CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

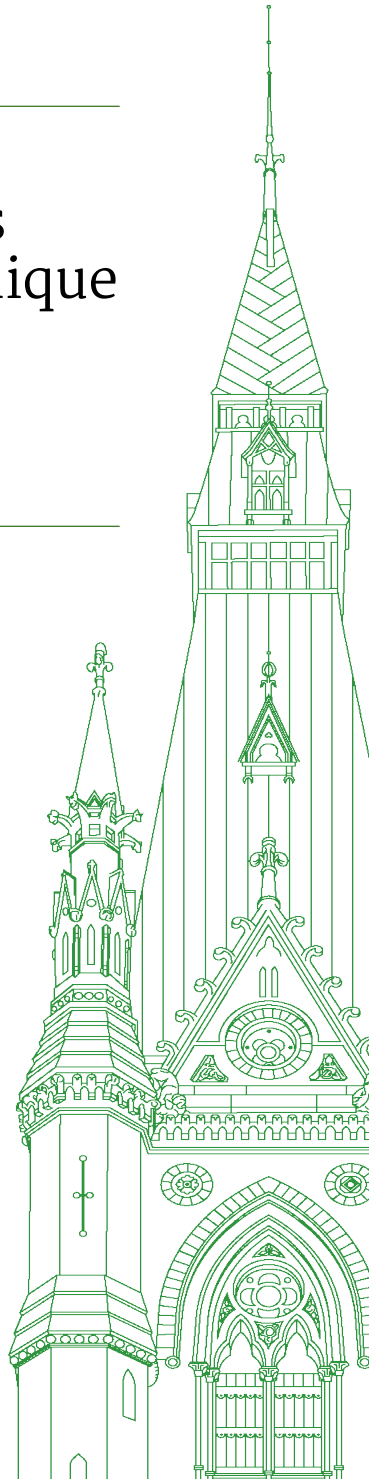
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 018

Le lundi 2 mai 2022



Président : M. Pat Kelly

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

Le lundi 2 mai 2022

● (1105)

[*Traduction*]

Le président (M. Pat Kelly (Calgary Rocky Ridge, PCC)): La séance est ouverte.

Bienvenue à la 18e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes. Conformément à l'article 10 (3)h) du Règlement et à la motion adoptée par le Comité le lundi 13 décembre 2021, le Comité reprend son étude sur l'utilisation et les impacts de la technologie de reconnaissance faciale.

La réunion d'aujourd'hui se déroule en mode hybride, conformément à l'ordre de la Chambre du 25 novembre 2021. Les députés y participent donc en personne dans la salle ou à distance par Zoom. Conformément à la directive du Bureau de régie interne du 10 mars 2022, toutes les personnes ici présentes doivent porter un masque, sauf les députés lorsqu'ils sont assis à leur place pendant les délibérations.

J'aimerais maintenant formuler quelques commentaires à l'intention des témoins et des députés. Tout d'abord, veuillez attendre que je vous nomme avant de prendre la parole. Les personnes qui participent à la séance par vidéoconférence sont priées de cliquer sur l'icône du microphone pour activer leur micro et de le mettre en sourdine lorsqu'elles ne s'expriment pas.

En ce qui concerne l'interprétation, sachez que si vous participez à la séance par Zoom, vous pouvez sélectionner au bas de votre écran l'audio du parquet, l'audio anglais ou l'audio français. Si vous êtes présents dans la salle, veuillez utiliser votre écouteur et sélectionnez le canal souhaité comme vous le feriez normalement.

J'aimerais maintenant souhaiter la bienvenue à nos témoins. Nous accueillons des représentants du Commissariat à la protection de la vie privée du Canada, à savoir Daniel Therrien, commissaire à la protection de la vie privée du Canada, et David Weinkauf, analyste principal de recherche en technologie de l'information.

Nous recevons également des représentants du Commissariat à l'information et à la protection de la vie privée de l'Ontario, à savoir Patricia Kosseim, commissaire, et Vance Lockton, conseiller principal en technologie et politique.

Enfin, nous accueillons la présidente de la Commission d'accès à l'information du Québec, Diane Poitras.

Nous allons maintenant entendre notre premier témoin. Chaque témoin peut faire une déclaration préliminaire d'une durée maximale de cinq minutes.

Commissaire Therrien, la parole est à vous.

[*Français*]

M. Daniel Therrien (commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée du Canada): Bonjour, monsieur le président.

Je vous remercie tous de m'avoir invité aujourd'hui. Je vous félicite d'avoir entrepris cet important travail dans le dossier de la reconnaissance faciale.

Comme c'est le cas de toutes les technologies, la reconnaissance faciale peut, si elle est utilisée de manière responsable, offrir d'importants avantages à la société. Cependant, elle peut aussi s'avérer extrêmement envahissante, permettre la surveillance à grande échelle, produire des résultats tendancieux et miner les droits de la personne, y compris le droit de participer librement, sans surveillance, à la vie démocratique. Elle se distingue des autres technologies dans la mesure où elle s'appuie sur la biométrie, c'est-à-dire sur des caractéristiques permanentes qui, contrairement à un mot de passe, ne peuvent être modifiées. Elle réduit considérablement l'autonomie personnelle, y compris le contrôle que chacun devrait exercer sur ses renseignements personnels. Son utilisation couvre les secteurs publics et privés, parfois pour des raisons importantes, comme lors d'enquêtes portant sur des crimes graves, ou pour prouver l'identité de quelqu'un, parfois pour des raisons de simple commodité.

La portée de votre étude est vaste. Dans le temps qui est à ma disposition, je mettrai l'accent sur l'utilisation de la technologie de reconnaissance faciale dans un contexte policier. Lors de ma dernière comparution devant vous au sujet de votre présente étude, le Commissariat avait terminé son enquête sur Clearview AI, une plateforme du secteur privé qui, selon nous et nos collègues du Québec, de la Colombie-Britannique et de l'Alberta, effectuait de la surveillance de masse.

Depuis, le Commissariat a examiné l'usage qu'avait fait la GRC de la technologie de Clearview AI. Nous en sommes venus à la conclusion que la GRC n'avait pas pris de mesures pour vérifier la légalité de la collecte de renseignements par Clearview AI et, en fait, qu'elle ne disposait d'aucun système lui permettant de s'assurer que les nouvelles technologies utilisées par l'entreprise sont conformes à la loi. Au bout du compte, nous avons déterminé que l'usage que faisait la GRC de la technologie de Clearview AI était illégal, puisqu'il reposait sur la collecte et l'utilisation illégale d'images faciales par son partenaire commercial.

[*Traduction*]

Forts de ces constatations, nous avons travaillé de concert avec nos homologues chargés de la protection de la vie privée de l'ensemble du Canada en vue d'élaborer des orientations conjointes sur l'utilisation de la reconnaissance faciale par les corps policiers. Ce document a pour objectif d'aider les services de police à s'assurer que toute utilisation de la technologie de reconnaissance faciale est conforme à la loi, limite les risques d'atteinte à la vie privée et respecte le droit à la vie privée. Nous publions la version finale de ce document aujourd'hui.

Dans le cadre de ce travail, nous avons lancé une consultation publique nationale portant sur l'utilisation de la technologie de la reconnaissance faciale par les services de police. Durant cette consultation, nous avons régulièrement entendu dire que les lois actuelles qui réglementent l'utilisation de la reconnaissance faciale n'offrent pas une protection suffisante contre les risques liés à la technologie. Même si tous les intervenants ont convenu que la loi devait être clarifiée, aucun consensus n'a été établi relativement à la teneur de nouvelles dispositions législatives. Il reviendra aux législateurs de décider comment concilier divers intérêts.

Au terme de cette consultation, mes collègues des provinces et territoires et moi-même sommes d'avis que l'approche à privilégier serait d'adopter un cadre législatif fondé sur quatre éléments clés, que nous avons décrit dans une déclaration commune que nous rendons publique aujourd'hui.

Nous recommandons en premier lieu que la loi définisse clairement et de manière explicite les fins pour lesquelles les services de police seraient autorisés à faire usage de la technologie de reconnaissance faciale, en plus d'interdire tout autre usage. Les fins autorisées devraient être impérieuses et proportionnelles aux risques très élevés que présente la technologie.

En deuxième lieu, puisqu'il n'est pas réaliste de penser que la loi puisse prévoir toutes les situations possibles, il importe qu'en plus de prévoir des restrictions concernant les fins autorisées, la loi exige aussi que l'utilisation de la reconnaissance faciale par les services de police soit à la fois nécessaire et proportionnelle pour tout déploiement donné de la technologie.

En troisième lieu, nous recommandons que l'usage de la reconnaissance faciale par les services de police fasse l'objet d'une surveillance indépendante rigoureuse. Cette surveillance devrait inclure des mesures de mobilisation préventive, comme des évaluations des facteurs relatifs à la vie privée, ou EFVP, des autorisations préalables au niveau des programmes, des préavis avant l'utilisation de la technologie ou le pouvoir de réaliser des vérifications et de rendre des ordonnances.

Enfin, nous recommandons que des mesures de protection de la vie privée appropriées soient mises en place afin d'atténuer les risques pour les personnes, y compris des mesures relatives à l'exactitude, à la conservation et à la transparence dans le cadre des projets d'utilisation de la reconnaissance faciale.

Je vous invite à tenir compte de nos recommandations pendant la mise au point de votre étude sur cet enjeu important.

● (1110)

[*Français*]

Je vous remercie de m'avoir donné l'occasion de témoigner devant vous.

Je répondrai volontiers à vos questions après les déclarations de mes collègues.

[*Traduction*]

Le président: Merci.

Nous allons maintenant entendre la commissaire Kosseim pendant cinq minutes ou moins.

[*Français*]

Me Patricia Kosseim (commissaire, Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario): Bonjour.

Je vous remercie de m'avoir invitée à prendre la parole aujourd'hui.

Je suis accompagnée de M. Vance Lockton, conseiller principal en technologie et politiques de mon bureau.

J'aimerais m'appuyer sur ce que vous venez d'entendre de la part du commissaire Therrien. Bien que tous les commissaires à la protection de la vie privée du Canada recommandent l'adoption d'un cadre législatif sur l'utilisation de la reconnaissance faciale dans le domaine de l'application de la loi, nous reconnaissons également que certains services de police utilisent déjà cette technologie ou envisagent de le faire. C'est pourquoi nous publions, aujourd'hui, un document d'orientation pour les services de police dans le but de minimiser les risques en attendant la mise en place d'un cadre législatif, tel que l'a décrit mon collègue, M. Therrien.

J'aimerais souligner cinq éléments clés de ce document d'orientation.

Premièrement, avant de recourir à la reconnaissance faciale à quelque fin que ce soit, les services de police doivent établir que la loi les autorise à le faire. Cela n'est pas acquis et ne peut pas être présumé. La reconnaissance faciale nécessite de recourir à des données biométriques délicates. La police doit donc consulter ses conseillers juridiques pour confirmer qu'elle dispose d'une autorité légale en vertu de la common law ou d'une loi particulière en vigueur sur son territoire de compétence. Elle doit aussi s'assurer que la Charte canadienne des droits et libertés est respectée et que l'utilisation de la reconnaissance faciale est nécessaire et pertinente, compte tenu des circonstances.

[*Traduction*]

Deuxièmement, les services de police doivent établir des mesures rigoureuses en matière de responsabilité. Ainsi, ils doivent intégrer des mesures de protection de la vie privée à toutes les étapes d'un projet de reconnaissance faciale et mener une évaluation des facteurs relatifs à la vie privée, ou une EFVP, afin de déterminer les risques et de les atténuer avant la mise en œuvre.

