y compris pour tout enfant de 13 ans ou moins[95].

93 Voir aussi : ETHI, *Témoignages*, Curran.

94 Voir : INDU, *Correspondance de l'honorable François-Philippe Champagne, ministre de l'Innovation, des Sciences et de l'Industrie*, 3 octobre 2023.

95 CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, 13 août 2021.

La LPRPDE ne contient aucune obligation spécifique relative aux renseignements personnels des mineurs. La LPVPC prévoit que tout renseignement d'un mineur est un renseignement de nature sensible[96].

Le CCAP définirait le terme « mineur » dans la LPVPC comme un individu de 14 ans et moins pour assurer une uniformité avec la loi québécoise, qui exige le consentement parental pour la collecte de renseignements personnels d'un individu de 14 ans ou moins[97]. Une modification adoptée par le comité parlementaire chargé d'examiner le projet de loi C-27 a inclus la définition suivante du terme mineur dans la LPVPC : « un individu âgé de moins de 18 ans[98] ».

Un autre droit important pour les mineurs, selon M. Dufresne, est le droit de retrait que l'on trouve à l'article 55 de la LPVPC. Il a dit à ce sujet :

> Quand je dis que les enfants ont le droit d'être des enfants, c'est ce à quoi je fais allusion. Les enfants font des choses en ligne. Si le contenu reste en ligne pour toujours, ils seront traités comme des adultes dès leur adolescence. Si le contenu reste en permanence, il pourrait être utilisé contre eux pour des emplois et ainsi de suite.

Concernant la possibilité d'imposer un mécanisme de vérification de l'âge en ligne, M. Dufresne a dit que le CPVP prend la position que les outils de vérification d'âge doivent être appropriés et ne pas demander trop de renseignements personnels. Il faut aussi s'assurer que la vérification de l'âge soit adaptée au contexte. Certains sites Web présentent un plus haut risque et demandent une vérification plus serrée. D'autres sont peut-être destinés aux enfants.

M^me^ Polsky a aussi exprimé des réserves à l'égard de cette pratique. Le CCAP estime que la vérification de l'âge en ligne nécessite la communication et la collecte de renseignements personnels sensibles, ce qui va à l'encontre de l'objectif de protection des mineurs du projet de loi C-27[99]. Il a noté, par exemple, qu'une telle exigence se trouve dans le projet de loi S-210, Loi limitant l'accès en ligne des jeunes au matériel sexuellement explicite. Même si le projet de loi prévoit une obligation de détruire les renseignements personnels

96 Projet de loi C-27, LPVPC, par. 2(2).

97 CCAP, *Mémoire*, p. 22, Recommandation 21.

98 Chambres des communes, Comité permanent de l'industrie et de la technologie, *Procès-verbal*, 29 avril 2024.

99 Projet de loi S-210, Loi limitant l'accès en ligne des jeunes au matériel sexuellement explicite.

recueillis une fois l'âge vérifié, le CCAP estime que rien ne garantit que cette exigence sera respectée[100].

En ce qui concerne la possibilité d'utiliser des technologies de détection et de vérification d'âge, M. Lieber a affirmé que bien qu'elles permettraient de connaître avec plus de précision l'âge des utilisateurs, ces technologies ont des incidences du point de vue de la protection de la vie privée.

À la question de savoir s'il serait pertinent d'imposer le consentement parental pour qu'une personne de moins de 16 ans puisse télécharger une application de médias sociaux, M. Larkin n'a pas rejeté l'idée. M. Andrey a dit qu'une telle obligation ne nuirait probablement pas, mais que la logistique associée à la vérification de l'âge est complexe. M. Malone a pris la position contraire. Selon lui, imposer un consentement parental pour le téléchargement d'application aurait des effets négatifs. À son avis, la responsabilité ne devrait pas revenir aux parents. Ce qu'il faut plutôt, c'est une loi sur la protection des renseignements personnels qui protège les enfants par défaut.

M. Fernandez n'a pas pris de position formelle sur la possibilité d'imposer un contrôle parental pour le téléchargement d'application de médias sociaux par des adolescents. Il a noté qu'X n'est pas la plateforme de choix des adolescents. M^me^ Curran a dit que Meta appuierait ce genre d'exigence, pourvu qu'elle s'applique à l'ensemble de l'industrie. M^me^ Patell a noté qu'il est possible de mettre des contrôles parentaux sur les appareils Android, qui peuvent limiter le contenu qui peut être téléchargé sur l'appareil à partir de Google Play en fonction de l'âge.

Considérant ce qui précède et l'importance qu'il accorde à la protection de la vie privée des mineurs en ligne, le Comité fait la recommandation suivante.

Recommandation 5

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* afin d'imposer aux organisations assujetties à la *Loi* l'obligation de fournir des mécanismes de consentement adaptés aux mineurs et d'y inclure un droit explicite à la suppression et la désindexation des données personnelles pour les mineurs.

