Un outil de sensibilisation aux droits humains

Les technologies de reconnaissance faciale

Au service du capitalisme de surveillance

Ligue des droits et libertés

Table des matières

1 – Qu'est-ce que le capitalisme de surveillance

« Mon point de vue est le suivant : qu'il s'agisse de l'antitrust ou du Règlement général sur la protection des données (RGPD), nous n'avons pas encore le type de lois et de paradigmes de réglementation (de chartes, des droits et de structures institutionnelles) dont nous avons besoin pour rendre cet avenir numérique compatible avec la démocratie. Et cela veut dire que nous n'avons pas les outils, les outils juridiques dont nous avons besoin pour suspendre et interdire les mécanismes clés du capitalisme de surveillance. Il est donc essentiel de comprendre ces mécanismes, car, une fois qu'on les a compris, la perspective de les suspendre et de les interdire n'est pas aussi écrasante. »

Source : Shoshana Zuboff : « Nous avons besoin de nouveaux droits pour sortir du capitalisme de surveillance », par Yves Citton, Professeur de littérature et médias, 24 octobre 2020

La reconnaissance faciale est un outil au service du capitalisme de surveillance

Depuis le début du 21e siècle, nous sommes entré-e-s dans une nouvelle ère – celle du capitalisme de surveillance – marquée par la transformation de nos **données personnelles en produits marchands**.

Le capitalisme de surveillance : dernier stade du capitalisme à l'ère numérique

- Le capitalisme se développe en **transformant** toutes les activités humaines et tous les éléments de la vie sur terre **en marchandises** qui peuvent **être vendues et achetées.**
- Or, une **nouvelle source de matière première** qui pouvait être introduite dans la logique du marché est apparue : l'**expérience humaine personnelle**, traduite en données comportementales par des processus informatiques.
- À partir des données personnelles que nous rendons disponibles en échange de services, les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) induisent ou **déduisent des informations** nous concernant que **nous n'avions jamais eu l'intention** ni la conscience de divulguer (orientation politique, personnalité, orientation sexuelle, etc.)
- Avec Facebook, la collecte d'informations s'étend à l'utilisation de points d'exclamation dans des textes et d'émoticônes, des mouvements des muscles des visages, etc. **pour déceler des micro-expressions qui trahissent des émotions, des comportements** - c'est ce qu'on appelle « le surplus comportemental ».
- Ces entreprises s'approprient notre expérience personnelle afin de comprendre et d'influencer nos comportements. C'est ce que Zuboff appelle le commerce de l'avenir humain.

Un cadre réglementaire s'impose

- Aux débuts de la révolution industrielle, il n'y avait pas de lois interdisant le travail des enfants, de syndicats reconnus, de droit de négociation, de droit de grève, de protection sociale des salarié-e-s, etc. Ces protections ont été obtenues après plusieurs décennies de lutte.

- De la même manière, nous nous dirigeons vers un avenir numérique sans encadrement de ce développement qui menace les droits et libertés et la démocratie. En cette **3e décennie du capitalisme de surveillance, il y a urgence de s'atteler au travail et d'exiger la mise en place d'un cadre réglementaire avant qu'il ne soit trop tard.**

- Les marchés qui font le **commerce de l'avenir humain devraient être illégaux** – ils entraînent des conséquences néfastes, dangereuses et antidémocratiques, et des préjudices intolérables dans une société démocratique.

- Nous **revendiquons un droit à la protection de l'expérience personnelle.**

- **Non à la reconnaissance faciale** : vous ne pouvez pas prendre mon visage!

Soustrayons **la technologie numérique de l'emprise du capitalisme de surveillance afin de la mettre au service de nos aspirations et qu'elle réponde aux véritables besoins sociaux**.

La revue Droits et libertés consacre un dossier sur le capitalisme de surveillance, consultez le numéro du printemps/été 2022.

2 – Qu'est-ce que la reconnaissance faciale?

La biométrie est la mesure de caractéristiques physiques ou biologiques qui permettent de distinguer un individu d'un autre. L'évolution des technologies permet d'exploiter à des fins biométriques de plus en plus de caractéristiques physiologiques, biologiques et comportementales d'un individu :

- **Physiologiques** – empreintes digitales, iris, rétine, faciès, forme de la main;
- **Biologiques** – ADN, odeur, salive, urine;
- **Comportementales** – écriture, démarche, expressions faciales.

La puissance des ordinateurs, l'existence de réseaux qui permettent de partager de grandes masses de données ainsi que le développement d'algorithmes sophistiqués capables d'analyser ces données (autrement appelée intelligence artificielle) permettent, non seulement de faire autrement des tâches existantes, comme l'**authentification**, mais aussi d'accomplir pour la première fois sur une grande échelle des tâches d'**identification.**

Authentification et identification

- L'**authentification** consiste à s'assurer de la concordance d'une personne avec les données colligées sur un support (passeport, carte d'identité, etc.). C'est ce que fait un douanier lorsqu'il compare un visage à la photo d'un passeport. Cette opération peut maintenant être faite par un algorithme de reconnaissance faciale comme en sont dotés les téléphones qui se déverrouillent à la vue du propriétaire.
- L'**identification** biométrique est la recherche de l'identité d'une personne en comparant les données biométriques de la personne avec celles d'un ensemble de personnes dans une base de données. La capacité d'identifier les individus, de les relier à des banques de données et de partager ces données requiert des systèmes d'identification standardisés, et exploitables par des machines. Les systèmes d'identification biométriques répondent à ces exigences.