Ils doivent aussi mettre en place un programme solide de gestion de la protection de la vie privée, assorti de politiques et de procédures clairement documentées visant à limiter les fins de la reconnaissance faciale, de systèmes rigoureux de consignation de toutes les utilisations et divulgations connexes, et de titulaires de poste clairement responsables de la surveillance et de la conformité.

Un tel programme doit être examiné chaque année pour en garantir l'efficacité; il doit prévoir une formation appropriée et veiller à ce que les tiers fournisseurs de services respectent toutes leurs obligations en matière de protection de la vie privée.

Troisièmement, les services de police doivent garantir la qualité et l'exactitude des renseignements personnels utilisés par le système de RF, afin de prévenir les faux positifs, de réduire les risques de préjugés et d'éviter de causer des préjudices à des particuliers, des groupes ou des communautés. Pour assurer cette exactitude, il faut mener des essais internes et externes du système de RF afin de déterminer s'il a un effet discriminatoire et de prévoir une intervention humaine pour atténuer les risques associés aux décisions automatisées qui pourraient avoir une incidence importante sur les droits des personnes.

Quatrièmement, les services de police ne devraient pas conserver de renseignements personnels plus longtemps que nécessaire. Il faut donc détruire les images qui ne permettent pas d'établir de correspondance, et supprimer de la base de données les empreintes faciales dès que les critères de conservation ne sont plus respectés.

Cinquièmement, les services de police doivent s'occuper des questions de transparence et de communication avec le public. Dans le contexte d'enquêtes policières, il n'est pas toujours possible d'avertir directement le public chaque fois que la reconnaissance faciale est utilisée. Cependant, il est possible pour un service de police de faire preuve de transparence au niveau des programmes, par exemple, en publiant ses politiques officielles sur le recours à la RF, en décrivant en termes simples son programme de RF et en fournissant un résumé de son évaluation des facteurs relatifs à la vie privée.

Toutefois, la communication avec le public ne doit pas être à sens unique — les principaux intervenants et, en particulier, les représentants des groupes faisant l'objet d'une surveillance policière excessive doivent être consultés au cours de la conception même du programme de reconnaissance faciale. Compte tenu de l'importance de la réconciliation au Canada, cette consultation doit inclure la participation des communautés et des groupes autochtones.

Ce ne sont là que quelques-unes des mesures décrites dans le document d'orientation.

Nous croyons que ce document contient des mesures importantes d'atténuation des risques, mais je répète que notre principale recommandation porte sur l'établissement éventuel d'un cadre législatif complet pour régir l'utilisation de la RF par les services de police canadiens. Il faut établir des balises claires ayant force de loi pour que les services de police puissent faire un usage approprié de la technologie de RF, dans un cadre transparent susceptible de mériter la confiance durable du public.

Merci.

[*Français*]

Le président: Je vous remercie.

La présidente de la Commission d'accès à l'information du Québec, M^{e} Diane Poitras, a maintenant la parole pour cinq minutes.

● (1115)

Me Diane Poitras (présidente, Commission d'accès à l'information du Québec): Merci, monsieur le président.

Bonjour, je vous remercie de cette invitation à échanger au sujet de la reconnaissance faciale.

En complément des propos de mes collègues, j'aimerais aborder brièvement les problèmes soulevés par d'autres utilisations de cette technologie et présenter ce que prévoit la législation québécoise. Comme l'ont mentionné plusieurs intervenants, l'utilisation de plus en plus répandue de la reconnaissance faciale dans différents contextes soulève des problèmes importants, notamment en ce qui a trait au respect de la vie privée.

Cette technologie qui allie biométrie et intelligence artificielle, notamment, est particulièrement invasive, entre autres parce qu'elle collecte et utilise des caractéristiques uniques du corps pour les transformer en données. Ces caractéristiques, comme certains traits de notre visage, sont au cœur de notre identité. Le fait que cette technologie puisse être utilisée à notre insu augmente la perte de contrôle sur nos renseignements et les risques de surveillance indue. Certaines utilisations proposées pour la reconnaissance faciale et ses dérivés infèrent des caractéristiques intimes à partir du visage ou de nos expressions faciales, comme l'âge, le sexe, l'origine ethnique, nos émotions, notre niveau d'attention, de fatigue ou de stress, des renseignements de santé ou certains traits de notre personnalité. Ces caractéristiques peuvent servir à catégoriser, détecter ou profiler des individus, et ce, à des fins commerciales, pour effectuer une certaine forme de surveillance ou encore pour prendre des décisions à leur sujet.

La création de banques de renseignements biométriques pose aussi des risques importants pour la vie privée. Il est difficile pour une personne dont les données biométriques ont été compromises de contester une transaction ou une action en cas d'erreur ou de fraude à l'identité compte tenu de la grande fiabilité qu'on accorde à ces renseignements uniques et permanents. Puisqu'il est quasi impossible de remplacer une donnée biométrique compromise, il peut être tout aussi complexe de rétablir son identité.

Soulignons aussi les risques élevés que ces banques biométriques créées dans un but précis soient utilisées à d'autres fins à notre insu et sans une évaluation adéquate des problèmes et des risques de cette nouvelle utilisation. C'est pourquoi la création de telles banques et le recours à la biométrie à des fins d'identification sont encadrés au Québec par la Loi concernant le cadre juridique des technologies de l'information et par les lois protégeant les renseignements personnels applicables aux organisations publiques et privées. Ainsi, la création de toute banque biométrique doit être déclarée à la Commission. À compter de septembre prochain, cela sera le cas de toute utilisation de la biométrie à des fins d'identification.

Au Québec, on ne peut recourir à la biométrie à des fins d'identification sans le consentement exprès de la personne concernée. Aucune caractéristique biométrique ne peut être saisie à son insu. Seul le minimum de caractéristiques biométriques peut être recueilli et utilisé. Tout autre renseignement qui pourrait être découvert à partir de ces caractéristiques ne peut être ni utilisé ni conservé. Enfin, les renseignements biométriques et toute note les concernant doivent être détruits lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli. La Commission a de larges pouvoirs et peut rendre toute ordonnance concernant de telles banques, incluant les pouvoirs de suspendre ou d'interdire leur mise en service ou d'ordonner leur destruction. En plus de ces dispositions précises, les règles générales relatives à la protection des renseignements personnels s'appliquent. Cela implique, entre autres, que le recours à la reconnaissance faciale soit nécessaire et proportionnel à l'objectif poursuivi.

Nous constatons que les organisations n'accordent malheureusement pas toute l'importance qu'elles devraient à cette évaluation de conformité et aux problèmes liés à l'utilisation de la reconnaissance faciale. La popularité de la biométrie engendre une certaine banalisation de ses implications sur les citoyens. C'est pourquoi la Commission recommande qu'une évaluation des facteurs relatifs à la vie privée soit obligatoirement réalisée au préalable. Une telle évaluation sera d'ailleurs obligatoire à compter de septembre 2023. De plus, les renseignements biométriques seront expressément désignés comme des renseignements personnels sensibles. Bien que l'encadrement actuel de la biométrie au Québec permette à la Commission d'avoir un certain portrait de l'utilisation de la reconnaissance faciale et qu'il lui accorde des pouvoirs d'intervention, nous avons demandé qu'il soit bonifié pour tenir compte de l'évolution de cette technologie et des différents contextes de son utilisation.

Je vous remercie de votre attention. Je me ferai un plaisir d'échanger avec vous au cours des prochaines minutes.

● (1120)

[*Traduction*]

Le président: Cela dit, nous allons passer directement aux séries de questions.

Monsieur Kurek, vous avez la parole pendant un intervalle maximal de six minutes.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup.

Je me réjouis de la présence et des compétences de tous les commissaires qui participent à la séance d'aujourd'hui.

Je signale à tous les témoins que j'espère que nous serons en mesure d'obtenir une copie de la déclaration commune mentionnée afin qu'elle puisse être intégrée aux témoignages. Pourriez-vous simplement confirmer que cela est possible? Merci beaucoup.

Commissaire Therrien, au cours des dernières réunions consacrées à l'étude qui nous occupe, nous avons appris et entendu beaucoup de choses à propos de certains des défis associés à la technologie de reconnaissance faciale. Vous avez fait allusion aux consultations qui ont été menées. Pourriez-vous expliquer au Comité la nature de ces consultations en ce qui concerne la technologie de reconnaissance faciale et son utilisation, énumérer certains des intervenants qui ont participé à ces consultations et décrire certaines des tendances que vous avez pu remarquer au cours de ce processus?

M. Daniel Therrien: Bien sûr.

Lorsque nous avons publié notre rapport d'enquête sur l'utilisation de Clearview par la GRC en juin dernier dans un rapport spécial au Parlement, nous avons lancé en même temps une consultation auprès des intervenants qui souhaitaient parler du projet de directives que nous avions publié au même moment. Une trentaine de groupes ou de personnes nous ont écrit, et nous avons également tenu des réunions avec un certain nombre d'intervenants.

Les intervenants représentaient la société civile, les groupes minoritaires et la police elle-même. J'ai rencontré à plusieurs reprises la GRC et l'Association canadienne des chefs de police, et mes collègues ont également rencontré les équivalents provinciaux. Un large éventail de personnes a été consulté. Les points de vue étaient variés, évidemment, parce que les intérêts étaient différents, mais tous étaient d'accord pour dire que, dans sa forme actuelle, la loi est insuffisante. Selon leurs intérêts, les divers intervenants ne s'entendaient pas nécessairement sur le contenu de cette loi.

M. Damien Kurek: Bien sûr, et dans votre déclaration préliminaire, vous avez indiqué qu'il n'y avait pas de consensus clair entre les intervenants, et c'est certainement le sentiment que j'ai remarqué en entendant les différents témoins. Nous avons entendu la GRC dire très clairement qu'elle n'approuvait les conclusions de votre bureau en ce qui concerne son utilisation de Clearview AI.

Je suis curieux de savoir si vous pouvez faire part au Comité de certaines de vos observations sur les tendances que vous avez remarquées en consultant la grande variété de groupes avec lesquels vous avez dialogué dans le cadre de ce processus.

M. Daniel Therrien: Je commencerai par parler des cas où les gens sont tombés d'accord sans parler de la nécessité de modifier la loi.

De nombreuses personnes estimaient que les orientations avaient été rédigées ou élaborées avec un certain degré de généralité afin que les conseils soient utiles, mais elles souhaiteraient que les orientations soient au moins complétées par des conseils sur ce qui a été qualifié de « cas d'utilisation ». Notre réaction à cela est qu'il est effectivement nécessaire de fournir des conseils sur des utilisations particulières dans des contextes différents, car le contexte a une grande importance, mais nous pensons toujours qu'il est important et pertinent de disposer de conseils généraux qui peuvent être complétés à mesure que des cas d'utilisation sont définis.

Certains intervenants appartenant à la société civile ou à des groupes minoritaires ont demandé un moratoire sur l'utilisation de la reconnaissance faciale. La GRC n'approuvait évidemment pas cette idée. Notre position, en tant que commissaires, est que des lois claires devraient prescrire quand la reconnaissance faciale peut être utilisée, car elle peut être utilisée à des fins légitimes et utiles, ainsi que pour le bien de la société dans certaines circonstances — par exemple, dans des cas de crime grave ou pour retrouver des enfants disparus —, mais ces utilisations devraient être définies de manière assez étroite. La loi devrait également prescrire les utilisations interdites, ce qui serait, je suppose, une interdiction partielle ou un moratoire partiel sur l'utilisation de la reconnaissance faciale.

Si vous le permettez, je préciserai qu'en ce qui concerne la question du moratoire, nous ne pouvons pas, en tant qu'autorités de protection des données, imposer un moratoire ayant force de loi. Pour qu'un moratoire soit contraignant pour les services de police, il faudrait qu'il prenne la forme d'une loi.