100 CCAP, *Mémoire*, paras. 40, 83, 104-106; Projet de loi S-210, Loi limitant l'accès en ligne des jeunes au matériel sexuellement explicite. Au moment de l'adoption du présent rapport, le projet de loi était à l'étape de la troisième lecture à la Chambre des communes.

Contrer la désinformation, la mésinformation et les contenus préjudiciables en ligne

Désinformation et mésinformation

Pour lutter contre la désinformation, M. Gruzd a recommandé une approche globale qui obligerait les plateformes à faire trois choses. Les plateformes devraient : s'engager à adopter les principes de protection de la vie privée dès la conception et par défaut; investir dans l'élargissement de leurs équipes chargées de la confiance et de la sécurité; et communiquer leurs données aux chercheurs et journalistes.

M. Gruzd a rappelé que l'éducation individuelle est l'une des façons de lutter contre la désinformation et la mésinformation, mais que les plateformes devraient être tenues d'incorporer des outils qui peuvent signaler les problèmes potentiels. Il a donné l'exemple de la pandémie de COVID-19, lorsque les plateformes se sont mobilisées et ont fait des interventions utiles, comme l'ajout d'un lien vers Santé Canada lorsque quelqu'un parlait de la COVID-19 ou le signalement qu'une partie du contenu de l'article peut ne pas refléter fidèlement les connaissances scientifiques. De telles interventions sont utiles pour réduire la propagation de la désinformation et de la mésinformation, selon lui.

M^{me} Laidlaw a reconnu que trouver des solutions est particulièrement difficile dans un contexte de désinformation et de mésinformation, car il est « légal — sauf dans des cas très précis — de croire et de diffuser de fausses informations ».

Pour évaluer dans quelle mesure les plateformes luttent contre la désinformation, M. Gruzd a aussi recommandé que le Canada crée un code de pratique sur la désinformation calqué sur le code de l'Union européenne (UE), ainsi qu'un référentiel de transparence qui obligerait les grandes plateformes à rendre régulièrement compte de leurs activités en matière de confiance et de sécurité au Canada[101]. Par exemple, il a expliqué qu'en vertu du Règlement sur les services numériques de l'UE, les plateformes qui comptent plus de 45 millions d'utilisateurs doivent rendre compte de leurs activités et des mesures qu'elles ont prises pour mettre fin à l'ingérence étrangère dans chaque pays environ tous les six mois. Elles doivent aussi rendre compte des mesures prises pour lutter contre la désinformation[102].

---

101 Commission européenne, 2022 code de bonnes pratiques renforcé contre la désinformation, 16 juin 2022; ETHI, *Témoignages*, Gruzd. Il s'agit de normes d'autorégulation pour l'industrie.

102 ETHI, *Témoignages*, Gruzd; Union européenne, *Journal officiel de l'Union européenne*, Règlement sur les services numériques.

Pour renforcer la transparence et la surveillance, M. Gruzd a aussi recommandé de rendre obligatoire l'accès aux données pour les chercheurs et journalistes. Selon lui, un tel accès est essentiel pour détecter de manière indépendante les tendances néfastes. Il a noté que dans l'UE, cet accès est prévu par le Règlement sur les services numériques[103]. Il a dit que TikTok n'accorde pas aux chercheurs canadiens l'accès à ses données, mais elle le fait pour ceux qui résident aux États-Unis et dans l'UE. Il a dit qu'X a récemment fermé son accès gratuit aux données pour les chercheurs[104]. M. Fernández a toutefois indiqué qu'X a une

> [Interface de programmation d'applications] ouverte au public qui met des données à la disposition des développeurs, des journalistes, des marques et des chercheurs à des fins d'analyse et pour bâtir des entreprises, offrir des services et créer des produits novateurs.

M. Gruzd a aussi recommandé que les équipes de modération de contenu soient élargies. Il a noté que la taille des équipes de confiance et sécurité des entreprises semble diminuer. Selon lui, avoir moins d'équipes de confiance et sécurité peut affecter la prolifération de contenus préjudiciables en ligne.

Considérant ce qui précède, le Comité fait la recommandation suivante.

Recommandation 6

Que le gouvernement du Canada adopte un code de pratique sur la désinformation similaire à celui de l'Union européenne et qu'il oblige les plateformes de médias sociaux à rendre régulièrement compte de leurs activités en matière de confiance et de sécurité au Canada et à donner aux chercheurs canadiens l'accès à leurs données.

Cadre législatif concernant les préjudices en ligne

En 2021, le gouvernement s'est engagé à mettre en place un cadre réglementaire transparent et responsable pour la sécurité en ligne au Canada[105]. Le guide de discussion de la consultation en ligne qui a eu lieu la même année précisait les cinq catégories de contenus préjudiciables visées par ce projet de cadre législatif: le contenu terroriste; le

103 *Ibid.*, art. 40.