Une technique comme la reconnaissance du visage peut être utilisée à distance et donc à l'insu de la personne. Avec la multiplication des caméras dans l'espace public et la prolifération de notre image dans l'espace virtuel, un usage sans contrôle de la reconnaissance faciale ne peut qu'annihiler toute prétention à l'anonymat. L'identité biométrique a aussi la propriété d'être « indélébile ». Nous ne pouvons pas nous départir de nos caractéristiques physiologiques ou biologiques pour passer inaperçu.

Même si la caractéristique physique utilisée par un système biométrique est réputée être unique à cette personne, cela ne signifie pas que les systèmes biométriques sont sans failles. Un système de reconnaissance faciale prend une image du visage au moyen d'un capteur, puis un algorithme la convertit en un identifiant électronique (un code).

Or, d'une fois à l'autre, pour des raisons qui dépendent de la technique utilisée et de la condition de prise de vue, le système ne génère pas exactement le même code pour le même individu. Les concepteurs du système doivent donc prévoir une marge d'erreur dans la comparaison des codes.

Une marge trop étroite engendrera un haut taux de faux rejets (faux négatifs), c'est-à-dire de personnes qui ne sont pas reconnues par le système. Par contre, une marge trop large augmentera le taux de fausses identifications (faux positifs). Le taux d'erreur d'un système d'identification biométrique augmente lorsque la taille de la banque de données augmente.

En 2018, l'American Civil Liberties Union (ACLU) a demandé au système de reconnaissance faciale d'Amazon de comparer les photos des membres du Congrès des États-Unis à une banque de photos de 25 000 personnes associées à des crimes. Le logiciel a faussement identifié 28 membres du Congrès comme étant une des 25 000 personnes de la banque de données. Le taux d'erreur est plus élevé pour les personnes racisées. Les algorithmes sur lesquels se basent les outils actuels de reconnaissance faciale étant façonnés en majorité par des hommes blancs, ces machines intelligentes présentent des biais d'apprentissage qui reflètent ceux de leurs concepteurs : certaines expériences de reconnaissance faciale ont montré plus d'erreurs à l'identification des personnes noires, en particulier les femmes noires. Cela est d'autant plus préoccupant que les personnes racisées sont celles qui sont le plus visées par les systèmes d'identification judiciaires.

Il faut également retenir les risques associés à l'utilisation de données biométriques : risques de vol permanent d'identité, de sécurité reliée à la centralisation des bases de données, de sécurité des réseaux, de discrimination des personnes, de piratage de technologies, etc.

3 – Utilisations de la reconnaissance faciale

Au fur et à mesure du perfectionnement des technologies et des avancées techniques, notamment dans le domaine du numérique et des algorithmes, les utilisations de la reconnaissance faciale se sont multipliées de façon exponentielle en un court laps de temps.

Au-delà des utilisations qui sont déjà connues et avérées, d'autres utilisations pourraient éventuellement être envisagées, dans le secteur public ou encore dans le secteur privé. Elles soulèvent de nombreuses interrogations au regard du respect de la vie privée et de la protection des données personnelles, notamment celles qui sont jugées sensibles.

L'usage de la reconnaissance faciale dans le secteur public

L'usage en vue de l'application de la loi et de la protection de la sécurité nationale

Qu'il s'agisse des corps de police ou des agences de renseignements des gouvernements, la reconnaissance faciale a déjà été utilisée à plusieurs reprises, et pas seulement par des États jugés autoritaires ou dictatoriaux. Bien au contraire, même dans un État comme le Canada, des utilisations contestables de la reconnaissance faciale ont déjà été constatées.

Par exemple, la Gendarmerie royale du Canada (GRC) a déjà fait usage du logiciel *Clearview AI* en recueillant des données biométriques sensibles à l'insu ou sans le consentement des personnes concernées. L'acquisition de deux licences d'exploitation au mois d'octobre 2019 a permis à la GRC d'avoir accès à « une gigantesque base de données photographique que [l'entreprise Clearview] met à la disposition de ses clients (corps policiers, agences gouvernementales, institutions bancaires, etc.) pour identifier des personnes à partir de leurs données biométriques ».

À l'issue de leur enquête sur *Clearview AI*, le commissaire à la protection de la vie privée du Canada, et les commissaires de la Colombie-Britannique, de l'Alberta et du Québec ont conclu en juin 2021 que « l'utilisation par la GRC du logiciel controversé de reconnaissance faciale Clearview AI constitue une ''violation grave'' des droits des Canadiens ».