J'ai été frappé par le témoignage que vous avez entendu la semaine dernière de la part d'un représentant de la GRC, à savoir que « La GRC croit que l'utilisation de la reconnaissance faciale doit être ciblée, limitée dans le temps et assujettie à des vérifications effectuées par des experts formés. »

● (1125)

M. Damien Kurek: Je vais poser une question maintenant, car mon temps est limité. Pourriez-vous fournir au Comité une liste des pratiques exemplaires qui ont cours dans d'autres pays où des cadres sont déjà en place, afin que nous puissions les consulter?

M. Daniel Therrien: Oui, bien sûr.

M. Damien Kurek: Je suis désolé; mon temps est essentiellement écoulé.

Je remercie tous les témoins de leur présence et de leur expertise.

Le président: Monsieur Fergus, allez-y. Vous avez six minutes.

[*Français*]

L'hon. Greg Fergus (Hull—Aylmer, Lib.): Merci beaucoup, monsieur le président.

Je remercie également M. Therrien, Mme Kosseim et Mme Poitras de leurs témoignages aujourd'hui.

Je vais d'abord m'adresser à M. Therrien. Ensuite, je m'adresserai aux deux autres témoins.

Monsieur Therrien, je sais que vous avez déposé un rapport concernant l'utilisation de la reconnaissance faciale par la GRC, et je vous en remercie. J'ai trouvé cela très intéressant et très utile. Cela dit, j'aimerais prendre un peu de recul afin de pouvoir appliquer cela à tout le monde, non seulement aux gouvernements, mais aussi au secteur privé, comme la loi du Québec tente de le faire.

Croyez-vous que les conseils que vous avez donnés à la GRC relativement à l'utilisation de la reconnaissance faciale s'appliqueraient de manière générale au secteur privé?

M. Daniel Therrien: Selon moi, l'élément commun qui s'applique de façon horizontale à tous les acteurs qui souhaitent utiliser la reconnaissance faciale est le principe de la nécessité et de la proportionnalité dont mes deux collègues ont parlé. Cela s'applique à tous les acteurs, qu'il s'agisse de services policiers, d'autres ministères et gouvernements ou d'entreprises.

Cela dit, dans le domaine des services policiers, recourir à la reconnaissance faciale peut avoir des conséquences extrêmement graves et même à la perte de liberté. Je dirais que beaucoup de principes communs devraient être pris en compte. Tous les acteurs, y compris les législateurs, devaient tenir compte du contexte et des conséquences que comporte le recours à cette technologie. Par exemple, l'interdiction totale d'y avoir recours dans certaines circonstances pour les corps policiers ne s'appliquerait pas nécessairement à tous les acteurs.

L'hon. Greg Fergus: Je conviens avec vous que l'utilisation de la reconnaissance faciale par les services policiers peut comporter de sérieux enjeux.

Nous avons accueilli quelques témoins de l'Université de Princeton, aux États-Unis. Ils ont fait valoir que les gouvernements jouent un rôle prépondérant dans le recours à cette technologie, mais que les entreprises privées jouent également un rôle. Par exemple, si l'on utilise cette technologie pour déterminer quel genre de risque un citoyen représente en matière de crédit, cela peut avoir de graves conséquences. Le recours à cette technologie est fondé sur une théorie qui ne contient pas suffisamment de données probantes pour justifier son utilisation.

Madame Kosseim, je vous remercie beaucoup d'avoir nommé les cinq éléments clés du document d'orientation. Pensez-vous qu'ils peuvent aussi s'appliquer au secteur privé?

Me Patricia Kosseim: Je vous remercie de votre question.

Comme mon collègue l'a dit, il est certain que les principes devraient s'appliquer, peu importe le secteur, en tenant compte évidemment du contexte et de l'éventail des risques en jeu. Je précise que l'Ontario ne possède pas de loi sur la protection des renseignements personnels qui s'appliquent au secteur privé. Toutefois, mon bureau est fortement d'accord sur l'idée proposée par le gouvernement d'en adopter une un jour.

En matière de protection des renseignements personnels, la plupart des entreprises sont assujetties aux lois fédérales. Or, cela laisse beaucoup de lacunes en Ontario. Dans beaucoup de secteurs, aucune loi ne protège les renseignements personnels des employés d'une grande majorité d'entreprises. Il s'agit donc d'une grande lacune. Je crois qu'il est important que les principes de base que nous mettons de l'avant dans nos lignes directrices s'appliquent et que nous procédions aux adaptations nécessaires pour les autres contextes. Nos lignes directrices sont précisément conçues pour le secteur de l'application de la loi et des services policiers.

● (1130)

L'hon. Greg Fergus: Merci.

Madame Poitras, j'applaudis à votre projet de loi, qui oblige les entreprises à se soumettre aux directives prévues par la loi d'ici 2023.

Je sais que je vous place dans une situation un peu inconfortable en vous posant cette question, mais pouvons-nous en faire plus, au Québec ou au gouvernement fédéral, pour protéger les citoyens des déboires de la technologie de reconnaissance faciale?

Le gouvernement fédéral devrait-il adopter une loi semblable à celle qui existe au Québec?

Me Diane Poitras: Je vous remercie de votre question.

Il est certain que la loi du Québec représente un début, mais nous avons déjà fait aux parlementaires québécois certaines recommandations pour l'améliorer. Par exemple, pour l'instant, le cadre n'impose des obligations que lorsque le recours à la biométrie, dont la reconnaissance faciale, sert à vérifier l'identité. Or, d'après les déclarations des banques biométriques que nous recevons, cette technologie sert aussi à d'autres fins. J'en ai fait état dans ma présentation. Par conséquent, une première recommandation consisterait à s'assurer...

Le président: Je suis désolé.

L'hon. Greg Fergus: Monsieur le président, pouvez-vous demander aux témoins, s'ils ont des choses à ajouter sur cette question, qu'ils en fassent part par écrit au Comité?

Le président: D'accord.

[*Traduction*]

Monsieur Fergus, vous ne lui avez pas laissé beaucoup de temps pour répondre à votre question. Je suis désolé, mais nous devons poursuivre.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

M. René Villemure (Trois-Rivières, BQ): Je vous remercie, monsieur le président.

Je remercie tous les commissaires de leur présence aujourd'hui.

Je les félicite d'avoir publié le cadre d'orientation, un document attendu de notre part.

Monsieur Therrien, comment définiriez-vous en quelques mots ce qu'est la surveillance?

M. Daniel Therrien: Quand la surveillance est faite par des corps policiers ou des compagnies privées, il s'agit d'une collecte de renseignements au sujet d'activités ou de caractéristiques d'individus effectuée en vue de prendre certaines décisions à leur sujet.

La question est de savoir si cela se fait avec le consentement des gens ou en vertu de lois qui protègent l'exercice par les citoyens des droits qui sont observés. C'est la clé, à mon avis. Les consommateurs face aux compagnies et les citoyens face à l'État devraient pouvoir exercer leur droit de consulter les médias sociaux, de communiquer et de faire des démonstrations, et ce, sans faire l'objet d'une surveillance massive, sauf à des fins extrêmement limitées.

M. René Villemure: Merci beaucoup.

Dans le même ordre d'idées, on nous a dit, au sujet des policiers qui filmaient les manifestants, que c'était pour les archives. Il reste que c'est une forme de surveillance.

M. Daniel Therrien: Oui.

● (1135)

M. René Villemure: D'accord.

Vous étiez sur une lancée, tantôt, lorsque vous parliez de la GRC. Ayant entendu les témoignages de personnes qui ont comparu la semaine dernière, j'aimerais que vous reveniez sur ce sujet.

M. Daniel Therrien: À quelques reprises, on vous a parlé d'un moratoire, souhaitable ou non, qui serait appliqué en attendant qu'une loi bonifiée soit adoptée. Il est clair, selon moi, qu'un moratoire pouvant lier les corps de police doit prendre la forme d'une loi. Cela dit, j'ai trouvé intéressant que le représentant de la GRC, la semaine dernière, évoque certains principes quant à l'utilisation de la reconnaissance faciale par la GRC. C'est la version anglaise que j'ai ici.

[*Traduction*]

Il a dit qu'elle doit être « ciblée, limitée dans le temps et assujettie à des vérifications effectuées par des experts formés. De plus, [elle] ne doit pas servir à confirmer l'identité, mais plutôt être considérée comme un outil d'enquête. »

[*Français*]

La question de la revue par un individu a été évoquée.

Vous pourriez demander à la GRC de s'engager à n'utiliser la reconnaissance faciale qu'en vertu des principes énoncés par son représentant la semaine dernière. Ce serait, selon moi, la meilleure façon d'arriver à un moratoire en attendant que la loi soit bonifiée.

M. René Villemure: Les principes étaient quand même valables.

M. Daniel Therrien: Oui.

M. René Villemure: D'accord.

Merci beaucoup, monsieur Therrien.

Madame Poitras, pourriez-vous nous résumer en quelques mots la situation reliée à Clearview Al, qui a quand même été très importante dans le cadre de vos travaux, au Québec?

Me Diane Poitras: Je vous remercie de votre question.

Comme vous le savez, la Commission d'accès à l'information du Québec a participé à l'enquête conjointe, avec ses homologues du gouvernement fédéral, de l'Alberta et de la Colombie-Britannique. Par la suite, nous avons rendu une ordonnance en vertu de nos propres pouvoirs provinciaux. Notre décision a été portée en appel, comme il est possible de le faire au Québec, et elle est présentement devant les tribunaux.

Nous nous ferons un plaisir de vous faire parvenir la décision que nous avons rendue, qui explique notre position et qui se trouve sur notre site Internet. Malheureusement, comme l'affaire est devant les tribunaux, je m'abstiendrai de tout commentaire par respect pour le processus judiciaire.

M. René Villemure: Je vous remercie de nous envoyer le document.

Je ne vous demanderai pas de nous révéler de l'information secrète, mais êtes-vous en mesure de nous dire ce que Clearview AI conteste?

Me Diane Poitras: Pour résumer l'ensemble de la décision, il y a d'abord la compétence de la Commission de rendre cette ordonnance, puisqu'il s'agit d'une entreprise américaine, mais aussi toutes nos conclusions, en droit, sur le respect de la loi québécoise.

M. René Villemure: Merci beaucoup.

Monsieur Therrien, selon vous, la GRC exerce-t-elle déjà de la surveillance?

M. Daniel Therrien: Je vais revenir à ce que j'ai entendu la semaine dernière. La GRC dit ne pas faire de surveillance de masse. Or je n'ai pas de raison de mettre en doute cette déclaration. La GRC pourrait démontrer qu'elle utilise la reconnaissance faciale pour des motifs impérieux en s'engageant à ne l'utiliser qu'à ces fins. J'ai noté la semaine dernière que le représentant de la GRC n'était pas particulièrement clair pour ce qui est de savoir si, oui ou non, la GRC utilise la reconnaissance faciale.

Au mieux, je dirais que je n'ai pas de raison de croire que la GRC utilise la reconnaissance faciale à des fins de surveillance de masse. Par contre, la définition des circonstances dans lesquelles elle l'utilise semble assez ambigüe. C'est d'ailleurs pour cette raison que nous communiquons aujourd'hui le document d'orientation et que nous recommandons que les corps policiers soient assujettis à une loi claire qui autorise, mais prohibe également, l'utilisation de la reconnaissance faciale dans certaines circonstances.

M. René Villemure: Merci beaucoup.

Le président: Merci, monsieur Villemure.

[*Traduction*]

Madame Gazan, je vous souhaite la bienvenue au comité de l'éthique. Vous avez six minutes.

Mme Leah Gazan (Winnipeg-Centre, NPD): Je vous remercie beaucoup, monsieur le président.

Monsieur Therrien, votre bureau [*difficultés techniques*].

● (1140)

Le président: Votre microphone n'était pas activé.