104 ETHI, *Témoignages*, Gruzd.

105 Gouvernement du Canada, *L'engagement du gouvernement en faveur de la sécurité en ligne*.

contenu incitant à la violence; le discours haineux; le partage non consensuel d'images intimes et le contenu d'exploitation sexuelle des enfants en ligne[106].

Des tables rondes sur la sécurité en ligne et une assemblée citoyenne sur l'expression démocratique ont eu lieu en 2022. La même année, un groupe consultatif d'experts sur la sécurité en ligne a été créé pour fournir au ministre du Patrimoine canadien des conseils sur la conception d'un cadre législatif et réglementaire pour lutter contre les préjudices en ligne[107].

Le 26 février 2024, le gouvernement du Canada a présenté le projet de loi C-63, Loi édictant la Loi sur les préjudices en ligne, modifiant le Code criminel, la Loi canadienne sur les droits de la personne et la Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet et apportant des modifications corrélatives et connexes à d'autres lois. Selon son sommaire, entre autres objectifs du projet de loi, la partie 1

> édicte la *Loi sur les préjudices en ligne*, qui a notamment pour objet de promouvoir la sécurité en ligne des personnes au Canada, de réduire les préjudices qui leur sont causés par le contenu préjudiciable en ligne et de veiller à ce que les exploitants de services de médias sociaux assujettis à la loi soient transparents et tenus de rendre des comptes à l'égard des obligations qui leur incombent au titre de la loi.

Le projet de loi C-63, s'il était adopté dans sa forme actuelle, pourrait combler certaines des lacunes identifiées par les témoins.

L'accès à des contenus préjudiciables peut entraîner des effets négatifs. Par exemple, M^me^ Henderson a souligné que des jeunes vont parfois sur les réseaux sociaux, se retrouvent dans un milieu extrémiste et se font influencer négativement. Elle a expliqué que des organisations terroristes dans d'autres pays surveillent les médias sociaux, créent des sites Web et tentent d'attirer les jeunes qui sont vulnérables.

M^me^ Laidlaw a rappelé qu'actuellement, la santé de notre écosystème d'information dépend des choix que font des plateformes numériques du secteur privé concernant la conception de leurs produits, la gouvernance et la culture de leur entreprise, et les systèmes de modération de contenu qu'elles utilisent. Elle a souligné que le Canada tire de l'arrière sur le plan de la réglementation des plateformes de médias sociaux, car il n'a pas encore adopté de loi sur les préjudices en ligne. Une telle loi existe déjà en Europe, au Royaume-Uni et en Australie. Le Canada peut donc s'inspirer d'autres lois en vigueur.

---

106 Gouvernement du Canada, L'engagement du gouvernement en faveur de la sécurité en ligne, *Guide de discussion*.

107 Gouvernement du Canada, *L'engagement du gouvernement en faveur de la sécurité en ligne*.

Selon elle, il devrait adopter une loi sur les préjudices en ligne avant que des enquêtes mondiales plus coordonnées voient le jour.

M. Andrey a aussi noté que le Canada peut apprendre des erreurs d'autres pays. Il a donné l'exemple de l'Allemagne, qui a créé un régime de retrait de contenu préjudiciable dans les 24 heures qui a mené à une censure excessive. Les plateformes de médias sociaux, ne voulant pas être tenues responsables, ont retiré du contenu légal. La loi a depuis été modifiée[108].

Mme Laidlaw a expliqué les risques d'adopter une loi inadéquate.

> Si vous adoptez une loi qui ne fait que mettre l'accent sur les préjudices, vous inciterez les entreprises à mettre en place des solutions rudimentaires qui, en fait, entraîneront des conséquences fortuites. Beaucoup de preuves démontrent que l'effet inverse peut se produire: ce sont les voix racisées et d'autres voix marginalisées qui finissent par être réduites au silence.

Ainsi, selon elle, les plateformes de médias sociaux, si elles se soucient des préjudices causés aux personnes, doivent avoir deux priorités : la protection et la promotion de la liberté d'expression; et la capacité de démontrer à un organisme de réglementation les mesures qu'elles prennent pour éliminer les contenus préjudiciables et prouver que ces mesures sont adaptées à leurs contextes et à leurs services.

Mme Laidlaw a aussi expliqué pourquoi un cadre législatif encadrant les plateformes de médias sociaux est important et comment un tel cadre doit être conçu. Premièrement, la réglementation des plateformes comporte des similitudes avec la protection de l'environnement, en ce sens que de nombreux domaines du droit doivent se conjuguer pour protéger notre sécurité et nos droits. Les lois sur la protection des renseignements personnels et les lois sur les contenus préjudiciables en ligne se renforcent mutuellement. Elles sont donc toutes deux nécessaires[109]. Elle a expliqué :

> Les algorithmes qui poussent du contenu préjudiciable le font grâce à la collecte de renseignements permettant d'identifier une personne, ce qui relève du droit relatif au respect de la vie privée. Toutefois, l'algorithme peut aussi utiliser des données agrégées anonymisées, ce qui ne relève pas du droit relatif au respect de la vie privée.