Parallèlement, la Sûreté du Québec (SQ) a fait appel à la société française Idemia en concluant un contrat en août 2020 consistant en la fourniture de logiciels de reconnaissance facile et d'empreintes digitales. Les policiers provinciaux devraient commencer à utiliser ces outils au cours de l'année 2021, notamment « dans le cadre d'enquêtes criminelles pour comparer des images de caméras de surveillance à une base de données comptant des dizaines de milliers de photos signalétiques (mugshots) de personnes ayant un dossier criminel ou ayant fait l'objet d'enquêtes ».

À Montréal, le manque de transparence du Service de police de la Ville de Montréal (SPVM) a déjà été dénoncé, en regard des risques associés à l'usage de technologies de surveillance invasives. L'utilisation de ces technologies affectent certaines communautés ou groupes de manière discriminatoire sur la base de « la race, l'origine nationale ou ethnique, la couleur, la religion, le sexe, l'âge ou les déficiences mentales ou physiques ».

Dans le cadre d'une manifestation, les participant-e-s seraient susceptibles d'être identifié-e-s par la police à leur insu, quand bien même il n'y aurait aucun motif légal les obligeant à donner leur identité à des policiers. L'utilisation de la reconnaissance faciale combinée au déploiement éventuel de caméras corporelles ouvrirait la porte à encore plus de surveillance policière abusive.

La décision de faire usage de tels dispositifs est bien souvent prise dans le cadre de processus opaques au regard desquels une résistance ou un désaccord de la part de la société civile ne peut pas s'exprimer. La peur et des circonstances exceptionnelles peuvent également être utilisées par les autorités comme des justifications à une surveillance de masse. Le risque d'aboutir à une telle surveillance de masse en raison de l'usage des technologies de reconnaissance faciale sous couvert de sécurité publique a déjà été souligné.

Par ailleurs, au-delà des risques d'atteintes à la vie privée ces technologies sont susceptibles de conduire à une surveillance de masse. Elles peuvent constituer un outil de contrôle au service de l'État par l'exploitation des données biométriques aux fins d'identification des personnes physiques. La dérive ultime est incarnée aujourd'hui par le système de « crédit social » mis en place par la Chine qui permet une surveillance généralisée de la population en raison de la reconnaissance faciale qui y est omniprésente.

Les avancées extrêmement rapides des technologies de reconnaissance faciale, et l'utilisation opaque qui en est faite, ne permettent pas au droit d'offrir un encadrement strict de l'usage de ces outils, ni de prévoir des sanctions dissuasives pour en limiter l'utilisation à des cas d'exception. Ainsi, l'utilisation de ces technologies invasives s'élargit avec comme seule base légale les lois de protection de la vie privée actuelles, et celles-ci sont nettement insuffisantes.

Et même avec des bases légales pour y avoir recours, il y a des risques incontournables, des dérives déjà constatées et des atteintes aux droits et libertés en raison de l'exploitation de données sensibles permettant l'identification des personnes.

Dans le cadre de la sécurité à la frontière et du contrôle de l'accès au territoire, le passeport biométrique devient la norme et la reconnaissance faciale est de plus en plus utilisée par l'Agence des services frontaliers pour vérifier l'identité des voyageurs.

Usages de la reconnaissance faciale par le secteur privé

Dans le domaine privé, les utilisations de la reconnaissance faciale sont également très nombreuses, notamment dans le cadre des services offerts en ligne, la sécurité des appareils mobiles, la sécurité chez soi, les applications dans les commerces de détail et les banques ou encore dans le domaine de la télévision.

Pour ne citer que quelques exemples, ces logiciels peuvent ainsi être utilisés :

- comme un deuxième facteur d'identification afin de sécuriser le processus de connexion à un service;
- afin de donner accès aux applications et à des téléphones intelligents sans mot de passe;
- en vue d'avoir accès à des services en ligne pour lesquels un abonnement a été souscrit;

- afin d'avoir accès à des immeubles qu'il s'agisse d'immeubles de bureau, pour accéder à des événements ou à des installations spécifiques;
- comme un moyen de paiement en vue du règlement des factures à la fois dans les magasins physiques et en ligne;
- comme un mode d'accès sécurisé à un dispositif verrouillé;
- afin de procéder à l'enregistrement à des services offerts aux touristes dans les aéroports ou les hôtels;
- dans le cadre spécifique des réseaux sociaux, afin de suivre les activités numériques d'une personne en l'identifiant sur toutes les images où elle est présente et qui sont mises sur Internet;
- dans les lieux publics comme les centres d'achats, en vue de suivre les activités d'une personne avec l'objectif d'effectuer une analyse comportementale à l'insu de celle-ci.

Les utilisations et les avancées technologiques proposées par le secteur privé qui sont fondées sur les outils de la reconnaissance faciale peuvent être accueillies favorablement par le public, en étant perçues comme des avancées pour la vie en société et comme un moyen de faciliter les activités quotidiennes. Toutefois, c'est une révolution tranquille qui s'opère dans le silence, sournoisement.

Même si ces technologies sont susceptibles d'être perçues comme des avancées, il ne faut néanmoins pas oublier les dérives éventuelles et les violations des droits et libertés auxquelles ces outils peuvent aboutir.

