Tendances technologiques

Reconnaissance faciale

Architecture d'entreprise, Direction générale du dirigeant principal de la technologie

Version 1.1
Date : 2019-06-25

Shared Services Canada
Services partagés Canada

Canada

Table des matières

Sommaire opérationnel

La reconnaissance faciale est une technologie biométrique servant à établir et à valider l'identité d'une personne. Elle fait appel à une application informatique, ou système de reconnaissance faciale, qui extrait une image numérique d'une photo, d'un cadre vidéo ou d'une numérisation tridimensionnelle et crée une empreinte faciale, soit un ensemble de mesures caractéristiques d'un visage, qui identifie le visage particulier d'une personne aux fins d'authentification. Généralement, l'authentification et l'identification se font par correspondance entre les caractéristiques faciales et les empreintes faciales d'un profil dans une base de données. La technologie de reconnaissance faciale se décline en de nombreuses applications (contrôle d'accès, surveillance et enquêtes criminelles). Elle s'utilise également en combinaison avec d'autres technologies biométriques pour renforcer les mesures de sécurité.

Les grandes sociétés technologiques comme Apple, Google, Samsung, Facebook et Amazon ont commencé à prendre conscience de l'importance que revêt la reconnaissance faciale pour leurs infrastructures de sécurité. Apple a essayé de perfectionner la technologie en y ajoutant la reconnaissance de mouvements. La personne dont le visage est numérisé peut maintenant parler ou bouger pendant la numérisation, et ainsi la reconnaissance faciale peut se combiner avec d'autres mesures de sécurité biométriques comme la reconnaissance vocale. Étant donné que les visages en mouvement peuvent être numérisés, les systèmes de reconnaissance faciale peuvent identifier les gens même dans une foule, et ce, sans intrusion.

Sommaire technique

Les systèmes de reconnaissance faciale peuvent utiliser une image bidimensionnelle ou tridimensionnelle ou une alimentation vidéo pour créer une image numérique, établir l'empreinte faciale et identifier un visage en comparant l'image numérique avec les empreintes faciales dans la base de données. Chaque visage a ses caractéristiques déterminantes que le système marquera comme des points nodaux. Un visage humain peut compter jusqu'à 80 de ces points. Ils constituent des zones d'intérêt sur le visage mesurées par le système. La distance entre les yeux, la largeur du nez et la profondeur de l'orbite en sont des exemples. Ces mesures seront stockées dans une base de données sous forme d'empreinte faciale. Lorsque le système numérise un visage, il compare toutes ces mesures aux profils, soit les empreintes faciales, dans la base de données. Les systèmes de reconnaissance faciale utilisent un algorithme, comme le Facial Recognition Vendor Test, qui permet de prédire s'il y a une correspondance en fonction des points nodaux du visage d'une personne. Habituellement, la technologie suit quatre étapes[*] :

capture – un échantillon physique ou comportemental est capté par le système lors d'une analyse;

extraction – des données uniques sont extraites de l'échantillon, et un modèle est créé;

comparaison – le modèle est ensuite comparé à un autre échantillon;

correspondance – le système décide alors si la caractéristique extraite du nouvel échantillon a une correspondance.

Utilisation au sein des entreprises

La reconnaissance faciale offre une autre forme d'identification et d'authentification biométriques. Plusieurs fournisseurs utilisent la reconnaissance faciale comme outil de contrôle d'accès et d'authentification pour leurs clients ou pour un usage interne. Son application ne se limite pas à la sécurité; la technologie sert également aux soins de santé et à la vente au détail. Bien que la reconnaissance faciale bidimensionnelle ne soit pas aussi précise que d'autres formes de technologies biométriques comme les lecteurs d'empreintes digitales, elle a ses avantages. La personne dont le visage est numérisé ne sait pas nécessairement quand il y a numérisation; ainsi, la technologie peut s'utiliser dans de grandes foules et mettre rapidement en évidence les menaces.