Mme Laidlaw a aussi expliqué que le projet de loi C-27, qui s'appuie sur le paradigme du consentement, n'aborde pas certains des aspects les plus problématiques des médias

---

108 Voir, par exemple: États-Unis, Library of Congress, *Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech* [DISPONIBLE EN ANGLAIS SEULEMENT].

109 ETHI, *Témoignages*, Emily Laidlaw (professeure agrégée et titulaire de la Chaire de recherche du Canada en droit de la cybersécurité, University of Calgary).

sociaux et de leur influence, auxquels, en réalité, personne ne peut consentir. Le Canada a donc également besoin d'une loi sur les préjudices en ligne, qui ciblerait les choix des plateformes de médias sociaux en matière de conception de produits et de systèmes de modération de contenu[110].

Deuxièmement, les plateformes de médias sociaux peuvent être d'importants collaborateurs et innovateurs dans la résolution de problèmes. Ils doivent faire partie de la solution. Cependant, M^me^ Laidlaw a reconnu qu'une friction existe lorsque le rôle d'une plateforme s'apparente à celui d'un État, par exemple dans le cas où elle dispose d'une équipe de sécurité nationale qui établit essentiellement des politiques dans ce domaine. D'autres plateformes, en revanche, font très peu pour gérer les risques associés à leurs produits, selon elle. Ainsi, même s'il est essentiel que les plateformes de médias sociaux participent à la lutte contre le contenu haineux, la désinformation et l'extrémisme violent, M^me^ Laidlaw estime que cette participation ne remplace pas une loi établissant les normes de l'industrie.

Troisièmement, M^me^ Laidlaw a rappelé que les risques de préjudice ne sont pas les mêmes pour tous les types de contenus préjudiciables. Selon elle, la protection des enfants, la propagande haineuse et terroriste, la désinformation et la violence ont chacune leur propre dynamique et ne devraient pas être regroupées sous une seule règle de droit, sauf l'idée fondamentale de la diligence raisonnable des entreprises. Ce type de contenu crée des risques pour les droits fondamentaux comme le droit à la liberté d'expression, le droit à la vie privée et le droit à l'égalité.

M^me^ Laidlaw a résumé les éléments de base nécessaires à l'élaboration d'une loi sur les préjudices en ligne. D'abord, une telle loi devrait exiger que les plateformes de médias sociaux gèrent les risques de préjudice de leurs produits et protègent les droits fondamentaux. Ensuite, elle devrait imposer des obligations de transparence assorties d'un mécanisme d'évaluation qui permettrait à des chercheurs autorisés de faire des vérifications et d'avoir accès aux données. Un organisme de réglementation chargé d'enquêter sur les entreprises et d'éduquer le public devrait aussi être créé. Enfin, la loi devrait prévoir des recours pour les victimes, en tenant compte du fait que le préjudice est à la fois collectif et individuel.

M^me^ Laidlaw a rappelé qu'à elle seule, la transparence ne donne rien. Il faut un mécanisme d'enquête et de vérification pour lever le voile sur les pratiques des entreprises de façon proactive, selon elle. M. Caraway a lui aussi noté l'importance des vérifications indépendantes sur la façon dont les données sont utilisées par une plateforme numérique.

110 ETHI, *Témoignages*, Laidlaw.

Au sujet de l'organisme de réglementation responsable d'une loi sur les préjudices en ligne, M^me^ Laidlaw a affirmé que l'organisme de réglementation pourrait intervenir avec plus d'agilité que les tribunaux[111]. Elle a recommandé que l'organisme ait le pouvoir d'enquêter sur les entreprises et de vérifier si elles se conforment à des obligations précises. Elle a précisé que cet organisme de réglementation devrait être indépendant du gouvernement et en mesure d'imposer des sanctions pécuniaires sévères.

M. Andrey, de son côté, a suggéré que l'organisme de réglementation d'une loi sur les préjudices en ligne soit le même que celui créé par le projet de loi C-27 dans la partie 3, la Loi sur l'intelligence artificielle et les données (LIAD). Comme M^me^ Laidlaw, il a insisté sur le fait que l'organisme de réglementation devrait être indépendant du ministère de l'Innovation, des Sciences et du Développement économique du Canada (ISDE).

Selon M^me^ Laidlaw, l'organisme de réglementation de la sécurité en ligne devrait aussi jouer un rôle d'éducation du public important, comme le commissaire à la sécurité en ligne en Australie[112]. Tout en reconnaissant la compétence des provinces en matière d'éducation, elle a indiqué qu'un programme fédéral d'éducation pourrait être établi et partagé avec les provinces afin d'influencer les programmes offerts dans les écoles et même dans les municipalités.