4 – Le cas de *Clearview AI*

En 2013, le Commissaire à la protection de la vie privée du Canada (CPVP) s'inquiétait de ce que « la reconnaissance faciale pourrait devenir la plus envahissante des technologies d'identification biométrique populaires moderne […] » parce qu'elle peut être utilisée à l'insu des individus, à partir d'une banque de photos trouvées en ligne.

Le CPVP rapportait une étude menée en 2011 à l'Université Carnegie Mellon qui démontrait « qu'il est possible d'établir un lien avec l'identité en ligne et hors ligne d'un individu à partir de son visage sans avoir accès à une base de données spéciale ».

Quelques années plus tard, l'affaire *Clearview AI* prouvera, hors de tout doute, le bien-fondé des craintes du CPVP…

L'affaire Clearview

En janvier 2020, le New-York Times levait le voile sur l'application de reconnaissance faciale mise au point par la compagnie *Clearview AI* et susceptible, selon les termes de la journaliste Kashmir Hill, de « mettre fin à la vie privée telle que nous la connaissons ».

Ces révélations ont semé l'émoi au Canada et au Québec et ont conduit, en février 2020, les Commissaires à la protection de la vie privée du Canada (CPVP), de la Colombie-Britannique, de l'Alberta et du Québec, la Commission d'accès à l'information (CAI), à lancer une enquête conjointe en vue d'établir la conformité du dispositif de reconnaissance faciale avec les lois canadiennes sur la protection des renseignements personnels.

L'enquête qui s'est conclue en février 2021 a révélé comment fonctionne le dispositif de reconnaissance faciale commercialisé par *Clearview AI*.

1. L'application prélève les images à partir d'éléments en ligne accessibles au public (dont les médias sociaux) et les emmagasine dans sa base de données.
2. Elle crée des identifiants biométriques (représentations numériques des visages).
3. Elle permet ensuite de télécharger une image pour la comparer à celles de la banque.
4. Finalement elle fournit une liste de résultats (visages qui semblent correspondre) permettant d'être redirigé vers la page source de l'image, et donc éventuellement d'identifier la personne.

Plus de **3 milliards de photos d'individus** (au Canada et ailleurs dans le monde) ont été ratissées sur Internet pour mettre au point ce dispositif de reconnaissance faciale. *Clearview AI* n'a pas cherché à obtenir le consentement des personnes dont les images ont été recueillies. *Clearview AI* prétendait qu'elles étaient du domaine public puisque glanées sur des pages web accessibles sur Internet.

Des corps policiers (48 au Canada, dont la Gendarmerie royale du Canada) et diverses autres organisations, y compris du secteur privé, ont eu recours à ce service pour un essai gratuit.

Rapport d'enquête des Commissaires

Le 3 février 2021, les commissaires ont rejeté les prétentions de *Clearview AI* et ont conclu que :

- *Clearview AI* **devait recueillir le consentement** des personnes dont on a utilisé l'image ;

- l'exception de « renseignements auquel le public a accès » - qui permettrait de se passer du consentement - ne s'applique pas. Le rapport écarte donc l'idée qu'un renseignement personnel, du fait qu'il est accessible sur internet, soit un renseignement en quelque sorte abandonné et dont un tiers pourrait user à sa guise ;

- dans le cas du Québec s'ajoutent le non-respect par *Clearview AI* de l'obligation de déclarer à la CAI la constitution d'une banque de mesures biométriques et l'absence de consentement express des individus fichés à l'utilisation d'un procédé de reconnaissance faciale ;
- de plus *Clearview AI* a recueilli, utilisé et communiqué des renseignements personnels d'individus au Canada à des **fins inappropriées, qui ne peuvent pas être justifiées** par l'obtention d'un consentement.

Sur ce dernier point, les commissaires affirment :

> « Nous constatons que la collecte d'images et la création de dispositifs de reconnaissance faciale biométriques par Clearview, dans le but avoué de fournir un service au personnel des organismes d'application de la loi, et leur utilisation par d'autres personnes au moyen des comptes d'essai, représentent **l'identification et la surveillance de masse de personnes par une entité privée dans le cadre d'une activité commerciale** […] une personne raisonnable ne considérerait pas cette fin comme acceptable, raisonnable ou légitime dans les circonstances » (par. 72 et 73 du rapport d'enquête).

Le rapport des commissaires ordonne à *Clearview AI* :

- de cesser d'offrir, au pays, les services de reconnaissance faciale visés par l'enquête ;
- de mettre fin à la collecte et à l'utilisation d'images et identifiants biométriques recueillis auprès d'individus au Canada ;
- et de supprimer ces images et identifiants.

Sans quoi les Commissaires entreprendront des actions pour obliger *Clearview AI* à respecter les lois fédérale et provinciales sur la protection des renseignements personnels applicables au secteur privé.

L'enquête connexe sur la Gendarmerie Royale du Canada (GRC)

Le 10 juin 2021, le Commissaire à la protection de la vie privée du Canada (CPVP) publiait ses conclusions d'enquête sur l'utilisation par la GRC de la technologie de reconnaissance faciale de *Clearview AI*.