Mme Leah Gazan: Oh, il ne l'était pas? Je suis désolée.

Le président: Je vais redémarrer le chronomètre. Allez-y, madame Gazan. Je vais vous demander de répéter votre question.

Mme Leah Gazan: Je vous remercie, monsieur le président. À titre d'information, ce n'est pas ma première séance. Je m'excuse auprès de chacun.

Monsieur Therrien, votre bureau a publié un rapport en juin 2021 intitulé *Technologie de reconnaissance faciale: utilisation par les services de police au Canada et approche proposée*. Le rapport contient une série de recommandations que la GRC s'est engagée à mettre en œuvre au plus tard 12 mois après la réception du rapport. Parmi les recommandations, il y a la mise en place d'un programme de formation pour s'assurer que tous les décideurs sont formés sur les limites de la collecte de renseignements personnels au titre de la Loi sur la protection des renseignements personnels, l'adoption de politiques visant à préciser les personnes habilitées à prendre les décisions au sujet de la collecte de renseignements personnels, et la mise en place de mécanismes de surveillance des collectes non autorisées.

Pourriez-vous nous en dire plus sur les recommandations que la GRC a acceptées, et sur l'amélioration des pratiques qui en résultera?

M. Daniel Therrien: Je vous remercie de la question.

La GRC n'était pas d'accord avec notre conclusion sur une question de droit, à savoir qu'elle violait la loi visant le secteur public en recourant à Clearview, mais elle a beaucoup collaboré avec nous en reconnaissant qu'elle devait se doter d'un meilleur mécanisme de vérification lorsqu'elle utilise des nouvelles technologies, qu'il s'agisse de reconnaissance faciale ou d'autres technologies.

Elle a donc accepté, je crois, l'idée qu'elle doit mettre en place des mécanismes de vérification, et nous avons de bonnes discussions avec elle depuis juin l'an dernier. Je ne pense pas qu'elle arrivera à mettre en œuvre toutes ces recommandations dans un délai d'un an, mais il y a eu d'importants progrès de réalisés.

Mme Leah Gazan: Elle avait toutefois convenu de les mettre en œuvre au plus tard 12 mois après la réception du rapport. Vous dites donc que les recommandations n'ont pas été mises en œuvre et que cela fait plus de 12 mois. Est-ce exact?

M. Daniel Therrien: Elle ne l'a pas encore fait, et il est peu probable qu'elle respecte l'échéance des 12 mois, mais il y a de bons progrès, et je constate qu'elle déploie des efforts sincères.

Il s'agit d'une question relativement complexe, mais nous souhaiterions bien entendu que les recommandations soient mises en œuvre le plus tôt possible.

Mme Leah Gazan: Je vais poursuivre.

Le rapport de juin 2021 mentionne également:

> La GRC a commis des manquements graves et systémiques à l'obligation de se conformer à la Loi avant de recueillir des renseignements auprès de Clearview et, de façon plus générale, avant toute nouvelle collecte de renseignements personnels. Il s'agit notamment d'omissions généralisées pour ce qui est de savoir ce qu'elle recueillait, de contrôler la méthode de collecte, de cerner les problèmes éventuels de conformité, ainsi que d'évaluer et de prévenir les contraventions à la Loi.

Les mots « systémiques » et « généralisées » laissent entendre qu'il ne s'agissait pas d'une erreur ponctuelle ou d'une mauvaise décision. Comment peut-on alors s'assurer que la GRC respectera à l'avenir les lois sur la protection des renseignements personnels et qu'il n'y aura pas d'autres cas comme celui de Clearview qui passent en douce sous le radar?

Je pose cette question parce qu'on utilise dans le rapport les mots « systémiques » et « généralisées ».

M. Daniel Therrien: Les mots utilisés renvoient au fait qu'à ce moment, la GRC n'avait aucun mécanisme en place pour veiller à ce que, lorsque ses agents utilisent une nouvelle technologie, une procédure de vérification et d'approbation soit en place pour s'assurer que cette technologie respecte la loi, y compris le droit à la vie privée.

C'est une situation qui est loin d'être idéale, et c'est le moins qu'on puisse dire, mais la GRC a reconnu le problème et s'emploie à mettre un mécanisme en place. Il lui faudra un peu plus de temps que nous l'espérions, mais je pense que les choses vont dans le bon sens.

● (1145)

Mme Leah Gazan: Je trouve cela inquiétant, parce qu'il s'agit d'enjeux liés à la protection de la vie privée. Vous dites que cela prendra un certain temps. Avez-vous une idée du temps qu'il faudra?

Je pose la question parce que la GRC devait mettre en œuvre les recommandations 12 mois après la réception du rapport. Elle ne l'a pas fait. Nous savons que le problème est systémique et généralisé. Selon vous, combien de temps faudra-t-il?

M. Daniel Therrien: La GRC a mis en place un mécanisme. C'est la mise en œuvre des éléments qui l'entourent — la formation des agents, par exemple — qui prend plus de temps que ce que nous espérions.

Je vous proposerais de poser la question à la GRC. Nous l'avons fait, bien entendu. Je peux vous fournir sa réponse. Je peux prendre des dispositions à cet égard. Je vais faire cela.

Mme Leah Gazan: Je vous remercie beaucoup. Pourriez-vous faire parvenir l'information au Comité? Est-ce possible?

M. Daniel Therrien: Oui.

Mme Leah Gazan: D'accord. Je vous remercie beaucoup.

Je ne suis pas certaine du temps qu'il me reste, monsieur le président.

Le président: Il vous reste 20 secondes. Vous avez le temps de poser une question très brève.

Mme Leah Gazan: J'ai le temps donc...

Le président: Vous devez faire très vite, toutefois.

Mme Leah Gazan: Lors d'une enquête conjointe sur Clearview...

Je ne sais pas combien de temps il me reste maintenant.

Une voix: Il ne vous en reste plus.

Mme Leah Gazan: Il ne m'en reste plus. Très bien. Je vous remercie...

Le président: Nous avons du temps aujourd'hui. Je me montre un peu généreux, alors vous pouvez poser votre question. Après une brève question et une brève réponse, nous allons poursuivre.

Mme Leah Gazan: Je vous remercie beaucoup, monsieur le président.

Lors de l'enquête conjointe sur Clearview menée par le commissaire à la protection de la vie privée du Canada, le commissaire à l'information et à la vie privée de la Colombie-Britannique et la commissaire à l'information et à la vie privée de l'Alberta, les recommandations ont été les suivantes: premièrement, cesser d'offrir à des clients au Canada les services de reconnaissance faciale qui ont fait l'objet de l'enquête; deuxièmement, mettre fin à la collecte, à l'utilisation et à la communication d'images et de matrices faciales biométriques auprès d'individus au Canada; troisièmement, supprimer les images et les matrices faciales biométriques recueillies auprès d'individus au Canada qu'elle a en sa possession.

Clearview a-t-elle mis en place ces mesures?

M. Daniel Therrien: Clearview a cessé d'offrir ses services au Canada en 2020, je crois, pendant que l'enquête était encore en cours, mais elle conteste les décisions de mes collègues devant les tribunaux, parce qu'elle ne veut pas s'engager à ne plus offrir ses services de façon permanente. En ce moment, elle n'offre pas ses services au Canada.

Mme Leah Gazan: Je vous remercie.

Le président: Monsieur Williams, vous avez cinq minutes.

M. Ryan Williams (Baie de Quinte, PCC): Je vous remercie, monsieur le président, et par votre entremise, je remercie aussi M. Therrien.

Comme vous l'avez mentionné, des représentants de la GRC sont venus témoigner la semaine dernière. Ils ont dit ne pas être d'accord avec votre conclusion voulant que l'utilisation par la GRC de la technologie de Clearview AI était illégale. Cette position a été réaffirmée.

Est-ce que la raison de leur désaccord avec votre conclusion est valable, et pourquoi l'est-elle ou ne l'est-elle pas?

M. Daniel Therrien: Je vais donner une réponse d'avocat, qui, je pense, sera claire.

La disposition en cause est celle de la Loi sur la protection des renseignements personnels qui régit la collecte de renseignements, dans ce cas-ci par la GRC. Ce que dit la GRC, c'est que cet article, l'article 4 de la Loi sur la protection des renseignements personnels, n'exige pas explicitement qu'une institution fédérale comme la GRC s'assure de la légalité des pratiques de son partenaire commercial avant que le secteur public n'utilise l'information.

Il est vrai que l'article 4 n'exige pas explicitement cela d'une institution fédérale; nous pensons que l'exigence existe implicitement. En gros, imaginez que les institutions fédérales puissent sous-traiter et être en mesure, par l'entremise de contrats avec le secteur privé, de s'engager dans des pratiques qu'elles ne peuvent pas adopter directement. C'est inacceptable. Nous pensons que la loi ne le permet pas.

Cela dit, est-ce crédible ou raisonnable? La position de la GRC repose sur une base crédible. Dans la mesure où il y a une ambiguïté dans la loi, je vous encourage vivement à combler cette lacune et à exiger des institutions gouvernementales — pas seulement de la GRC, mais de toutes les institutions gouvernementales — qu'elles s'assurent que ce qu'elles achètent est légal lorsqu'elles font appel au secteur privé.

● (1150)

M. Ryan Williams: Je vous remercie.

Comme question de suivi, les pouvoirs de votre bureau devraient-ils être renforcés pour que les décisions sur les violations de la Loi sur la protection des renseignements personnels soient contraignantes et correctement appliquées, puisque la GRC semble en avoir fait fi?

M. Daniel Therrien: La réponse courte est oui. Nous l'avons recommandé à plusieurs reprises. Oui.

M. Ryan Williams: D'accord.

Au sujet de l'utilisation des données par la GRC, savez-vous combien de condamnations ont été obtenues à l'aide de preuves recueillies par Clearview AI?

M. Daniel Therrien: Non, je ne le sais pas. Nous leur avons demandé combien de fois ils les avaient utilisées, et je crois que c'était dans des dizaines de cas. Quant aux condamnations, non, je n'en connais pas le nombre.

M. Ryan Williams: À votre avis, est-ce l'utilisation de la technologie de reconnaissance faciale de Clearview AI pourrait risquer de faire annuler la condamnation d'un criminel arrêté ou poursuivi en justice à l'aide de ces données?

M. Daniel Therrien: Je pense que c'est une question hypothétique. La GRC dit, ce dont je n'ai aucune raison de douter, que lorsqu'elle utilise la technologie, il y a un examen par un agent. J'en conclus qu'un agent de police entreprend ensuite une enquête et présente les preuves par l'entremise d'un procureur de la Couronne selon les règles normales. C'est mon hypothèse, mais je ne le sais pas.

M. Ryan Williams: Jeudi dernier, la GRC a déclaré au Comité que Clearview AI était le seul système de reconnaissance faciale moderne qu'elle utilisait, mais sans pouvoir donner de détails sur les systèmes non modernes. Votre enquête vous a-t-elle permis de savoir si la GRC utilise d'autres systèmes de reconnaissance faciale?

M. Daniel Therrien: Nous ne sommes pas au courant que la GRC utilise d'autres systèmes de reconnaissance faciale. Il existe, bien sûr, de nombreux autres systèmes, à part celui de Clearview, mais ils n'ont pas tous le même niveau de précision, ce qui est préoccupant.

En ce qui concerne la GRC, nous ne savons pas si elle utilise un autre système que Clearview. Elle n'utilise pas Clearview actuellement.

M. Ryan Williams: Je vous remercie.

Madame Kosseim, savons-nous comment les images des Ontariens sont recueillies et stockées à l'heure actuelle? Les entreprises qui utilisent la technologie de reconnaissance faciale recueillent des images. Savons-nous comment elles sont recueillies et stockées en Ontario?