Encadrer l'utilisation de l'intelligence artificielle

Le projet de loi C-27 crée la Loi sur l'intelligence artificielle et les données (LIAD) dont l'objet est :

- de réglementer les échanges et le commerce internationaux et interprovinciaux en matière de systèmes d'intelligence artificielle par l'établissement d'exigences communes à l'échelle du Canada pour la conception, le développement et l'utilisation de ces systèmes;

- d'interdire certaines conduites relativement aux systèmes d'intelligence artificielle qui peuvent causer un préjudice sérieux aux individus ou un préjudice à leurs intérêts.

M^me^ Laidlaw a dit que dans sa forme actuelle, la LIAD n'est pas suffisamment étoffée pour nous permettre de faire face aux problèmes liés à l'IA. Selon elle, elle devrait être

111 ETHI, *Témoignages*, Laidlaw.

112 ETHI, *Témoignages*, Laidlaw; Australia, eSafety Commissioner, eSafetyeducation [DISPONIBLE EN ANGLAIS SEULEMENT].

retirée du projet de loi pour permettre une discussion réfléchie sur les façons d'utiliser l'IA qui peuvent perturber fondamentalement la démocratie, miner notre capacité de prendre des décisions et créer des risques physiques pour nous, individuellement ou collectivement.

M. Malone, a de son côté critiqué le fait que le la LIAD ne s'applique pas au gouvernement et qu'elle tombe sous la responsabilité d'un commissaire qui n'est pas entièrement indépendant d'ISDE, dont le mandat est de faire croître l'économie.

De façon plus générale, M. Gruzd a expliqué qu'en raison de l'évolution de l'IA générative, il faudra trouver des outils permettant aux utilisateurs de détecter ce qui est réel et authentique sur les plateformes, par exemple à l'aide d'une certification numérique ou en exigeant que les créateurs de contenus divulguent si des outils d'IA générative ont été utilisés pour produire du contenu[113]. Il a aussi soulevé le besoin de savoir si des données canadiennes ont été utilisées pour entraîner des applications d'IA générative et si le contenu est généré par l'IA ou non. Par exemple, il a fait remarquer que les utilisateurs canadiens fournissent des renseignements personnels à des sites offrant des outils d'IA générative comme ChatGPT, sans se rendre compte qu'ils consentent à ce que ces renseignements soient utilisés pour l'entraînement futur de l'application.

M. Gruzd a rappelé que l'apprentissage automatique dans le domaine de l'IA est aussi très utilisé pour « mettre du contenu devant des yeux ». C'est cela qui mène parfois un individu à se retrouver dans une chambre d'écho qui pourrait être remplie de mésinformation pilotée par un système de recommandations. Selon lui, tout emploi non réglementé de l'IA risque de donner lieu à de futurs abus.

M. Gruzd a aussi soulevé une inquiétude à l'égard de l'utilisation de l'IA pour déceler des contenus préjudiciables en ligne. Il a noté, par exemple, que selon les rapports de transparence de Meta, l'entreprise supprime automatiquement 65 % du contenu classé comme du harcèlement ou de l'intimidation. Pour les 35 % restant, il faut qu'un utilisateur ait signalé le contenu problématique pour que les plateformes agissent.

Dans sa réponse écrite, la GRC a avancé que, du point de vue de l'application de la loi, l'IA pourrait constituer une nouvelle voie pour les outils d'enquête, surtout dans le cadre d'enquêtes complexes et riches en données[114]. La GRC a écrit qu'elle

113 ETHI, *Témoignages*, Gruzd.

114 Gendarmerie royale du Canada, *Réponse écrite soumise au Comité ETHI*, p. 2 [HYPERLIEN NON DISPONIBLE]. Voir aussi : ETHI, *Témoignages*, Brigitte Gauvin (commissaire adjointe par intérim, Police fédérale, Sécurité nationale, Gendarmerie Royale du Canada).

> évalue l'utilisation de l'IA comme outil d'enquête pour les organismes d'application de la loi afin d'élargir et de soutenir les tactiques d'enquêtes policières traditionnelles et de veiller à ce qu'elle soit utilisée de façon responsable, transparente et légale. L'utilisation de l'IA comporte toutefois des risques, notamment celui d'introduire ou d'exacerber des préjugés. C'est pourquoi la GRC reconnaît la nécessité d'élaborer des politiques, des procédures et de la formation pour guider l'adoption et l'utilisation de la technologie de l'IA dans un environnement d'application de la loi afin de s'assurer que son utilisation répond à toutes les préoccupations juridiques et de protection des renseignements personnels[115].