La GRC avait acquis deux licences de *Clearview AI* en 2019. Dans le cadre de l'enquête du CPVP, la GRC a d'abord nié avoir utilisé l'outil de reconnaissance faciale. Puis la liste des clients de *Clearview AI* ayant été divulguée, la GRC a admis qu'elle avait fait usage de l'application de reconnaissance faciale quelques 78 fois.

Or, l'enquête du commissariat révèle plutôt que cette technologie a servi à 521 occasions, et dans 85 % des cas pour des motifs ou objets inconnus. Le CPVP note de graves lacunes du corps policier dans le respect de la *Loi sur la protection des renseignements personnels* et s'inquiète du danger que présente une technologie aussi invasive : « le recours par la GRC à la technologie de reconnaissance faciale pour effectuer des recherches dans d'énormes dépôts de données sur des Canadiens nullement soupçonnés d'actes criminels constitue une importante atteinte à la vie privée […] ».

Le CPVP conclut que l'outil de reconnaissance faciale de *Clearview AI* ayant été jugé illégal, son utilisation par la GRC l'est tout autant :

> « […] la collecte de renseignements personnels sur les Canadiens par Clearview contrevenait aux lois canadiennes en matière de protection des renseignements personnels. Il s'ensuit donc que la GRC a contrevenu à la *Loi* lorsqu'elle a par la suite recueilli ces renseignements personnels illégalement obtenus par Clearview » (par. 86).

Le CPVP n'interdit pas toute utilisation de la reconnaissance faciale par la GRC. Il recommande cependant la mise en place d'un programme de mesures systémiques et de formation « pour assurer le suivi, analyser, examiner et contrôler cette nouvelle façon de recueillir des renseignements personnels, afin de veiller à ce que la collecte soit limitée comme l'exige la *Loi* » (par. 6).

La GRC n'utilise plus la technologie de reconnaissance faciale de *Clearview AI* depuis juillet 2020, moment où cette entreprise a cessé d'offrir ses services au Canada.

La GRC s'est engagée à mettre en œuvre les recommandations du CPVP, tout en refusant de souscrire aux conclusions du rapport et donc de reconnaître qu'elle a agi illégalement…

Le rapport du Commissariat fédéral contient également une version préliminaire du « Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale ». Ce document élaboré avec les commissaires provinciaux vise à « préciser les circonstances et les conditions dans lesquelles l'utilisation de la technologie ne pourrait être acceptable ». Une consultation publique s'est tenue sur ce document jusqu'au 15 octobre 2021.

La Ligue des droits et libertés a déposé un mémoire dans le cadre de cette consultation.

5 – Encadrement légal insuffisant

La reconnaissance faciale ne fait l'objet d'aucun encadrement légal spécifique au pays. Au Québec, la *Loi concernant le cadre juridique des technologies de l'information* impose quelques obligations dans l'utilisation de données biométriques. Ainsi :

- la vérification ou la confirmation de l'identité d'une personne au moyen d'un procédé utilisant des mesures biométriques doit faire l'objet d'un consentement exprès de cette personne (art. 44) ;

- la création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information (CAI) (art.45).

Pour le reste, ce sont les lois générales sur la protection des renseignements personnels qui régissent la reconnaissance faciale. Or, ce cadre est nettement insuffisant.

Les lois de protection des renseignements personnels sont truffées d'exceptions permettant de passer outre au consentement. On peut aussi se questionner sur la valeur de ce consentement.

Par exemple, le consentement est-il vraiment libre s'il est exigé dans le cadre d'une relation d'emploi? Ou encore la personne a-t-elle été bien informée des tenants et aboutissants du système de reconnaissance faciale? De plus en plus d'objets connectés (automobiles, cellulaires, etc.) intègrent cette technologie et l'industrie est en pleine expansion : de quel choix le consommateur dispose-t-il vraiment?

La reconnaissance faciale soulève en outre bien d'autres enjeux que la protection des renseignements personnels. Qu'on pense à la manipulation comportementale, aux atteintes possibles aux droits humains, aux biais discriminatoires des algorithmes et à la nécessaire transparence des systèmes.

Comme l'indique la CAI en septembre 2020 :

> « La Loi sur l'accès et la Loi sur le privé n'ont pas été conçues pour encadrer des pratiques aussi intrusives que la biométrie, dont la reconnaissance faciale, ni pour protéger les citoyens de nouveaux modèles d'affaires de géants du Web, fondés sur la marchandisation des renseignements personnels » (p. 3).

L'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) rappelle de son côté :

> « Or, les lois canadiennes et québécoises datent d'il y a 20 ans et sont loin d'être adaptées à la technologie d'aujourd'hui, a fortiori s'agissant de technologies intrusives comme la reconnaissance faciale dans l'espace public qui peut conduire à la surveillance généralisée et la perte d'anonymat ».

Le projet de loi 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, adopté le 21 septembre 2021 par l'Assemblée nationale, vise à moderniser les lois de protection des renseignements personnels au Québec. Or, il ne contient aucune disposition sur la reconnaissance faciale et il effleure à peine la question des données biométriques.

Tout au plus il assujettit la constitution d'une banque de mesures biométriques à un préavis de 60 jours à la CAI avant sa mise en service. Le mémoire présenté par la CAI déplore que le projet de loi 64 ne prévoit pas d'amélioration significative en ce qui concerne la biométrie malgré l'ampleur des enjeux en cause. La CAI formule quelques recommandations à saveur plutôt techniques et insuffisantes.