Me Patricia Kosseim: Malheureusement, je n'ai pas d'information sur les entreprises en Ontario, car cela ne relève pas de notre compétence. Je ne peux pas répondre à cette question avec certitude.

M. Ryan Williams: Je vais m'en tenir au secteur public, alors. Savons-nous comment ils sont stockés?

Me Patricia Kosseim: Est-ce en général ou dans le cadre de l'utilisation de la technologie de reconnaissance faciale?

M. Ryan Williams: Je dirais en général, y compris la technologie de reconnaissance faciale.

Me Patricia Kosseim: Je vais vous donner quelques exemples.

Les services de police utilisent assurément des images dans les bases de données de photos signalétiques en vertu des pouvoirs qui leur sont conférés par la Loi sur l'identification des criminels. Il y a aussi évidemment beaucoup de collecte de renseignements qui se fait par la vidéosurveillance, qu'elle soit générale, municipale ou autre. C'est une pratique qui a cours, qui est assez répandue, et qui permet donc de recueillir des images de personnes.

M. Ryan Williams: Je vous remercie beaucoup.

Je vous remercie, monsieur.

Le président: Je vous remercie.

Madame Hepfner, vous avez cinq minutes.

Mme Lisa Hepfner (Hamilton Mountain, Lib.): Je vous remercie beaucoup.

[*Français*]

Je remercie tous les témoins qui sont parmi nous aujourd'hui.

Je vais d'abord m'adresser à M. Therrien, mais je vais le faire en anglais, étant donné que c'est plus facile pour moi.

[*Traduction*]

Vous avez mentionné que tous les intervenants que vous avez consultés étaient d'accord pour dire que la loi sur la protection de la vie privée au Canada devait être mise à jour. C'est logique, car lorsqu'elle a été rédigée, nous ne connaissions pas la technologie de reconnaissance faciale.

J'aimerais savoir quel genre de conseil vous donneriez aux législateurs pour que la loi soit souple afin que nous n'ayons pas à la réécrire chaque fois qu'une nouvelle technologie apparaît. Comment pouvons-nous faire en sorte qu'elle soit souple et continue de s'appliquer lorsqu'il y a de nouveaux progrès technologiques?

M. Daniel Therrien: C'est une bonne question.

Je dirais tout d'abord que nous avons, en effet, des lois. Nous avons évidemment la Charte et nous avons la common law, et il y a certaines lois comme la Loi sur la GRC qui régissent la situation. Dans le secteur privé, nous avons la Loi sur la protection des renseignements personnels et les documents électroniques.

Pour ce qui est de la souplesse nécessaire pour éviter que la loi ne devienne obsolète, l'un des avantages de la Loi sur la protection des renseignements personnels et les documents électroniques est qu'elle est fondée sur des principes, de sorte qu'elle ne vise pas à réglementer des situations particulières, mais traite de principes. Cependant, je pense que la reconnaissance faciale est l'élément où nous commençons à voir les limites des avantages d'une approche basée sur des principes, parce que si on réglemente la reconnaissance faciale en disant que l'utilisateur doit rendre des comptes, ou si on applique des principes de cette nature, ou la proportionnalité, on laisse beaucoup de latitude à la police pour exercer ces grands principes d'une manière qui convient à ses intérêts.

Je ne dis pas qu'il ne devrait pas y avoir de loi fondée sur des principes. De façon générale, cela a beaucoup de sens, mais dans le cas de la reconnaissance faciale, en raison des risques extrêmement élevés concernant la vie privée et d'autres droits, comme les droits démocratiques, le droit de manifester ou le droit à l'égalité, nous disons qu'il devrait y avoir des dispositions particulières — par exemple, dans le cas de la police — pour interdire les utilisations sauf dans certaines circonstances.

Une loi fondée sur des principes qui repose sur une base solide a du sens, mais dans le cas de la reconnaissance faciale, elle devrait inclure l'ajout de quelques règles particulières qui garantissent que les grands principes ne sont pas utilisés abusivement ou interprétés de manière trop large.

● (1155)

Mme Lisa Hepfner: Très bien. C'est très utile. Je vous remercie.

Je sais que le Bureau de la concurrence se penche également sur la technologie et les nouveaux problèmes que cela crée pour protéger la vie privée. Pouvez-vous nous dire si vous entretenez des liens avec le Bureau de la concurrence et si votre bureau travaille de concert avec lui pour s'attaquer à certains de ces problèmes?

M. Daniel Therrien: La réponse courte est oui, nous travaillons avec les gens du Bureau de la concurrence. Nous avons des discussions avec eux assez régulièrement, mais nous sommes tous deux, le Bureau de la concurrence et le Commissariat à la protection de la vie privée, limités par les lois qui nous régissent actuellement, en ce sens que nous ne pouvons pas échanger, par exemple, les renseignements détaillés que nous recueillons dans le cadre d'une enquête parce que nous sommes tous deux liés par une règle de confidentialité qui nous empêche d'échanger avec l'autre organisme de réglementation les détails de ce que nous affirmons.

Nous pouvons avoir des discussions sur des principes généraux. Nous pouvons parler des tendances générales, mais il serait extrêmement utile, comme nous l'avons tous deux recommandé au cours des mois et des années passés, de pouvoir échanger ce que nous avons appris au cours des enquêtes afin que notre collaboration soit plus efficace.

Mme Lisa Hepfner: Il me reste 30 secondes, alors je vais faire vite.

Vous avez mentionné avoir été étonné par la déclaration de la GRC qui a dit que la technologie de reconnaissance faciale doit être ciblée, limitée dans le temps et assujettie à des vérifications par des experts formés. Quelles sont les bonnes utilisations de cette technologie? Vous avez donné des exemples, la lutte contre la criminalité, la recherche d'enfants disparus. Quelles sont les utilisations acceptables de cette technologie?

M. Daniel Therrien: Pour ce qui est de la police, je pense que ces deux exemples sont les plus importants. Quant au terme « crime », je le préciserais en parlant plutôt de « crime grave ». Je ne suis pas sûr que la reconnaissance faciale doive être utilisée pour les vols ordinaires, par exemple, étant donné les risques que présente l'utilisation de cette technologie pour le respect de la vie privée et d'autres droits démocratiques, mais elle peut assurément être utilisée pour les crimes graves, comme les disparitions d'enfants, et pour d'autres objectifs impérieux de l'État, comme dans le contexte des frontières, afin de garantir que les personnes suspectes puissent être identifiées à la frontière sans entraver le flux des voyageurs vers le pays. J'estime que la nécessité d'identifier les personnes suspectées à la frontière dans ce contexte constituerait un motif impérieux.

Le président: Merci, monsieur le commissaire. Nous avons accordé beaucoup de temps à cette série de questions, mais je pense que nous pouvons le faire aujourd'hui.

Vous pouvez commencer votre tour de deux minutes et demie, monsieur Villemure.

● (1200)

[*Français*]

M. René Villemure: Merci, monsieur le président.

Monsieur Therrien, je vais procéder rapidement, mais, si vous pouviez nous fournir des informations par la suite, ce serait formidable.

On a parlé de Clearview AI, qui a fui le pays pour aller quelque part où il ne serait pas assujetti à nos lois, mais il y a également des compagnies comme Palantir, qui sont des acteurs importants dans l'industrie de la reconnaissance faciale et de la gestion des données.

Ces entreprises sont-elles capables d'autoréglementation?

M. Daniel Therrien: Non.

M. René Villemure: Le plan éthique n'est pas un souci pour ces entreprises, qui sont assez ouvertes à exploiter les données sans trop de limites, je crois.

M. Daniel Therrien: En fait, je pense que c'est l'une des leçons que nous pouvons tirer des dernières années d'utilisation de la technologie: il faut mettre fin au régime d'autoréglementation des compagnies, et celles qui sont dans le champ de la surveillance devraient particulièrement être visées. De façon générale, il faut donc que les élus réglementent l'utilisation de la technologie. C'est la principale leçon à tirer des dernières années.

M. René Villemure: Pourriez-vous nous dire quelques mots sur Palantir, qui est toujours un fournisseur du gouvernement du Canada?

M. Daniel Therrien: Il est clair que les pratiques de cette compagnie nous préoccupent beaucoup, mais, comme nous n'avons pas enquêté sur Palantir, je ne me sentirais pas à l'aise de faire des commentaires sur cette compagnie.

M. René Villemure: Madame Kosseim, avez-vous enquêté sur Palantir?

Me Patricia Kosseim: Non.

M. René Villemure: Vous, maître Poitras, l'avez-vous fait?

Me Diane Poitras: Non.

M. René Villemure: D'accord.

Au sujet des quatre éléments qui ont été mentionnés plus tôt, vous avez dit qu'une entité était chargée de voir à leur application.

Quelle est cette entité?

M. Daniel Therrien: En tant qu'autorités de protection des données, nous croyons que nous aurions un rôle à jouer pour ce qui est de la protection des données personnelles. Cependant, la reconnaissance faciale met en cause d'autres droits, comme le droit à l'égalité dans les cas de discrimination contre certains groupes, et il y a les droits démocratiques aussi.

Alors, nous ne demandons pas d'avoir un monopole sur la réglementation de la reconnaissance faciale, mais je pense que, comme dans d'autres domaines, il serait possible et utile d'avoir un certain nombre d'organismes de réglementation. Dans les cas de discrimination, par exemple, ce seraient la Commission canadienne des droits de la personne ou les équivalents dans les provinces.

Alors, nous pensons que nous avons un rôle à jouer dans la protection des données, mais d'autres agences de réglementation devraient aussi avoir des responsabilités.

M. René Villemure: Il devrait donc y avoir un genre d'ensemble d'organismes, qui pourrait constituer une autre entité.

[*Traduction*]

Le président: Merci.

Nous passons à M. Green. Je suis heureux de vous revoir. Allez-y. Vous avez deux minutes et demie.

M. Matthew Green (Hamilton-Centre, NPD): Merci.

Monsieur le président, l'un des témoins nous a déjà répondu aujourd'hui qu'une industrie privée ne pouvait pas s'autoréglementer. Vous vous souvenez certainement que, dans un témoignage précédent, la GRC a exprimé son désaccord avec les conclusions du commissaire à la protection de la vie privée concernant les infractions présentes, et je veux donc interroger le Commissariat à la protection de la vie privée à ce sujet.

Le Commissariat à la protection de la vie privée a conclu que l'utilisation de Clearview AI par la GRC contrevenait à la Loi sur la protection des renseignements personnels et à la LPRPDE. Dans son témoignage, la GRC a exprimé son désaccord avec les conclusions de l'enquête. Par votre intermédiaire, monsieur le président, pourquoi le Commissariat à la protection de la vie privée estime-t-il que la GRC a enfreint la Loi sur la protection des renseignements personnels et la LPRPDE?

M. Daniel Therrien: La GRC affirme que la Loi sur la protection des renseignements personnels ne l'oblige pas explicitement à vérifier la légalité des pratiques de ses entrepreneurs du secteur privé. Il est vrai que la Loi sur la protection des renseignements personnels ne l'indique pas explicitement. Nous sommes d'avis qu'une interprétation correcte de cette loi est qu'ils ont cette responsabilité, et si la loi comporte une ambiguïté, j'invite vivement les parlementaires à combler cette lacune et à la rendre claire, comme je l'ai suggéré il y a quelques minutes.

M. Matthew Green: En d'autres termes, ils ne peuvent pas faire indirectement ce qu'ils ne peuvent pas faire directement. Est-ce exact?

● (1205)

M. Daniel Therrien: Exactement.

M. Matthew Green: Pourtant, nous nous trouvons face à un scénario dans lequel nous savons que les services de police utilisent ce système de façon détournée, par le biais de nombreuses méthodes de passation de marchés, d'achats et également d'essais.

