Allocution d'ouverture – Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique – Patricia Kosseim

Le 2 mai 2022

Sous réserve de modifications

- Bonjour, et merci de m'avoir invitée à prendre la parole aujourd'hui.

- Bien que j'ai déjà eu le plaisir de me présenter devant ce Comité, je m'adresse à vous aujourd'hui en tant que commissaire à l'information et à la protection de la vie privée de l'Ontario. Je suis accompagnée de Vance Lockton, conseiller principal en politiques et en technologie de mon bureau.

- J'aimerais m'appuyer sur ce que vous venez d'entendre de la part du commissaire Therrien.

- Bien que les commissaires à la protection de la vie privée du Canada aient recommandé 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 s'en servir.

- Nous avons donc publié un document d'orientation à l'intention des services de police pour minimiser les risques en attendant la mise en place d'un tel cadre législatif eventuel.

- J'aimerais souligner 5 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 être présumé. La reconnaissance faciale nécessite le recours à des données biométriques sensibles. La police doit consulter ses conseillers juridiques pour confirmer qu'elle dispose d'une autorité légale, soit en common law, soit en vertu d'une loi *spécifique* dans la juridiction en question. Elle doit aussi s'assurer que la Charte est respectée et que l'utilisation de la reconnaissance faciale est nécessaire et proportionnée compte tenu des circonstances.

- **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 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 documentées limitant les fins auxquelles on recourt à la reconnaissance faciale, de robustes systèmes de consignation de toutes les utilisations et divulgations connexes, et la désignation claire des rôles et des responsabilités en matière 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 fournisseurs de services respectent toutes leurs obligations en matière de protection de la vie privée.

- **Troisièmement**, les services de police doivent s'assurer de la qualité et de l'exactitude des renseignements personnels utilisés par le système de reconnaissance faciale , afin d'éviter les faux positifs, de réduire les risques de préjugés et de ne pas causer de préjudices à des particuliers, groupes et communautés.

- Pour assurer cette exactitude, il faut mener des essais internes et externes du système de reconnaissance faciale pour déterminer s'il a un effet discriminatoire, et 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'attarder à la transparence et à l'engagement du public.

- Dans le contexte d'enquêtes policières, il n'est pas toujours possible de communiquer publiquement lors de chaque instance spécifique de la reconnaissance faciale. Cependant, il est possible pour un service de police de faire preuve de transparence au niveau du programme, par exemple, en publiant

ses politiques officielles sur le recours à la reconnaissance faciale, en décrivant en langage clair son programme 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, en particulier les représentants des groupes faisant l'objet d'une surveillance policière excessive, doivent être consultés lors de la conception même du programme de reconnaissance faciale, y compris pendant le processus d'évaluation des facteurs relatifs à la vie privée. Compte tenu de l'importance de la réconciliation au Canada, cette consultation doit inclure la participation des peuples 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, en attendant que notre principale recommandation soit adoptée, soit l'établissement éventuel d'un cadre législatif pour régir l'utilisation de la reconnaissance faciale par la police.

- À notre avis, il faut établir des balises claires ayant force de loi pour que les services de police puissent faire un usage approprié de cette nouvelle technologie, dans un cadre transparent susceptible de mériter la confiance durable du public.

- Merci.