Les limites qu'il convient d'imposer à une technologie aussi invasive que la reconnaissance faciale relève du débat de société. A l'instar d'autres groupes, la LDL demande un moratoire sur l'utilisation de la reconnaissance faciale et la tenue d'un débat public transparent sur l'usage de cette technologie liberticide.

6 – Atteintes aux droits

La reconnaissance faciale est un procédé invasif de fouille. Elle peut révéler non seulement l'identité d'une personne, mais aussi faciliter l'obtention de renseignements permettant de la retracer. La reconnaissance faciale émotionnelle vise quant à elle à percer les sentiments et les émotions d'un individu afin d'influencer son comportement.

Ainsi, la reconnaissance faciale peut compromettre l'exercice de nombreux droits et libertés.

Elle mine le **droit à la vie privée**, qui inclut le droit à l'autonomie, à l'anonymat, à la tranquillité et à l'intimité. Elle repose sur une perte de contrôle de l'individu sur son image. Elle peut révéler l'identité d'une personne sans son consentement ; porter ainsi atteinte à sa sécurité physique ou psychologique, ou à sa réputation ; servir à des manipulations de comportements, notamment commerciales ou politiques.

Les risques de préjudices en cas de piratage, de bris de confidentialité ou de fuites dans les banques de données biométriques sont énormes, vu le caractère quasi-irremplaçable de telles données.

La reconnaissance faciale peut avoir un **effet inhibiteur sur l'exercice de nombreux droits et libertés fondamentaux**.

Liberté d'expression, d'association et de réunion : la reconnaissance faciale érode le droit à l'anonymat nécessaire à la participation à la vie démocratique, (manifestations, assemblées publiques, forums en ligne etc.). Elle peut dissuader des personnes, notamment celles issues de groupes ou communautés marginalisées, de participer à de tels évènements et de s'organiser pour la défense de leurs droits.

Droit à l'égalité : les biais discriminatoires que recèlent les outils de reconnaissance faciale peuvent engendrer des erreurs d'identification. « Plusieurs travaux de recherche établissent que les taux d'identification erronée sont significativement supérieurs pour les femmes et les personnes racisées » (p. 28). Les personnes faussement identifiées pourraient faire l'objet d'arrestations injustifiées, d'erreur judiciaire ou se voir refuser l'accès à des lieux ou des services (ex : aéroport). La reconnaissance faciale amplifie en outre le risque de profilage racial et social.

Droits démocratiques : La reconnaissance faciale permet une surveillance de masse qui menace la démocratie. La crainte d'être systématiquement observé et identifié, dans les endroits publics ou en ligne, détruit le sentiment de liberté nécessaire à la prise de parole, à la discussion publique et à la circulation des idées. Elle confère un pouvoir démesuré à son détenteur et « accentuera le fossé économique et social entre ceux qui ont accès à la technologie et les autres ».

7 – Campagnes d'opposition d'ici et d'ailleurs

Ligue des droits et libertés

1) Mémoire transmis au Commissariat à la protection de la vie privée du Canada et à la Commission d'accès à l'information du Québec, dans la cadre de la Consultation sur le *Document d'orientation préliminaire sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale*, 15 octobre 2021.

   Trois usages de la reconnaissance faciale par les services policiers devraient faire l'objet d'une **INTERDICTION IMMÉDIATE** par voie législative :

   1) La surveillance de masse des lieux et endroits publics ;
   2) La surveillance de masse en ligne (plateformes numériques, réseaux sociaux, etc.) ;
   3) L'utilisation de banques d'images constituées par des organismes publics ou ministères.

   De plus, un **MORATOIRE** sur toute autre utilisation de la reconnaissance faciale par les services policiers s'impose jusqu'à l'adoption d'une législation à la mesure des enjeux, fondée sur un débat public informé et transparent.

   Lire le mémoire : https://liguedesdroits.ca/memoire-consultation-cpvp-cai-reconnaissance-faciale-services-policiers-2021/

2) Mémoire déposé à la Commission de la sécurité publique de Montréal, *Étude des technologies de reconnaissance faciale et des lecteurs automatiques de plaques d'immatriculation : Un moratoire s'impose*, 30 octobre 2020.

   La Ligue des droits et libertés considère qu'un moratoire devrait être mis en place sur l'acquisition (à travers, notamment, le processus d'approvisionnement de biens et services) et l'utilisation de ces deux technologies par le Service de police de la Ville de Montréal (SPVM) de même que par tous les autres services municipaux de la Ville.

   La Ville de Montréal devrait faire des représentations en ce sens auprès du gouvernement du Québec, qui est celui qui dispose de l'autorité d'agir à cet effet. Bien évidemment, un moratoire visant l'ensemble du territoire du Québec s'impose également.