Concernant la possibilité de mettre en place un registre national de toutes les applications d'IA ou de leur utilisation par les plateformes de médias sociaux, M. Larkin s'est montré ouvert à ce qu'il y ait un débat sur la question, sans se prononcer sur la validité d'un tel registre. Mme Luelo ne s'est pas prononcée sur un tel registre. Elle a cependant souligné qu'à l'interne, les directives données au gouvernement visent à assurer la transparence relative à l'utilisation de l'IA, y compris l'IA générative[116].

CHAPITRE 4 : PROMOUVOIR UN USAGE SÉCURITAIRE DES PLATEFORMES DE MÉDIAS SOCIAUX

Éducation et sensibilisation de la population canadienne

M. Dufresne a indiqué qu'il souhaite que le CPVP en fasse davantage sur le plan de l'éducation à l'égard des enjeux liés à la protection de la vie privée. Il a toutefois noté que l'éducation doit faire l'objet d'un effort collectif de la part du gouvernement, des écoles et des enseignants. Mme Polsky a elle aussi indiqué que l'éducation est importante. Elle a rappelé que peu de gens, même ceux qui ont des connaissances en matière de vie privée, comprennent l'étendue du partage de renseignements personnels qui peut se faire en ligne.

M. Khoury, pour sa part, a expliqué que le CST publie des lignes directrices par l'entremise de son CCC. Ces ressources peuvent aider la population canadienne à prendre des décisions éclairées concernant les services en ligne qu'elle utilise. Par exemple, le CCC recommande d'effectuer des recherches sur toute application ou plateforme qu'une personne compte utiliser afin de déterminer si elle provient d'une source de confiance et de lire les conditions générales d'utilisation. Il recommande aussi

115 *Ibid.*

116 Voir par exemple : Gouvernement du Canada, *Guide sur l'utilisation de l'intelligence artificielle générative*.

de découvrir où les données recueillies par une application sont stockées et quel impact cela pourrait avoir sur la protection des renseignements personnels[117].

M^me^ Henderson a abondé dans le même sens. Elle a noté qu'il est important pour tout citoyen canadien qui crée des comptes sur des réseaux sociaux de savoir où ce compte est créé. Elle a aussi exprimé la conviction qu'il est important d'éduquer les gens sur la bonne hygiène sur les médias sociaux. Selon elle, chaque personne doit être responsable de ce qu'elle partage et être au courant du coût et des conséquences de ses choix[118].

M^me^ Henderson a rajouté qu'avec l'avènement des médias sociaux et de la technologie, la population canadienne est exposée à des activités d'États hostiles qui veulent saper la souveraineté du Canada et de ses institutions démocratiques. Il est donc fondamentalement important de protéger la sécurité nationale, entre autres « en conscientisant et en éduquant les gens, afin de nous protéger et de protéger nos systèmes dans l'avenir ». Selon elle, pour protéger sa sécurité nationale, le Canada doit adopter une approche qui implique toute la société, des communautés affectées aux universitaires et à tous les ordres de gouvernement.

M^me^ Gauvin a elle aussi affirmé que l'éducation est utile pour contrer l'ingérence étrangère qui se fait sur les plateformes de médias sociaux. Les gens doivent être à l'affût du fait qu'ils peuvent être surveillés par des entités étrangères en ligne. C'est pourquoi la GRC a des « programmes d'engagement avec le public, les entités privées et les communautés plus vulnérables pour éduquer les gens à propos des différentes façons ou des divers mécanismes utilisés par les entités étrangères pour effectuer des activités d'ingérence ».

M. Larkin a expliqué que le Centre national de coordination contre la cybercriminalité de la GRC et le Centre antifraude collaborent à la campagne « Pensez cybersécurité » pour sensibiliser le public à la sécurité en ligne[119]. Cette campagne nationale vise à fournir de l'information à tous les Canadiens, y compris les jeunes, sur les cybermenaces et les mesures de prévention. La GRC produit également des bulletins opérationnels et des outils de signalement de crimes à l'intention des agents de police de première ligne, des partenaires stratégiques et du public. Le but de ces activités est d'accroître le nombre de signalements de crimes à l'échelle fédérale et de mobiliser les diverses communautés

117 ETHI, *Témoignages*, Khoury.

118 ETHI, *Témoignages*, Henderson.

119 Gouvernement du Canada, Pensez Cybersécurité.

culturelles. Le Centre national contre l'exploitation d'enfants fait de son côté des campagnes de sensibilisation axées sur la protection des personnes vulnérables[120].

M. Larkin a néanmoins reconnu qu'il est difficile pour la GRC de réagir à l'impact des médias sociaux. Cela fait en sorte qu'une grande partie du travail de la GRC est de nature réactive. Il a aussi rappelé que la GRC a des capacités limitées.