Nous avons entendu la GRC déclarer dans son témoignage qu'elle ne savait pas qui avait approuvé l'utilisation de cette technologie. Savez-vous si d'autres services de police en Ontario utilisent actuellement Clearview?

M. Daniel Therrien: L'entreprise Clearview nous a indiqué qu'elle avait quitté le marché canadien. Pour l'instant, elle n'offre ses services à personne au Canada.

M. Matthew Green: Comment feriez-vous pour boucler la boucle et garantir que ces atteintes à la vie privée, aux droits à l'information et aux libertés civiles ne soient pas commises à nouveau à l'avenir, non seulement par le secteur privé, mais surtout par les forces de l'ordre?

M. Daniel Therrien: Aujourd'hui, j'ai formulé, avec les commissaires des provinces et des territoires, un certain nombre de recommandations visant à modifier la loi. Je pense qu'il est urgent de le faire, car les risques sont très importants.

Nous devons commencer par améliorer les lois. En attendant que celles-ci soient modifiées, nous avons publié des conseils sur la manière d'utiliser les lois actuelles, et nous espérons que ceux-ci atténueront les risques.

M. Matthew Green: Merci beaucoup.

Le président: Merci.

Nous allons maintenant passer à M. Bezan, qui aura cinq minutes.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Merci, monsieur le président.

Je tiens à remercier nos témoins pour leurs présentations et leur participation à cette importante étude. L'annonce que vous avez faite conjointement plus tôt aujourd'hui n'aurait pas pu mieux tomber, compte tenu du travail que nous effectuons en ce moment.

Monsieur Therrien, pour faire suite à la question de M. Green, vous avez dit que la GRC utilisait illégalement la technologie Clearview. Des sanctions ont-elles été imposées à la GRC, ou à Clearview, d'ailleurs?

M. Daniel Therrien: Non, mais nous devrions traiter cette question comme une question institutionnelle. J'aurais tendance à l'envisager du point de vue de l'institution, plutôt que du point de vue des personnes.

Nous avons recommandé à la GRC d'améliorer ses processus, mais je ne suis au fait d'aucune sanction.

M. James Bezan: Connaissez-vous l'organisation IntelCenter et la base de données IntelCenter consacrée à la technologie de reconnaissance faciale?

M. Daniel Therrien: Personnellement, je ne la connais pas. Certains de mes collègues du Commissariat de la protection de la vie privée en ont peut-être entendu parler. Nous pouvons fournir des renseignements si nous en avons.

M. James Bezan: D'après les demandes d'accès à l'information que nous venons de recevoir, il semble que la GRC, le SCRS et le ministère de la Défense nationale utilisent cette technologie. Je pense que c'est une chose sur laquelle nous devons également nous pencher.

Leurs propres documents suggèrent qu'ils utilisent des images de source ouverte pour identifier notamment des terroristes sur Internet et qu'ils les fournissent ensuite aux organismes d'application de la loi comme la GRC et le SCRS.

M. Daniel Therrien: Si nous disposons de renseignements, nous les fournirons.

M. James Bezan: Vous pourrez peut-être en tenir compte.

Lorsque vous parlez de modifier la législation existante, vous parlez de la Loi sur la protection des renseignements personnels et de la LPRPDE. Devrait-on également inclure le Code criminel?

M. Daniel Therrien: C'est possible. Je n'ai pas encore réfléchi aux éléments exacts de la législation qui devraient être modifiés.

Comme je l'ai indiqué dans ma réponse à une question précédente de Mme Hepfner, je pense que nous devons nous fonder sur des principes, auxquels s'ajouteraient quelques dispositions pour veiller à ce que les principes généraux ne puissent pas donner lieu à une interprétation trop généreuse. Il s'agirait assurément la LPRPDE, de la Loi sur la protection des renseignements personnels, et potentiellement du Code criminel.

La common law accorde une autorité importante à l'utilisation de diverses technologies. Le Code criminel pourrait éventuellement être examiné dans l'optique de restreindre certains de ces pouvoirs de la common law, mais je n'y ai pas réfléchi sérieusement.

M. James Bezan: Si l'on pense à l'utilisation de la technologie de reconnaissance faciale et à la protection de la charte et du droit à la vie privée, devrions-nous adopter la même approche que pour les écoutes téléphoniques?

Je sais que le CST et le SCRS surveillent beaucoup les discussions en ligne, en essayant de se concentrer sur le terrorisme et les organisations criminelles transnationales. Encore une fois, ils ne peuvent pas faire indirectement ce qu'il leur est interdit de faire directement. Chaque fois qu'ils risquent d'enfreindre la Charte, ils doivent obtenir un mandat ou une autorisation ministérielle pour s'assurer qu'ils la respectent. Lorsque vous parlez de fins autorisées, est-ce bien ce à quoi vous faites référence? Doit-il y avoir des mandats ou des autorisations ministérielles affirmant que ces fins sont nécessaires et proportionnelles à l'infraction qui pourrait être portée aux droits d'une personne?

● (1210)

M. Daniel Therrien: Il est concevable que des mandats soient nécessaires dans certains cas. Lorsque nous recommandons que la législation définisse les utilisations « permises » et « interdites », nous pensons à certaines catégories de circonstances, comme les crimes graves, quelle que soit la définition que les parlementaires souhaitent en donner. Voilà ce à quoi nous pensons, et non à des autorisations au cas par cas.

Nous nous rapprochons dans nos recommandations lorsque nous disons qu'il devrait y avoir une autorisation au niveau du programme ou un avis préalable à l'utilisation. Cette approche est semblable à celle de la législation québécoise, selon laquelle un corps policier se présenterait devant un organisme de réglementation indépendant et dirait qu'il veut utiliser la technologie de reconnaissance faciale dans le cas suivant — non pas une circonstance individuelle, mais un groupe de cas — qui serait ensuite examiné avec l'organisme responsable de la protection des données et approuvé au niveau du programme. Cette méthode se rapproche de l'autorisation individuelle.

Il n'est pas inconcevable que, dans certains cas, des mandats individuels soient émis par un juge pour un cas particulier, mais il ne s'agit pas de notre point de départ.

Le président: Merci, monsieur Bezan.

Madame Thompson, merci de vous joindre au Comité. Bienvenue.

Allez-y. Vous avez cinq minutes.

Mme Joanne Thompson (St. John's-Est, Lib.): Merci, monsieur le président. Je suis ravie d'être ici.

Ma question s'adresse au commissaire à la protection de la vie privée, M. Therrien.

Plus tôt aujourd'hui, vous avez parlé d'un moratoire. Je crois que vous avez indiqué que vous seriez favorable à l'utilisation de la technologie de reconnaissance faciale par les forces de l'ordre jusqu'à ce que le cadre réglementaire de cette technologie soit en place. Pouvez-vous nous en dire plus à ce sujet, si vous êtes effectivement favorable à un tel moratoire?

M. Daniel Therrien: Notre point de départ en tant que commissaires — mes collègues des provinces et territoires et moi-même — est que la loi devrait en définitive préciser les circonstances « permises » et « interdites » de l'utilisation de la reconnaissance faciale. Nous sommes en effet d'avis qu'il existe des circonstances impérieuses dans lesquelles cette technologie devrait être utilisable par les forces de police. Je ne serais pas favorable à une interdiction totale de cette technologie, nous devons pouvoir l'utiliser dans des circonstances impérieuses.

Lorsque j'ai fait référence à la GRC, je suggérais qu'à défaut de la législation que nous espérons vraiment voir adoptée dans un avenir assez proche, si la GRC s'engageait à n'utiliser cette technologie qu'en fonction d'une politique — et le représentant de la GRC la semaine dernière a relevé certaines caractéristiques de cette politique comme étant « ciblées, limitées dans le temps », etc. — il s'agirait d'un moratoire partiel volontaire, si vous me permettez cette expression.

En ce qui concerne l'interdiction totale de la reconnaissance faciale jusqu'à l'adoption d'une nouvelle loi, je n'y serais pas favorable.

Mme Joanne Thompson: Merci.

Cette démarche s'appliquerait-elle également à l'utilisation de la reconnaissance faciale dans les espaces publics?

M. Daniel Therrien: Oui, les recommandations que nous formulons s'appliquent également aux espaces publics.

Mme Joanne Thompson: J'aimerais passer à la protection des renseignements personnels dans les documents électroniques. J'ai consacré toute ma carrière à ce domaine.

Actuellement, elle est neutre sur le plan technologique, ce qui lui permet de perdurer dans le temps. Une loi neutre sur le plan technologique devrait-elle s'appliquer à la technologie de reconnaissance faciale?

M. Daniel Therrien: Nous revenons à la question à laquelle j'ai répondu il y a quelques minutes.

Une législation fondée sur des principes et neutre sur le plan technologique pour le secteur privé est un bon point de départ. La raison pour laquelle nous recommandons l'adoption d'une législation particulière pour les forces de police est liée aux inconvénients de cette technologie particulière de reconnaissance faciale. Il se pourrait que certaines utilisations de cette technologie par des entreprises privées présentent des risques extrêmement élevés, non seulement pour la protection des renseignements personnels, mais aussi pour d'autres droits. Clearview en est un bon exemple. C'est ce que nous appelons de la surveillance de masse.

M. Fergus a mentionné d'autres circonstances. Je suis d'accord pour dire que le fait de susciter des émotions dans le but de vendre un produit, ou dans tout autre but, ne devrait pas être autorisé.

Nous allons fournir quelques exemples de législations adéquates. Il existe un projet de législation dans l'Union européenne, qui n'a pas encore été adopté, et qui constitue un bon modèle. Il faudrait évidemment l'adapter. Il stipule, entre autres, que la reconnaissance faciale ne doit pas être utilisée pour enfreindre les droits de la personne. Ce principe s'applique horizontalement, que ce soit à l'État ou aux entreprises privées. Je pense que les parlementaires canadiens devraient y réfléchir sérieusement.

● (1215)

Mme Joanne Thompson: Merci.

L'un des éléments sur lesquels je reviens sans cesse dans la conversation de ce matin est la manière de concilier les réalités de la rapidité de la technologie de reconnaissance faciale avec la nécessité d'établir méthodiquement la législation et la protection des droits de la personne, de la sécurité et des renseignements personnels. Comment créer cet équilibre?

M. Daniel Therrien: Pour ce faire, il faut une législation fondée sur des principes, complétée — si nécessaire, compte tenu du contexte — par une législation plus spécifique.

Je tiens à ajouter ceci. Je vous ai entendu demander à certains témoins de ce Comité s'il est trop tard. Il n'est jamais trop tard. D'ailleurs, le fait que certaines pratiques se produisent actuellement ne devrait pas vous empêcher de faire le nécessaire et de réglementer la technologie d'une manière qui respecte les droits des Canadiens.

Nous vivons, pas complètement, mais en partie, dans un monde d'autorégulation qui a engendré certaines pratiques inacceptables. Le fait qu'elles soient routinières ou banales, comme le dirait ma collègue Diane Poitras, ne signifie pas que l'on doive continuer à les autoriser.

Le président: Merci, monsieur le commissaire.

Pour poursuivre cette journée, nous avons ajouté 35 à 40 secondes au tour de chaque personne.

Allez-y, monsieur Villemure. C'est à vous, pour deux minutes et demie environ.

[*Français*]

M. René Villemure: Merci, monsieur le président.

Certaines études dont nous avons pris connaissance manquent de données probantes, mais on y fait quand même état de la possibilité de déterminer les préférences sexuelles des gens, de déterminer leurs opinions politiques, de faire ce genre de discriminations. Parlons-nous d'un monde irréel ou allons-nous devoir nous pencher sur cette question dans un avenir prévisible, monsieur Therrien?

M. Daniel Therrien: Ce n'est pas du tout du domaine de l'irréel, et la législation proposée en Europe, que je viens d'évoquer, vise à interdire ce genre de pratiques, parce qu'elles posent un risque réel, aujourd'hui.