Plusieurs fournisseurs sur le marché actuel emploient la reconnaissance faciale pour leurs nombreuses applications. Par exemple, Amazon a mis au point un système qui permet aux utilisateurs de payer leurs articles à l'aide d'une image exploitable (égoportrait). L'utilisateur peut en effet utiliser un égoportrait dans lequel il se déplace ou prononce une phrase particulière comme mot de passe pour valider son identité lors du paiement d'un article. Le fait que le client doive prononcer une phrase ou faire un mouvement se veut un moyen d'éliminer la possibilité d'utiliser une image bidimensionnelle numérisée de la personne de manière frauduleuse. Amazon Rekognition est un autre produit qui fournit deux ensembles d'API : Amazon Rekognition Image pour les images et Amazon Rekognition Video pour les vidéos. Les deux API effectuent des analyses de détection et de reconnaissance d'images et de vidéos qui procurent de l'information utile à vos applications.

Après avoir acheté Face.com en 2012, Facebook a commencé à utiliser la technologie de reconnaissance faciale pour connecter les utilisateurs par leurs photos. Lorsqu'un utilisateur téléverse une photo, le logiciel suggère automatiquement d'autres personnes à identifier. Lorsqu'on est identifié dans une photo, on peut voir plus de contenu regroupé sur les personnes qui y sont identifiées.

Face ID est une technologie développée par Apple et accessible sur l'iPhone X. Elle offre une authentification intuitive et sécurisée grâce au système de caméra TrueDepth à la fine pointe de la technologie et aux technologies perfectionnées permettant de cartographier avec précision la géométrie du visage. D'un simple coup d'œil, Face ID déverrouille en toute sécurité votre iPhone ou iPad Pro. Vous pouvez l'utiliser pour autoriser des achats sur iTunes Store, App Store et Apple Books, et effectuer des paiements avec Apple Pay. Les iPhone XR, XS et XS Max sont tous équipés de la deuxième génération de Face ID, une version mise à jour du système d'authentification biométrique qui est censée être plus rapide que la version de l'iPhone X.

Utilité pour le gouvernement du Canada

Contrairement au secteur privé, l'utilité des applications d'identification faciale pour le gouvernement est principalement liée à la sécurité, en particulier pour la vérification d'identité et la prévention des fraudes. Par exemple, l'Agence des services frontaliers du Canada a récemment lancé le programme des bornes d'inspection primaire, dans le cadre duquel les passagers qui entrent au pays depuis des aéroports doivent s'enregistrer dans des kiosques libre-service[i]. Ces bornes vérifient l'identité des passagers par la reconnaissance faciale. L'adoption progressive des bornes sans personnel depuis 2015 a augmenté la sécurité tout en réduisant la congestion dans les aéroports. L'entreprise portugaise Vision-Box a installé 130 bornes à l'aéroport international Pearson de Toronto. Les bornes ont été conçues pour effectuer une reconnaissance biométrique en deux étapes : une étape de reconnaissance faciale et une autre de reconnaissance des empreintes digitales. Ces bornes seront également en mesure d'effectuer une reconnaissance de l'iris, une fonction réservée aux personnes inscrites au programme NEXUS.

Les systèmes de reconnaissance faciale sont également utilisés dans les casinos provinciaux pour identifier les visiteurs ayant une dépendance au jeu qui se sont volontairement inscrits sur des listes d'auto-exclusion et les empêcher d'entrer[ii]. Il convient de noter que le système a été élaboré conjointement avec le Commissaire à la protection de la vie privée de l'Ontario afin que soient prises en compte dans la conception par défaut les questions de protection de la vie privée. En temps réel, le système fait une lecture du visage des clients qui entrent dans le casino et compare leurs images à celles des joueurs de la liste d'auto-exclusion. S'il y a correspondance, le système avertit la sécurité, sinon le système supprime automatiquement l'image. L'accès à la base de données est restreint, et les renseignements d'une personne ne sont accessibles que si la personne sur la photo est physiquement sur place.

Passeport Canada utilise un logiciel de reconnaissance faciale depuis dix ans pour comparer les nouvelles photos de passeport à sa base de données afin de prévenir les fraudes. On effectue des comparaisons un à un pour confirmer l'identité d'une personne, ce qui signifie qu'une image récente est comparée à une image déjà dans la base de données qui est associée à l'identité de la personne en question. Les comparaisons un à plusieurs servent à comparer une image à l'ensemble de la base de données de photos d'identité afin de vérifier s'il y a des demandeurs en double ou des personnes ayant plusieurs identités[iii]. Le projet a réussi à mettre au jour des cas de personnes qui tentaient d'obtenir plusieurs passeports. Ce même concept est également utilisé pour les permis de conduire délivrés par les provinces[iv].