En effet, M. Malone a avancé et que les ressources disponibles de la GRC en matière de cybersécurité ne répondent pas à la demande et que son financement est insuffisant. Il a rappelé qu'en 2018, Sécurité publique a procédé à une mise à jour de la cybersécurité et a injecté de nouveaux fonds dans la GRC destinés à la lutte contre la cybercriminalité, annonçant la création du GNC3, le centre national de coordination contre la cybercriminalité. Il a noté que ce système de signalement a deux ans de retard et que le site Web est encore à l'étape des essais bêta et qu'il n'accepte que 25 plaintes concernant la cybercriminalité par jour pour l'ensemble du pays[121].

M. Malone a par ailleurs noté que le nombre de personnes qui travaillent pour les médias sociaux ou les communications du gouvernement est exponentiellement plus important que le nombre de ressources de la GRC consacrées à la lutte contre les préjudices en ligne. Par exemple, il a indiqué que l'équipe d'enquête sur la cybercriminalité de la GRC ne compte que huit employés pour l'ensemble de l'Alberta, quatre employés pour l'ensemble de la Colombie-Britannique et aucun employé en Saskatchewan, au Manitoba ou dans les provinces maritimes[122].

M. Gruzd, pour sa part, a rappelé que bien qu'enseigner la culture numérique aux utilisateurs est important, il est injuste de faire peser toutes les responsabilités sur ces derniers. Les plateformes de médias sociaux sont complexes et les algorithmes qui décident de ce que les utilisateurs voient ou ne voient pas restent opaques. Des stratégies qui obligent les entreprises à protéger les renseignements personnels de leurs utilisateurs dès la conception et par défaut devraient donc être élaborées. Il a ajouté qu'il peut être difficile de former chaque utilisateur et de modifier les comportements individuels, mais les plateformes, elles, peuvent intégrer des outils qui permettent aux utilisateurs de se protéger de façon plus efficace et efficiente.

120 ETHI, *Témoignages*, Larkin.

121 GRC, *Centre national de coordination en cybercriminalité (CNC3)*; GRC, *Nouveau système de signalement des incidents de cybercriminalité et de fraude*.

122 ETHI, *Témoignages*, Matt Malone (professeur adjoint de droit, Thompson Rivers University).

Éducation et sensibilisation des mineurs

M. Dufresne a exprimé le souhait qu'une formation soit obligatoire dans les écoles pour que les gens soient outillés tôt dans leur vie. M^me^ Polsky a elle aussi indiqué qu'il faudrait trouver un moyen d'inclure la littératie numérique dans le curriculum scolaire partout au Canada, reconnaissant toutefois que l'éducation tombe sous la compétence provinciale.

M. Gruzd, de son côté, a fait remarquer qu'il faut trouver des moyens intéressants d'éduquer les adolescents et les jeunes adultes, par exemple à l'aide de jeux où les participants doivent gérer une opération d'information en ligne, ce qui leur permet de devenir plus conscients de tout ce qui peut leur arriver dans leurs interactions en ligne.

M^me^ Henderson et M. Khoury ont aussi convenu qu'il faut éduquer toutes les personnes, y compris les jeunes. M. Khoury a par ailleurs souligné qu'il faut informer les jeunes et les moins jeunes des risques que publier certaines informations en ligne pose plus tard, une fois qu'une image un peu plus complète de l'individu a été formulée. M^me^ Polsky a donné l'exemple des questions posées en ligne par l'entremise de jeux-questionnaires amusants qui sont des moyens subtils de recueillir des renseignements personnels sur des individus, y compris leur profil psychologique et leurs préférences, pour utilisation future.

M. Larkin a reconnu que les jeunes sont particulièrement vulnérables à la cybercriminalité, car ils ont tendance à faire confiance à l'environnement numérique sans en comprendre pleinement les risques. « Leur utilisation intensive des plateformes de médias sociaux, conjugués à leur tendance à donner trop de renseignements personnels, en font des cibles particulièrement attrayantes pour les cybercriminels. » C'est pourquoi les Services nationaux à la jeunesse de la GRC communiquent avec les jeunes et les sensibilisent à la question de la sécurité en ligne, en collaboration avec des policiers éducateurs et divers organismes.

Considérant l'importance de l'éducation et de la sensibilisation de la population canadienne à la sécurité en ligne et du rôle de la GRC dans la lutte contre la cybercriminalité, le Comité fait les recommandations suivantes.

Recommandation 7

Que le gouvernement du Canada augmente le financement de la Gendarmerie royale du Canada pour qu'elle affecte davantage de ressources à l'éducation et à la lutte contre la cybercriminalité.

Recommandation 8

Que le gouvernement du Canada investisse davantage dans des efforts de littératie numérique afin que la population canadienne soit mieux outillée pour protéger ses renseignements personnels en ligne, reconnaître la désinformation et la mésinformation, et identifier les contenus préjudiciables en ligne.