   Lire le mémoire : https://liguedesdroits.ca/memoire-reconnaissance-faciale-lapi-csp-montreal-2020/

Open Media et la Coalition pour la surveillance internationale des libertés civiles (CSILC)

Une déclaration, endossée par 31 organisations canadiennes et internationales ainsi que 46 personnalités du domaine de la protection de la vie privée, des droits de la personne et des libertés civiles, a été transmis au ministre de la Sécurité publique, Bill Blair, lors du lancement de la campagne lui demandant :

- de lancer une consultation publique sur tous les aspects de la technologie de reconnaissance faciale au Canada ;
- d'établir des politiques et des lois claires et transparentes réglementant l'utilisation de la reconnaissance faciale au Canada, y compris des réformes de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et la *Loi sur la protection des renseignements personnels* (LPRP).

En savoir plus : https://iclmg.ca/fr/lettre-reconnaissance-faciale/

Campagne en Europe – La Quadrature du Net

> « La reconnaissance faciale change le visage du monde. Il n'est pas nécessaire de renvoyer aux pires dystopies et à *1984* pour voir tout ce que les pratiques actuelles ont de dangereux. On peut même percevoir un changement anthropologique possible dans le rapport avec le visage.
>
> La reconnaissance faciale attribue au visage, non plus une valeur de personnalité, l'expression même de la singularité d'une personne humaine, mais une fonction de dénonciation : le visage ne vaut plus pour lui-même, comme singularité prise avec son épaisseur et son secret, mais comme simple signe en lien avec des bases de données de toutes sortes, qui permettent de prendre des décisions concernant la personne visée, à son insu. »
>
> « Refuser la reconnaissance faciale et inscrire ce refus dans la loi est une première nécessité. »

Poursuivre la lecture : Le vrai visage de la reconnaissance faciale, 21 juin 2019, https://www.laquadrature.net/2019/06/21/le-vrai-visage-de-la-reconnaissance-faciale/

Campagnes aux États-Unis - American Civil Liberties Association (ACLU)

L'ACLU fait circuler une pétition adressée au président Biden :

> *"Face recognition technology is a threat to all our civil liberties and exhibits significant racial, gender, and other biases. I'm urging you to immediately impose a federal moratorium on face recognition technology and prevent state and local governments from using federal funds to purchase it."*

Lire la pétition : https://action.aclu.org/petition/tell-biden-halt-dangerous-face-recognition-technologies

Une pétition semblable adressée aux maires respectifs circule dans plusieurs villes étatsuniennes. Voici celle qui est adressée au maire de Boston :

> *"Face surveillance technology gives the government unprecedented power to track who we are, where we go, what we do, and who we know. It's time for Boston to press pause on the use of this dangerous technology."*

Lire la pétition : https://action.aclu.org/petition/ban-face-surveillance-boston

8 – Des voix s'élèvent contre la reconnaissance faciale

European Digital Rights association (EDRi)

— Un réseau de 44 ONG européennes qui défendent les droits fondamentaux à l'ère du numérique.

L'EDRi et ses membres demandent l'interdiction totale au niveau européen de l'utilisation des technologies de surveillance biométriques dans l'espace public.

Ils ont lancé une campagne « *Reclaim your face* » (Réappropriez-vous votre visage) avec l'appui de 12 organisations européennes.

> « *We are standing up for people's rights to participate in public life – without being treated as potential suspects or experimental test subjects.* » (Nous militons pour le droit des personnes de prendre part à la vie publique sans être traitées comme des suspects potentiels ou des sujets de laboratoire. – notre traduction)
>
> « *We would never accept a person following us constantly, monitoring and assessing who we are, what we do, when and where we move.* » (Nous n'accepterions jamais qu'une personne nous suive tout le temps, surveillant et évaluant qui nous sommes, ce que nous faisons, ainsi qu'où et quand nous nous déplaçons. – notre traduction)

https://www.rtbf.be/info/monde/detail_souriez-vous-etes-identifies-la-reconnaissance-faciale-un-filon-et-un-danger?id=10682924

Commissaire à la protection de la vie privée du Canada

> « Il est tout à fait inacceptable que des millions de personnes qui ne seront jamais impliquées dans un crime se retrouvent constamment dans une parade d'identification policière ».
>
> — Daniel Therrien, commissaire à la protection de la vie privée du Canada, le 3 février 2021.

En savoir plus : https://www.journaldequebec.com/2021/02/03/reconnaissance-faciale-les-pratiques-de-clearview-ai-illegales

Lire le communiqué : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2021/nr-c_210203/

Commission de l'éthique de la science et de la technologie (CEST)

« Dans certains contextes, l'utilisation d'un système de reconnaissance faciale pourrait avoir des effets discriminatoires sur certains groupes d'individus, ce qui va à l'encontre du droit à la non-discrimination [...] Plusieurs études démontrent que la reconnaissance faciale est moins fiable pour établir des correspondances lorsque les personnes visées sont non blanches, ou lorsqu'elles sont des femmes, des personnes âgées ou des enfants. Dans un tel cas, un problème de fiabilité entraîne un problème d'équité et de discrimination potentielle. »

En savoir plus : https://www.newswire.ca/fr/news-releases/un-avis-ethique-sur-la-reconnaissance-faciale-signe-par-des-etudiantes-et-etudiants-du-collegial-879180858.html

Citizen Lab

Rapport (2020) *To Surveil and Predict: A Human Rights Analysis of Algorithmic policing in Canada*

Extrait :

"Facial recognition technology has also been the focus of widespread concern and increasingly decisive action in the United States. As of writing (ndlr. 2020), four cities have banned the use of facial recognition technology by government and law enforcement: Boston and Somerville in the state of Massachusetts, and San Francisco and Oakland in the state of California.