M. René Villemure: C'est un outil de discrimination fascinant.

Nous avons aussi entendu parler de terrorisme biométrique, soit la corruption des bases de données, à l'entrée et à la sortie du pays, de façon à faciliter la commission d'actes criminels. Avez-vous été interpelé par ce genre d'information, pas nécessairement au Commissariat, mais dans vos recherches en général?

M. Daniel Therrien: Pourriez-vous préciser un peu la notion de terrorisme? Parlez-vous de gens voudraient entrer au pays en falsifiant des données?

M. René Villemure: Serait-il possible de faciliter l'entrée d'une personne en modifiant toutes ses données biométriques de sorte que la personne entre sous une fausse identité? Pourrait-on fausser les entrées biométriques à l'entrée et à la sortie du pays à des fins criminelles?

M. Daniel Therrien: Ce n'est pas impossible. Cela renvoie à la notion des protections nécessaires dans le cas de l'utilisation de la reconnaissance faciale. Des mesures de sécurité extrêmement serrées sont requises pour prévenir ce genre de risque.

M. René Villemure: D'accord.

Madame Poitras, vous avez dit tantôt qu'il n'y avait pas eu de consentement des personnes dans le cas de Clearview AI, mais tous nos témoins nous ont dit que le consentement était impossible à obtenir dans le cas de la reconnaissance faciale à grande échelle. Que suggérez-vous à cet égard?

Me Diane Poitras: C'est une bonne question parce que le consentement des personnes, dans le contexte de la reconnaissance faciale, n'est pas toujours approprié.

Premièrement, il y a une asymétrie des pouvoirs, que ce soit entre le citoyen et l'État ou entre le citoyen et une grosse entreprise, comme les géants du Web, par exemple.

Deuxièmement, il est difficile de donner un consentement éclairé, qui est l'une des qualités essentielles d'un consentement. C'est une technologie extrêmement complexe, et la capacité du citoyen à donner un consentement éclairé est, à mon avis, très limitée. La façon de pallier ces consentements est d'autoriser, dans la loi, certaines utilisations, comme, par exemple, certaines des recommandations qui sont faites aujourd'hui. On pourrait également interdire certaines utilisations, là où l'on croit que, même avec un consentement ou une autorisation, l'usage ne serait pas approprié dans une société démocratique. Je pense que le fait de définir dans la loi certaines utilisations acceptables ou non est un premier pas dans la bonne direction.

● (1220)

[*Traduction*]

Le président: Merci.

Nous allons maintenant donner la parole à M. Green.

M. Matthew Green: Merci, monsieur le président.

Vous savez sans doute que nous avons passé beaucoup de temps à essayer de commencer à comprendre la technologie de reconnaissance faciale, mais je crois que l'intelligence artificielle représente peut-être un outil encore plus important au moyen duquel les interventions du secteur public et du secteur privé dans notre vie quotidienne modifient rapidement notre contexte social. Je pense à *Rapport minoritaire*. Je pense à la rhétorique de la police en matière de maintien de l'ordre proactif et à sa capacité de pratiquer une surveillance prédictive.

Mes questions s'adressent à la commissaire à l'information et à la protection de la vie privée de l'Ontario, qui a participé au processus qui a mené à l'élaboration de la politique sur l'utilisation des technologies d'intelligence artificielle par la Commission des services policiers de Toronto en formulant des commentaires dans le cadre de l'ébauche de la politique avant la consultation publique.

Les recommandations que vous avez formulées en vue de l'amélioration du projet de politique ont-elles été prises en compte dans la politique finale?

Me Patricia Kosseim: Il est certain que toutes nos consultations avec le Service de police de Toronto, y compris le comité de surveillance, ont tendance à être constructives. Je pense en particulier à notre consultation, par exemple, sur les caméras corporelles, qui a entraîné l'élaboration d'un cadre général qui a depuis été publié.

En ce qui concerne le cadre relatif à l'intelligence artificielle qui a été élaboré récemment, ainsi que la politique connexe, nous avons été consultés. Nous avons formulé un certain nombre de recommandations — qui n'ont pas toutes été adoptées — et nous poursuivons les consultations pour l'élaboration des procédures.

M. Matthew Green: Afin d'obtenir des précisions sur ce point, selon vous, quelles recommandations importantes n'ont pas été adoptées par le Service de police de Toronto?

Me Patricia Kosseim: Si vous me le permettez, monsieur le président, j'aimerais demander à M. Vance Lockton de répondre à cette question, car il a mené une analyse et a comparé nos recommandations avec la politique définitive.

M. Vance Lockton (conseiller principal en technologie et politique, Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario): Je vous remercie.

Je dirais que les recommandations importantes qui n'ont pas été adoptées dans la politique pourront l'être dans les procédures.

On a beaucoup discuté de l'importance de créer de meilleures définitions des niveaux de risque ou de mieux comprendre la façon dont une partie de la surveillance allait être exercée. Nous avons accepté qu'il est compréhensible que cette politique de haut niveau ne contienne pas ces éléments, mais il sera important de les ajouter aux procédures de mise en œuvre de la politique.

M. Matthew Green: Monsieur le président, j'aimerais poser ma prochaine question à tous les témoins présents aujourd'hui. J'aimerais beaucoup connaître leur analyse sur l'intelligence artificielle — ils pourraient peut-être la fournir par écrit au Comité — en ce qui concerne les changements chez les extrémistes violents à motivation idéologique et la façon dont les algorithmes et les médias sociaux influencent le contexte social. Je fais référence aux récentes perturbations survenues ici, dans la capitale nationale, ainsi qu'à d'autres cas partout au pays.

Je vous remercie.

Le président: Je vous remercie.

La parole est maintenant à M. Bezan. Il a cinq minutes.

M. James Bezan: Ma question s'adresse aux trois commissaires.

Je pense qu'il est entendu qu'il y a certains cas où nous voulons utiliser la technologie de reconnaissance faciale pour l'application de la loi par la police. Mais devrait-on interdire les moyens par lesquels ces images sont obtenues, par exemple en écumant les médias sociaux?

M. Daniel Therrien: C'est la question que nous avons examinée dans le cas de Clearview. S'il s'agit d'un type de situation ou de circonstance dans laquelle la police devrait pouvoir utiliser la reconnaissance faciale et se fier à une technologie appartenant à un partenaire du secteur privé, nous pensons que la police devrait s'assurer que ce partenaire du secteur privé agit conformément à la loi. Par exemple, il ne serait pas légal d'extraire des données des médias sociaux et d'Internet sans tenir compte des paramètres de confidentialité des utilisateurs. Cela ne devrait pas être possible, même dans le cas d'un crime grave.

● (1225)

Me Patricia Kosseim: Je suis d'accord.

J'ajouterais simplement, au nom de tous les commissaires fédéraux, provinciaux et territoriaux, que la surveillance de masse est l'élément qui nous inquiète le plus. Qu'elle soit effectuée par une tierce partie du secteur privé au nom d'un service de police ou par un service de police lui-même, c'est un élément que nous avons souligné comme étant particulièrement inquiétant.

M. James Bezan: Madame Poitras, souhaitez-vous formuler des commentaires?

[*Français*]

Me Diane Poitras: Pour ma part, je n'ai rien à ajouter à ce que mes deux collègues ont dit. En effet, la surveillance de masse peut se faire autant par les autorités policières que par les compagnies privées, par toutes sortes de moyens, y compris la surveillance numérique, mais cela ne devrait pas se faire.

[*Traduction*]

M. James Bezan: Y a-t-il des exemples clairs de violation des droits garantis par la Charte parmi les poursuites intentées contre des individus sur le fondement de la technologie de reconnaissance faciale au Canada?

M. Daniel Therrien: Non, je ne connais aucun cas de ce genre.

M. James Bezan: Y a-t-il des exemples en Ontario?

Me Patricia Kosseim: Je ne connais aucun exemple dans cette province non plus.

Il faudra attendre longtemps avant d'en arriver au point où il y aura une jurisprudence en vertu de la Charte. C'était le point qui nous préoccupait, et c'est ce qui nous a poussés à recommander l'adoption d'un cadre législatif et, dans l'intervalle, l'élaboration de lignes directrices pour aider à atténuer les risques.

Il faudra peut-être plusieurs années avant d'avoir une jurisprudence en vertu de la Charte.

M. James Bezan: Y a-t-il des exemples au Québec?

[*Français*]

Me Diane Poitras: Je n'ai pas d'exemples à vous donner.

[*Traduction*]

M. James Bezan: J'apprécie les quatre recommandations pour aller de l'avant avec les mesures législatives et les lignes directrices proposées par l'Ontario. Commissaire Kosseim, nous sommes très reconnaissants de cette contribution.

Une partie de ma question concerne la Loi sur la protection des renseignements personnels et la LPRPDE, mais lorsque vous parlez de la common law et du droit législatif utilisé dans les affaires criminelles, j'aimerais savoir quelles parties du Code criminel nous allons modifier pour rendre l'utilisation de la technologie de reconnaissance faciale conforme à la Charte.

M. Daniel Therrien: Je vais revenir à l'une de vos questions précédentes.

Si, dans certaines circonstances, on exigeait un mandat délivré par un tribunal, nous serions probablement dans une situation où ces modifications seraient apportées par l'entremise du Code criminel. Je n'ai pas beaucoup réfléchi à l'instrument global. Il est important que la loi soit adaptable, et donc fondée sur des principes, et il faut déterminer les utilisations qui sont permises et celles qui sont interdites. Donc, si on souhaite entrer dans des mécanismes tels que les mandats, le Code criminel serait peut-être justifié.

Pour ajouter à ce que disait ma collègue, la commissaire Kosseim, à propos de l'évolution de la loi — ce qui prend du temps —, nous avons actuellement un ensemble disparate de lois qui régissent la reconnaissance faciale. Nous avons la Charte au plus haut niveau. Nous avons la common law. Nous avons certaines lois, notamment des lois sur la protection de la vie privée, mais nous avons aussi d'autres lois. C'est donc un réseau complexe de lois.

Nous n'avons pas vu beaucoup d'exemples de l'utilisation de la technologie, mais grâce à l'utilisation de Clearview par la GRC, nous avons constaté que l'utilisation de la technologie par les services de police est parfois discutable.

Ce que j'essaie de dire, c'est qu'il faut agir assez rapidement, parce qu'entretemps, cet ensemble de lois peut être utilisé de nombreuses façons.

● (1230)

Le président: La parole est maintenant à Mme Saks. Elle a cinq minutes.

Mme Ya'ara Saks (York-Centre, Lib.): Je vous remercie, monsieur le président.

J'aimerais remercier tous les témoins qui comparaissent aujourd'hui. Ce processus d'apprentissage est très instructif.

Je serais heureuse que les trois témoins répondent à ma prochaine question.

Vous avez tous parlé de la nécessité de se doter de pouvoirs de vérification forts et indépendants en matière de surveillance dans le cas des processus qui utilisent la technologie de reconnaissance faciale, en particulier lorsqu'il s'agit des organismes d'application de la loi. Des représentants de la GRC et du Service de police de Toronto ont comparu brièvement la semaine dernière, et ils nous ont parlé de l'évaluation des risques et des conditions d'utilisation.

Quels sont les mécanismes ou les recommandations proposées sur la question de savoir qui détermine le niveau de risque qui justifie l'utilisation? Je suis heureuse que des recommandations aient été formulées, mais les détails sur la façon dont cela serait fait sont plutôt limités. L'évaluation des risques pourrait se faire en fonction des besoins immédiats. C'est presque comme si nous allions évaluer si l'utilisation était justifiée après coup.