Le projet de loi C-309, la *Loi modifiant le Code criminel*, a rendu illégale la dissimulation d'identité (utilisation de masques ou de déguisements) dans les émeutes ou les assemblées illégales[v]. Bien que la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* mentionnent que le consentement doit être obtenu avant la collecte de

renseignements personnels, le projet de loi C-309 permet aux organismes d'application de la loi d'utiliser des logiciels de reconnaissance faciale dans les grandes foules pour mettre au jour l'identité des participants.

Répercussions pour Services partagés Canada

Proposition de valeur

SPC pourrait tirer parti de cette technologie pour offrir la reconnaissance faciale comme service. Cette technologie remplacerait l'actuelle carte de sécurité des employés du gouvernement. Une caméra intelligente saisit instantanément les données biométriques des personnes et les analyse localement, puis ouvre le portail pour accéder au bâtiment. Ce service pourrait réduire les coûts de sécurité récurrents qu'entraîne la présence d'une équipe de sécurité sur place, mais il n'y aura probablement pas d'économies à court terme en raison du coût de développement des applications et d'installation du matériel connexe.

La technologie de reconnaissance faciale est une forme non intrusive de vérification d'identité qui ne se perd pas. Dans la réalité de SPC, on élimine l'obligation pour les employés de transporter des cartes de sécurité. De plus, on empêcherait les personnes non autorisées d'accéder à des installations protégées. L'authentification à deux facteurs avec le visage de l'utilisateur pourrait également s'employer pour accéder à des fichiers protégés ayant des classifications de sécurité supérieures (tels que des documents secrets).

Les fabricants de téléphones intelligents ont de plus en plus tendance à créer des appareils qui peuvent être déverrouillés grâce à la technologie de reconnaissance faciale. Une société d'études de marché de Hong Kong estime que près de 64 % (soit un milliard) de tous les téléphones intelligents expédiés dans le monde entier seront dotés de fonctions de reconnaissance faciale en 2020[vi]. Prenant appui sur cette recherche, SPC pourrait ne distribuer aux employés que des téléphones dotés de fonctions de reconnaissance faciale. Les informations du visage peuvent être associées à un autre type de méthode d'authentification pour créer un processus de vérification en deux étapes pour tous les téléphones intelligents. SPC n'aurait pas besoin d'acquérir de licences logicielles supplémentaires, car ses téléphones seraient déjà dotés de la capacité de reconnaissance faciale. Comme la vérification est effectuée localement (les images de référence sont stockées sur l'appareil en dehors du nuage), les risques de sécurité associés à la technologie de reconnaissance faciale sont minimisés.

La reconnaissance faciale nécessite beaucoup de puissance pour le traitement des images en temps réel, un problème que pourrait résoudre l'informatique en périphérie. Les tâches de prétraitement de l'image peuvent être effectuées par l'appareil qui a pris la photo, ou beaucoup plus près de l'appareil que le centre de données. L'appareil capterait l'image, la balaierait à la recherche de visages puis extrairait

l'information sous forme d'empreinte faciale. Une fois que l'empreinte faciale a été créée, elle est envoyée au serveur principal pour l'authentification, et l'image d'origine est éliminée. Comme le prétraitement de l'empreinte faciale a été effectué à l'extérieur du serveur, ce dernier n'a qu'à vérifier s'il y a correspondance interne avec l'empreinte faciale récente.

Difficultés

La plus grande embûche sur le chemin de la technologie de reconnaissance faciale est la protection de la vie privée. L'une des solutions au problème de confidentialité est l'informatique en périphérie, grâce à laquelle on peut stocker les données biométriques localement et éviter la perte de données et la mauvaise mise en correspondance de données de deux systèmes différents. Il est préférable de stocker les données sous forme d'éléments biométriques (une empreinte faciale par exemple) plutôt que sous forme d'images de visages, qui devraient être détruites une fois l'empreinte collectée; les données d'empreinte faciale ne devraient être stockées, chiffrées et rendues accessibles que si on passe des contrôles de sécurité. De cette façon, on empêche l'utilisation de l'image pour des raisons non autorisées.