CONCLUSION

Cette étude a permis au Comité de confirmer que le modèle d'affaires et les pratiques des plateformes de médias sociaux posent certains risques à la santé et à la sécurité de leurs utilisateurs – et même de la population en général – ainsi qu'à la sécurité nationale du Canada. L'atténuation de ces risques devrait entre autres passer par la modernisation de la législation fédérale en matière de protection des renseignements personnels pour qu'elle encadre les transferts de données et qu'elle tienne compte d'avancées technologiques comme l'intelligence artificielle, notamment.

Le projet de loi C-27 pourrait combler certaines des lacunes du régime législatif actuel identifiées par les témoins, mais la teneur de ses dispositions finales, si elles sont adoptées, n'est pas encore connue.

Le Comité est aussi particulièrement préoccupé par la santé et la sécurité des enfants qui utilisent les médias sociaux et estime qu'il est primordial qu'ils soient mieux protégés dans leurs activités en ligne. Le Comité, comme le commissaire à la protection de la vie privée l'a bien exprimé durant l'étude, est convaincu que les enfants ont le droit d'être des enfants, même dans le monde numérique.

Enfin, le Comité est convaincu que plus d'efforts doivent être consacrés à la littératie numérique de la population canadienne et que la capacité des forces de l'ordre de contrer la cybercriminalité et l'ingérence étrangère doit être accrue de manière significative. Comme le comité l'a déjà indiqué dans des études antérieures, l'autoréglementation des plateformes de médias sociaux est insuffisante pour assurer la santé et à la sécurité de leurs utilisateurs et de la population canadienne. Le Comité considère qu'un encadrement législatif des plateformes de médias sociaux plus robuste est plus que jamais nécessaire.

ANNEXE A :
LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la page Web du Comité sur cette étude.

Organismes et individus	Date	Réunion
TikTok	2023/10/18	85
Steve de Eyre, directeur, Politiques publiques et affaires gouvernementales, Canada		
David Lieber, chef, Politiques publiques en matière de vie privée pour les Amériques		
Commissariats à l'information et à la protection de la vie privée au Canada	2023/10/25	87
Philippe Dufresne, commissaire à la protection de la vie privée du Canada		
Michael Maguire, directeur, Loi sur la protection des renseignements personnels et les documents électroniques, Direction de la conformité		
Centre de la sécurité des télécommunications	2023/11/20	92
Sami Khoury, dirigeant principal, Centre canadien pour la cybersécurité		
Conseil du Canada de l'accès et la vie privée	2023/11/20	92
Sharon Polsky, présidente		
Service canadien du renseignement de sécurité	2023/11/20	92
Cherie Henderson, directrice adjointe, Exigences		
Peter Madou, directeur général, Évaluation des renseignements		
À titre personnel	2023/11/27	94
Anatoliy Gruzd, professeur et titulaire de la chaire de recherche du Canada sur les technologies numériques de protection des renseignements personnels, Toronto Metropolitan University		

Organismes et individus	Date	Réunion
Gendarmerie royale du Canada	2023/11/27	94
Brigitte Gauvin, commissaire adjointe par intérim, Police fédérale, Sécurité nationale		
Bryan Larkin, sous-commissaire, Services de police spécialisés		
Secrétariat du Conseil du Trésor	2023/11/27	94
Catherine Luelo, sous-ministre et dirigeante principale de l'information du Canada		
À titre personnel	2023/12/04	95
Brett Caraway, professeur agrégé de l'économie des médias, University of Toronto		
Emily Laidlaw, professeure agrégée et titulaire de la Chaire de recherche du Canada en droit de la cybersécurité, University of Calgary		
Matt Malone, professeur adjoint, Thompson Rivers University		
The Dais	2023/12/04	95
Sam Andrey, directeur général		
Joe Masoodi, analyste principal des politiques		
Google Canada	2023/12/13	97
Shane Huntley, directeur principal, Groupe d'analyse des menaces, Google		
Jeanette Patell, cheffe des affaires gouvernementales et des politiques publiques du Canada, Google et YouTube		
Meta Platforms Inc.	2023/12/13	97
Rachel Curran, cheffe des politiques publiques, Canada		
Nathaniel Gleicher, chef des politiques de sécurité		
Lindsay Hundley, responsable des politiques d'influence		
X Corporation	2023/12/13	97
Wifredo Fernández, chef des affaires gouvernementales, États-Unis et Canada		
Josh Harris, conseiller principal en matière de protection de la vie privée et des données		

ANNEXE B :
LISTE DES MÉMOIRES

Ce qui suit est une liste alphabétique des organisations et des personnes qui ont présenté au Comité des mémoires reliés au présent rapport. Pour obtenir de plus amples renseignements, veuillez consulter la page Web du Comité sur cette étude.

Conseil du Canada de l'accès et la vie privée

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des *procès-verbaux* pertinents (réunions nos 85, 87, 92, 94, 95, 97, 106 et 137) est déposé.

Respectueusement soumis,

Le président,
John Brassard