M. Therrien pourrait peut-être répondre en premier.

M. Daniel Therrien: Nous revenons à la complexité de l'élaboration de la loi.

Prenons l'exemple d'un crime grave qui, selon nos recommandations, permettrait à la police d'utiliser la reconnaissance faciale. La loi ne peut pas prévoir tous les cas individuels. Comme vous le dîtes, un service de police devra, dans ce cas, mener une évaluation de la gestion des risques.

Qu'est-ce qui fait partie de la discussion avec l'organe de surveillance, y compris les commissaires à la protection de la vie privée? Je pense que cela commence par une discussion avant la mise en place du programme, c'est-à-dire une évaluation des facteurs relatifs à la vie privée. Comment évaluera-t-on le risque dans certaines circonstances?

Ensuite, si la police souhaite mettre sur pied un programme, nous pensons qu'il faudrait une autorisation dans le cadre du programme. Par exemple, la police décrit un programme qui vise à assurer la protection de personnes très importantes dans les espaces publics. C'est l'objectif du programme. La police et le Commissariat à la protection de la vie privée discutent de ce programme avant l'utilisation de la technologie. Une fois que la technologie est adoptée et effectivement utilisée, le cadre de surveillance devrait inclure le pouvoir d'enquêter sur les plaintes et de rendre des décisions sur la légalité de l'utilisation de la technologie dans un cas donné.

Mme Ya'ara Saks: Je vous remercie.

Pour en revenir à la question de la transparence, lorsqu'une évaluation des risques est effectuée et que le niveau de risque détermine que la technologie de reconnaissance faciale doit être utilisée, selon vous, cela devrait-il faire l'objet d'une transparence publique, qu'il s'agisse des organismes d'application de la loi ou…? Nous allons bientôt aborder les environnements commerciaux.

Tous les témoins peuvent répondre à cette question.

Me Patricia Kosseim: Je vous remercie de votre question.

Pour répondre directement à votre dernière question, nous croyons qu'un certain niveau de transparence est absolument essentiel. Nous comprenons qu'il ne sera pas possible de faire preuve de transparence pour chaque utilisation précise, mais la transparence devrait certainement s'appliquer aux programmes, notamment dans les évaluations des facteurs relatifs à la vie privée — si ce n'est pas dans leur intégralité, au moins sous forme de résumé des évaluations des facteurs relatifs à la vie privée.

En ce qui concerne votre question précédente sur la surveillance, je pense qu'il existe de multiples façons d'exercer cette surveillance sans passer par un examen législatif complet. Cela comprend les commissions qui jouent un rôle important en matière de surveillance, l'autorité provinciale en matière de protection des données, y compris mon bureau et mes collègues, ainsi que le public. La Commission ontarienne des droits de la personne, par exemple, dans ma province, a joué un rôle important en consultation avec notre organisme et d'autres intervenants dans l'élaboration d'un programme de caméra corporelle qui a été adopté.

Je pense qu'un processus de consultation multilatérale doit avoir lieu pour déterminer l'éventail complet des risques. Je tiens à souligner un point que nous avons évoqué à plusieurs reprises, à savoir qu'il existe un large éventail de cas d'utilisation, y compris des utilisations administratives de la reconnaissance faciale qui pourraient être acceptables et être adoptées.

● (1235)

Mme Ya'ara Saks: Je vous remercie.

Je sais que je vais manquer de temps et je veux être sûre de pouvoir poser ma prochaine question.

Madame Poitras, j'aimerais vous poser cette question.

Vous avez parlé de consentement, notamment en ce qui concerne l'utilisation commerciale et d'autres contextes. Par exemple, Cadillac Fairview et d'autres entreprises exploitent des espaces publics, mais ce sont des espaces de propriété privée.

Quels types de mécanismes pourrions-nous envisager pour l'exploitation et la gestion de la technologie de la reconnaissance faciale dans ces espaces, tout en nous assurant que le public est informé?

Le président: Pourriez-vous répondre très brièvement, s'il vous plaît?

[*Français*]

Me Diane Poitras: Merci, monsieur le président.

Encore une fois, je pense que les mécanismes peuvent être modulés selon le type d'utilisation. Il y a différentes formes de reconnaissance faciale. Il y a la reconnaissance faciale proprement dite, qui vise à identifier les individus. Toutefois, on emploie parfois le terme « reconnaissance faciale » pour désigner des dérivés de cette technologie, qui peuvent être utilisés à des fins commerciales, par exemple, dans les centres d'achat, où l'objectif n'est pas d'identifier l'individu, mais ses caractéristiques, comme son âge, son sexe, le temps qu'il a passé à regarder...

[*Traduction*]

Le président: Je dois vous arrêter ici, car nous avons largement dépassé le temps imparti. Je pense que nous pourrons peut-être, si tout va bien, terminer notre dernière série de questions juste à temps pour la sonnerie du vote.

La parole est d'abord à M. Villemure.

[*Français*]

M. René Villemure: Est-ce que je dispose toujours de deux minutes et demie, monsieur le président?

Le président: Oui.

M. René Villemure: Merci.

Monsieur Therrien, un peu plus tôt, vous avez évoqué les travaux faits par la Commission européenne. Ceux-ci incluent-ils les entreprises privées, ou portent-ils seulement sur les organisations gouvernementales?

Vous me faites signe qu'ils concernent les deux, d'accord.

Votre document d'orientation peut-il servir d'inspiration également pour les entreprises privées?

M. Daniel Therrien: [*Inaudible*] avec une adaptation selon le contexte.

M. René Villemure: Oui, évidemment.

Aujourd'hui, savez-vous si des entités qui ne sont ni commerciales ni gouvernementales, possiblement criminelles, utilisent la reconnaissance faciale?

M. Daniel Therrien: Nous n'avons pas de renseignements sur cette question.

M. René Villemure: D'accord, merci beaucoup.

Madame Poitras, j'aimerais vous poser la même question.

Savez-vous s'il existe des entités ni commerciales ni gouvernementales, possiblement criminelles, qui utilisent la reconnaissance faciale?

Me Diane Poitras: Je n'ai pas d'information à ce sujet.

M. René Villemure: Merci beaucoup.

Monsieur Therrien, iriez-vous jusqu'à dire que nous pourrions nous inspirer des travaux actuels de la Commission européenne sur la reconnaissance faciale?

Évidemment, il faut tenir compte du contexte, mais ces travaux représentent-ils les meilleures avancées en la matière en ce moment?

M. Daniel Therrien: C'est une loi qui vise à protéger les droits constitutionnels et les droits de la personne. En ce sens, la réponse est oui, tout à fait. Maintenant, est-ce le meilleur modèle? Je ne sais pas si mes collègues seraient tous d'accord, mais je dirais que c'est un très bon modèle.

M. René Villemure: Madame Kosseim, qu'en pensez-vous?

Me Patricia Kosseim: Excusez-moi, je n'ai pas compris de quel modèle vous parlez.

M. René Villemure: Je parle des travaux de la Commission européenne.

Est-ce que vous croyez que c'est une bonne source d'inspiration ou un bon modèle pour nos travaux?

Me Patricia Kosseim: Oui, tout à fait, c'est un bon modèle. Nous pouvons certainement nous en inspirer.

M. René Villemure: Merci beaucoup.

Madame Poitras, qu'en pensez-vous?

Me Diane Poitras: C'est unanime. C'est une bonne source d'inspiration, avec les adaptations nécessaires.

M. René Villemure: D'ailleurs, le Règlement général sur la protection des données, ou RGPD, avait aussi été un bon modèle en ce qui a trait à la protection de la vie privée.

Monsieur Therrien, pour le temps qu'il me reste, avez-vous une dernière remarque à faire?

M. Daniel Therrien: La reconnaissance faciale est une technologie qui, lorsqu'elle est mal utilisée, peut causer des violations très importantes des droits fondamentaux. J'ai entendu des questions qui portaient sur le caractère souhaitable d'une loi flexible et fondée sur les principes. C'est généralement vrai, mais, compte tenu des conséquences de la reconnaissance faciale, je vous encourage fortement à aller au-delà des principes et à prévoir des dispositions particulières.

M. René Villemure: Merci beaucoup.

[*Traduction*]

Le président: Je vous remercie.

La parole est à M. Green pour la dernière série de questions. Il a deux minutes et demie.

M. Matthew Green: Je vous remercie.

Je reviens à la notion de l'utilisation de l'intelligence artificielle par le secteur privé et des tierces parties avec les organismes d'application de la loi. Il y a même eu des allégations d'utilisation politique dans certains cas.

Ma question, par votre entremise, au Commissariat à l'information, est la suivante: avez-vous été en mesure, dans le cadre de votre mandat, d'explorer ou d'étudier l'utilisation de l'intelligence artificielle à des fins néfastes dans le secteur privé, tel que la surveillance des citoyens, le piratage téléphonique et ce genre de choses?

● (1240)

M. Daniel Therrien: Que voulez-vous dire par néfaste?

M. Matthew Green: Je vais vous donner un exemple.

Une poursuite a été intentée contre l'entreprise NSO et son logiciel Pegasus. En effet, ce système a été utilisé pour pirater les téléphones de personnes qui critiquaient l'État d'Israël. Cette technologie a été utilisée de différentes façons. Nous savons que Clearview est un cas particulier, mais il y a certainement le cas de Cambridge Analytica et d'autres cas. Que fait votre bureau pour mieux comprendre l'utilisation néfaste de l'intelligence artificielle dans le cadre de menaces pour la sécurité nationale?

M. Daniel Therrien: Je reviens à mon point général. Oui, nous avons enquêté sur le lien entre Facebook et Cambridge Analytica. Nous avons étudié l'utilisation des données par Cambridge Analytica, dans certains cas pour tenter d'influencer les processus politiques. D'autres utilisations néfastes sont également possibles.

Je pense qu'il est grand temps de cesser de considérer la vie privée comme étant une question de technologie réservée à un petit nombre de personnes et de se pencher sur l'utilisation des technologies, en particulier lorsqu'elles servent à collecter des renseignements personnels, afin d'établir un lien entre ces technologies et les droits fondamentaux et de légiférer en conséquence.

M. Matthew Green: Monsieur le président, en terminant, j'ai hâte de pouvoir étoffer ce point et d'aborder la question des élections à venir à la lumière des allégations qui ont été faites par diverses usines à troll et de différents types d'interventions sociales qui ont eu lieu.

Je ne sais pas si nous aurons le temps d'en parler cette fois-ci…

Le président: Vous avez un peu de temps. Vous pouvez poser une autre question.

M. Matthew Green: D'accord.

Avons-nous la capacité, dans le cadre des lois existantes, de tenir compte de façon adéquate de l'influence politique du secteur privé dans notre contexte social?

M. Daniel Therrien: Les règles sont trop vagues pour offrir le niveau de confiance que les citoyens devraient avoir à l'égard de la collecte de renseignements par de nombreuses parties, y compris le secteur public et le secteur privé. Je pense que le gouvernement reconnaît qu'il est nécessaire de rétablir la confiance dans ce domaine.

À l'heure actuelle, les gens utilisent la technologie parce que c'est pratique. Honnêtement, pour vivre à l'époque moderne, on n'a d'autre choix que d'utiliser la technologie, mais les gens le font avec une certaine méfiance, et il est grand temps que les élus réglementent ces différents éléments.

M. Matthew Green: Je vous remercie de vos témoignages.

Je vous remercie, monsieur le président.

Le président: Je vous remercie. Vous avez parfaitement choisi votre moment pour vous arrêter. En effet, la sonnerie se fait entendre, et je vais donc mettre fin à la réunion. Nous avons eu quatre séries de questions complètes, et je pense donc que nous sommes prêts à mettre fin à la réunion et à participer aux votes à la Chambre des communes.

Merci beaucoup à nos trois témoins. C'était très instructif. Encore une fois, nous vous sommes très reconnaissants.

La séance est levée.