Si cette technologie devait être utilisée pour authentifier l'identité de personnes à plusieurs endroits, la puissance nécessaire exigerait la contribution de beaucoup de matériel. Si la technologie de reconnaissance faciale, avec ses millions d'empreintes faciales numérisées, devait être adoptée par au moins un ministère, la puissance nécessaire aux traitements et aux mises en correspondance avec les empreintes faciales dans la base de données serait considérable. De ce point de vue, si SPC devait prendre en charge un tel projet, la puissance requise pourrait provenir d'un nuage privé ou public.

Certains facteurs peuvent également limiter l'efficacité des systèmes de reconnaissance faciale. Si la photo a été prise de profil ou si la qualité de l'image est trop basse, il se peut que le système ne dispose pas d'informations suffisantes pour extraire de l'information et trouver une correspondance. Les coupes de cheveux, la couleur de la peau, le maquillage, les lunettes et les protections faciales comme les masques chirurgicaux peuvent également nuire à la reconnaissance. Compte tenu du fait que ces systèmes font appel à l'intelligence artificielle, il y a aussi la possibilité de leur faire apprendre les mauvaises choses.

Il devrait y avoir un quelconque mécanisme pour récompenser les systèmes de reconnaissance faciale qui établissent de bonnes correspondances, mais si les exemples utilisés pour l'apprentissage ne comptent qu'un groupe démographique bien circonscrit, les systèmes ne pourront pas détecter les autres types de visages. L'absence de diversité dans l'apprentissage crée des biais de reconnaissance à tel point que les systèmes n'auront de facilité que pour identifier des personnes ayant des traits particuliers.

Dans une étude menée par Joy Buolamwini, où trois systèmes de reconnaissance faciale ont été testés pour déterminer le sexe, le taux d'erreur se situait entre 21 et 35 % chez les femmes dont la peau était plus foncée, alors que le taux d'erreur était inférieur à 1 % chez les hommes à la peau claire[vii]. On peut donc se poser des questions sur la fiabilité de ces systèmes. Pour éviter toute discrimination à l'endroit de groupes minoritaires, il faut mettre à l'essai et perfectionner les systèmes de manière à éviter les biais.

Ces systèmes ont également des correspondances partielles, autrement dit qui n'atteignent jamais la pleine certitude, lorsqu'ils effectuent la recherche dans une base de données d'images, par exemple. La possibilité de faux positifs est bien réelle (une correspondance est trouvée, mais ce n'est pas la bonne personne), comme celle de faux négatifs (il y a réellement une correspondance dans la base de données, mais le système ne la trouve pas). De tels risques d'erreur montrent que les systèmes ne devraient être utilisés que par des personnes formées qui en comprennent le fonctionnement et que des procédures devraient être établies lorsqu'il y a correspondance.

En voici un bon exemple concret : le service de police de Toronto utilise le système, mais seulement six agents formés par le FBI peuvent s'en prévaloir, et le système ne génère qu'une liste de candidats. Le système ne peut pas en lui-même servir à arrêter des gens; il doit être utilisé de pair avec d'autres méthodes traditionnelles de collecte de preuves[viii]. Les systèmes d'intelligence artificielle, lorsqu'ils contribuent à la prise de décisions importantes, ne devraient jamais être utilisés seuls sans regard critique ni constituer l'argument central d'une décision.

Pour régler les problèmes de mauvais éclairage ou d'angles trop prononcés, certains systèmes modifient les images pour qu'elles soient plus faciles à lire. Panasonic a créé un logiciel de reconnaissance faciale qui analyse les mouvements, la vitesse et l'éclairage présents dans les vidéos et corrige automatiquement les images fixes qui seraient autrement floues[ix]. Comme le logiciel modifie l'image avant de l'analyser, il augmente le risque de faux positifs. Le fait de retoucher une image avant de l'intégrer à un système de reconnaissance faciale peut modifier l'empreinte faciale analysée et créer un biais dans les résultats de la recherche.