Additionally, in June 2020, the Association for Computing Machinery (ACM) United States Technology Policing Committee (USPTC) publicly called for *"an immediate suspension of the current and future private and governmental use of facial recognition (FR) technologies in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights."*

Major technology players have added their weight to concerns about facial recognition, contributing to a rising tide questioning the value and impacts of the technology. IBM publicly withdrew from any further development or sales of facial recognition technology, citing concerns with racial profiling by police. Microsoft stated that it would refuse to sell its facial recognition technology to police services until there are federal laws in place that regulate its use. Amazon imposed on itself a one-year moratorium on sales of facial recognition technology to police services, ostensibly to "give Congress enough time" to implement regulations. Google has also indicated support for a temporary ban on facial recognition technology. In 2019, Axon Enterprise (formerly TASER) banned facial recognition systems from its body cameras."

Lire le rapport : https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

Contrôleur européen de la protection des données

> “Facial recognition should be banned in Europe because of its “deep and non- democratic intrusion” into people’s private lives” – 23 avril 2021

En savoir plus : https://www.reuters.com/technology/facial-recognition-should-be-banned-eu-privacy-watchdog-says-2021-04-23/

Observatoire international sur les impacts sociétaux de l’IA et du numérique (OBVIA)

Petit guide sur les enjeux de la reconnaissance faciale

> « De façon générale, l’utilisation de la reconnaissance faciale par les services de police dans l’espace public peut donc faire craindre à l’instauration d’une surveillance généralisée des individus, manifestement disproportionnée au regard de l’objectif de maintien de l’ordre public. »

Lire le guide : https://observatoire-ia.ulaval.ca/petit-guide-sur-la-reconnaissance-faciale/

Haut-Commissaire de l’ONU

« La reconnaissance faciale ne devrait pas être utilisée dans le cadre de manifestations pacifiques sans la mise en place de garanties essentielles en matière de transparence, de protection des données et de surveillance », a déclaré Michelle Bachelet, Haute-Commissaire des Nations Unies aux droits de l’homme, dans un communiqué, le 25 juin 2020.

Elle demande par conséquent que la technologie de reconnaissance faciale dans le cadre de manifestations pacifiques fasse l’objet d’un moratoire, jusqu’à ce que les États remplissent certaines conditions en matière de respect des droits humains.

Ces conditions comprennent notamment « une surveillance efficace et indépendante de son utilisation, des lois strictes sur la protection de la vie privée et des données, et une transparence totale quant à l’utilisation des enregistrements d’images et de la technologie de reconnaissance faciale dans le contexte des rassemblements ».

Lire le communiqué : https://news.un.org/fr/story/2020/06/1071702

Association Canadienne des Libertés Civiles (ACLC/CCLA)

La Canadian Civil Liberties Association (CCLA) appelle à un moratoire sur l'utilisation de la technologie de reconnaissance faciale tant que les Canadien-ne-s ne sont pas mieux protégé-e-s par une législation claire et efficace car cette technologie peut entraîner de graves violations du droit à la vie privée et à la sécurité.

La CCLA a participé, avec des organisations de défense des libertés civiles de 12 autres pays, à un important rapport du *International Network of Civil Liberties Organisations* (INCLO) sur l'utilisation abusive de la reconnaissance faciale au Canada et à travers le monde, *Facial Recognition Tech Stories and Rights Harms From Around the World.*

British Columbia Civil Liberties Association (BCCLA)

BCCLA, une importante organisation vouée à la défense des libertés civiles et de protection de la vie privée, appelle le gouvernement fédéral à interdire l'utilisation de la reconnaissance faciale par les agences de renseignement et les force de l'ordre fédérales.

"At a time when society is pushing to address systemic racism in policing, adopting a technology that is known for its racial biases is a move in the wrong direction," says Harsha Walia, Executive Director.

"Now is the time for all levels of government in Canada to enact bans on facial recognition surveillance by law enforcement and intelligence agencies."

03-02-2021

Surveillance Studies Centre - Queen's University

Article "Police and governments may increasingly adopt surveillance technologies in response to coronavirus fears", 23 mars 2020.

> "Government and agencies including law enforcement need to practice extreme caution and openness if measures involve surveillance technologies. There is potential that they may become features of everyday life long after the virus has gone, opening up new areas of use (or abuse) – a phenomenon known as surveillance creep.
>
> Surveillance technologies can come at a cost not only to privacy, but to other political rights and freedoms – their use can cost innocent people the right to live their lives free of surveillance. Marginalized communities are even more vulnerable given their history in being over-policed."

Poursuivre la lecture : https://theconversation.com/police-and-governments-may-increasingly-adopt-surveillance-technologies-in-response-to-coronavirus-fears-133737