Autre limite, ces systèmes ne peuvent reconnaître que les personnes dont les images sont déjà contenues dans leur base de données. Les systèmes doivent également être capables de déterminer si la personne est réellement devant eux, car les visages ne peuvent être cachés comme les mots de passe. En effet, les systèmes ne sont efficaces que parce qu'il est trop difficile de se faire passer pour un autre. Le système doit ainsi être capable de faire la différence entre une personne réelle et une simple photo.

La technologie de reconnaissance faciale n'a pas encore été réglementée au Canada, et les organisations qui l'utilisent actuellement doivent respecter un cadre

juridique précis. Conformément à la *Loi sur la protection des renseignements personnels* du Canada, les institutions fédérales ne peuvent utiliser les renseignements personnels qu'aux fins auxquelles ils ont été recueillis, et il faut le consentement de la personne concernée avant que ces renseignements puissent être utilisés à une autre fin. Comme l'exige la *Loi sur la protection des renseignements personnels et les documents électroniques*, une organisation doit informer les personnes et obtenir leur consentement concernant l'utilisation de leurs renseignements personnels[x]. Il s'agit là d'un obstacle juridique potentiel pour toute organisation qui voudrait faire une lecture de foule, car chaque personne devrait alors consentir à la collecte et à l'utilisation de son visage (renseignements personnels). Les lois font en sorte que les bases de données contenant des renseignements personnels appartenant à différents ministères du gouvernement du Canada ne peuvent être partagées entre eux à des fins autres que celles qui ont fait l'objet du consentement.

Éléments à considérer

Toute utilisation à grande échelle envisagée par SPC devra être soumise à l'évaluation du Commissariat à la protection de la vie privée. SPC devra également dans tous les cas se conformer à la *Loi sur la protection des renseignements personnels* et à la *Loi sur la protection des renseignements personnels et les documents électroniques*. Il est aussi obligatoire de justifier les utilisations étant donné les intrusions possibles dans la vie privée; le Commissariat à la protection de la vie privée propose à cet effet un test en quatre parties[xi] :

- Est-il démontré que la mesure est nécessaire pour répondre à un besoin précis?
- Cette mesure est-elle susceptible de répondre efficacement à ce besoin?
- La perte au chapitre de la vie privée serait-elle proportionnelle à l'avantage obtenu?
- Existe-t-il un autre moyen moins envahissant qui pourrait permettre d'atteindre le même but?

De plus, les utilisations à grande échelle au sein de SPC, comme dans le cas des systèmes de reconnaissance faciale pour accéder aux bâtiments sécurisés, devraient être soumises au consentement de tous les participants. Des photos de haute qualité avec des expressions faciales neutres devraient également être prises ou tirées de bases de données existantes (comme celle des cartes d'accès). Les répertoires centraux de photos du personnel pourraient également devenir la cible d'attaques de cybersécurité. Une protection maximale devra leur être accordée. Les utilisations de moindre ampleur, comme pour le déverrouillage d'un appareil avec capture faciale, poseraient moins de risques puisque l'information est stockée localement.

Si SPC devait adopter ou créer un logiciel de reconnaissance faciale, le logiciel devrait être testé afin de mettre au jour les biais potentiels. Autrement dit, le logiciel devrait pouvoir reconnaître tout le monde, peu importe le sexe, le type de peau ou l'âge. S'il y a des biais, le logiciel devrait retourner en développement, ce qui pourrait entraîner d'autres coûts. Les applications de reconnaissance faciale achetées d'un fournisseur devraient être étudiées avec soin étant donné que SPC ne saurait pas exactement

comment l'application a été conçue. De plus, il n'existe aucune norme applicable aux produits de reconnaissance faciale, ce qui signifie qu'il n'y a pas de niveau de performance à atteindre avant qu'un produit ne soit mis en marché. Si SPC créait lui-même son logiciel, il saurait intégralement comment il fonctionne et aurait la mainmise sur lui.

Enfin, il est important de tenir compte du contexte juridique applicable à tout système de reconnaissance faciale déployé au sein de SPC. À l'heure actuelle, la technologie n'est pas réglementée et aucune norme de performance n'a été établie pour les développeurs. Le paysage juridique pourrait avoir changé au moment où SPC sera prêt à adopter la technologie. Il pourrait être utile d'évaluer à long terme comment les services actuellement offerts respectent les exigences de protection de la vie privée si on veut bien comprendre les effets potentiels de la technologie de reconnaissance faciale.

Ouvrages de référence

https://en.wikipedia.org/wiki/Facial_recognition_system.

https://www.gartner.com/doc/341020/face-recognition-software-antiterrorism-tool.

https://www.upwork.com/hiring/for-clients/pros-cons-facial-recognition-technology-business/.

https://disruptionhub.com/5-applications-facial-recognition-technology/.

https://findbiometrics.com/solutions/facial-recognition/.

https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition2.htm.

https://www.kairos.com/blog/5-companies-using-facial-recognition-to-change-the-world.

https://www.techemergence.com/facial-recognition-applications/.

https://www.priv.gc.ca/media/1766/fr_201303_f.pdf.

http://www.cbc.ca/news/technology/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344.

https://www.biometricupdate.com/201606/canadian-government-used-facial-recognition-to-detect-passport-fraudsters.

https://www.upwork.com/hiring/for-clients/pros-cons-facial-recognition-technology-business/.

https://www.apple.com/ca/business-docs/FaceID_Security_Guide.pdf.

[*] http://www.ex-sight.com/technology.htm.

[i] Braga, Matthew. 2 mars 2017. *Facial Recognition Technology is coming to Canadian Airports this spring.* Canadian Broadcasting Corporation. Repéré le 17-05-2019 à https://www.cbc.ca/news/technology/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344.

[ii] Elash, Anita et Luk, Vivian. 25 juillet 2011. *Canadian Casinos, Banks, Police use Facial-Recognition Technology.* The Globe and Mail. Toronto, Ontario. Repéré le 21-05-2019 à https://www.theglobeandmail.com/news/national/time-to-lead/canadian-casinos-banks-police-use-facial-recognition-technology/article590998/.

[iii] Mackrael, Kim et Ha, Tu Thanh. 15 mai 2014. *Facial Recognition Program Allows RCMP to Identify Alleged Passport Fraud.* The Globe and Mail. Toronto, Ontario. Repéré le 27-05-2019 à https://www.theglobeandmail.com/news/national/facial-recognition-program-allows-rcmp-to-nab-alleged-passport-fraudster/article18703608/.

[iv] Commissariat à la protection de la vie privée du Canada. Mars 2013. *Reconnaissance faciale automatisée dans les secteurs public et privé.* Gouvernement du Canada. Repéré le 23-05-2019 à https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303/.

[v] Parlement du Canada. 19 juin 2013. *Projet de loi C-309, Loi modifiant le Code criminel (dissimulation d'identité).* Gouvernement du Canada. Repéré le 03-06-2019 à https://www.parl.ca/LegisInfo/BillDetails.aspx?Bill=C309&Mode=1&Parl=41&Ses=1&Language=F.

[vi] Naiya, Pavel. 7 février 2018. *More than one billion smartphones to feature facial recognition in 2020.* Counterpoint Technology Market Research. Hong Kong, Chine. Repéré le 27-05-2019 à https://www.counterpointresearch.com/one-billion-smartphones-feature-face-recognition-2020/.

[vii] Lohr, Steve. 9 février 2018. *Facial Recognition is Accurate, if You're a White Guy.* New York Times. New York, É.-U. Repéré le 29-05-2019 à https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[viii] Burt, Chris. 28 mai 2019. *Toronto police using facial recognition as Canadian government ponders rules.* Biometrics Research Group Inc. Repéré le 29-05-2019 à https://www.biometricupdate.com/201905/toronto-police-using-facial-recognition-as-canadian-government-ponders-rules.

[ix] Panasonic. 20 février 2018. *Panasonic to Launch Face Recognition Server Software Using Deep Learning Technology.* Panasonic Corporation. Kadoma, Japon. Repéré le 15-05-2019 à https://security.panasonic.com/news/archives/686.

[x] Commissariat à la protection de la vie privée du Canada. Mars 2013. *Reconnaissance faciale automatisée dans les secteurs public et privé.* Gouvernement du Canada. Repéré le 23-05-2019 à https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303/.

[xi] Commissariat à la protection de la vie privée du Canada. Mars 2013. *Reconnaissance faciale automatisée dans les secteurs public et privé.* Gouvernement du Canada. Repéré le 23-05-2019 à https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303/.