Commissariat
à la protection de
la vie privée du Canada

# Reconnaissance faciale automatisée

*dans les secteurs public et privé*

Mars 2013

# Table des matières

## Résumé

Nous n'en sommes pas encore au point de pouvoir prendre en photo des gens dans la rue au moyen de notre téléphone intelligent, les identifier et avoir accès à des renseignements à leur sujet. Toutefois, cette réalité n'est peut-être pas si lointaine et on peut en imaginer les répercussions sur nos interactions, nos relations interpersonnelles et la façon dont nous vivons notre vie. Entre autres choses, cela accentuera le fossé économique et social entre ceux qui ont accès à la technologie et les autres. Cela banalisera aussi le recours à la surveillance et à la reconnaissance faciale. Et si le recours à cette technologie devient généralisé, personne ne la remettra en question ni n'imposera de limites quant à ses finalités et à ceux qui l'utilisent.

## Introduction

Le Commissariat à la protection de la vie privée du Canada (CPVP) suit l'évolution de la technologie de reconnaissance faciale depuis de nombreuses années dans le cadre de son intérêt pour la biométrie en général. Il y a près de dix ans, nous avons déterminé que la reconnaissance faciale pourrait devenir la plus envahissante des technologies d'identification biométrique populaires modernes, car le sujet n'a pas à donner son consentement ou même à participer sciemment.

La reconnaissance faciale automatisée consiste à identifier un individu à partir de la géométrie de son visage. Pour que la technologie soit efficace, il faut disposer d'une image numérique de qualité du visage de l'individu en question, d'une base de données d'images numériques d'individus identifiés et d'un logiciel de reconnaissance faciale capable d'établir une correspondance exacte entre l'image d'un individu et une image d'un individu identifié qui est enregistrée dans la base de données.

Parmi toutes les technologies biométriques, la reconnaissance faciale est celle qui imite le plus la façon dont les gens s'y prennent pour identifier les autres, c'est-à-dire en examinant leur visage. Il est extrêmement difficile et coûteux de doter une machine de cette aptitude qui ne nécessite aucun effort de la part des humains. Cela dit, grâce à une convergence de facteurs au cours des dernières années, la reconnaissance faciale est devenue une technologie viable et de plus en plus exacte.

Les images numériques sont désormais omniprésentes en raison de la prolifération des caméras de surveillance, des téléphones intelligents équipés d'un appareil photo et des appareils photos numériques de qualité bon marché. Les dispositifs de stockage à prix modique ont donné lieu à la création de vastes bases de données en ligne renfermant des images d'individus identifiés, par exemple les titulaires de permis de conduire ou de passeport, les personnes possédant une carte d'identité d'employé et celles ayant un casier judiciaire. Les individus ont adopté l'affichage et l'étiquetage des photos en ligne sur des plateformes comme Facebook, Instagram, Picasa et Flickr. En outre, la technologie de reconnaissance faciale a fait l'objet de perfectionnements considérables, notamment au chapitre de l'analyse des images et de l'extraction des données.

Les visages ont été transformés en données électroniques qu'il est désormais possible de regrouper, d'analyser et de classer de façons inédites. Les données d'images du visage sont d'autant plus précieuses et sensibles qu'il s'agit d'une caractéristique de notre corps mesurable de façon unique et d'un élément clé de notre identité.
Certaines applications de cette technologie à des fins de sécurité sont incontestablement bénéfiques, par exemple l'authentification des employés autorisés à avoir accès à une centrale nucléaire. La reconnaissance

faciale a des répercussions telles au chapitre de la protection de la vie privée et des valeurs de la société en général que certains observateurs[1] estiment que cette technologie pourrait sonner le glas de l'anonymat.

Le présent rapport de recherche a pour ambition d'expliquer en termes simples le mode de fonctionnement de la technologie de reconnaissance faciale, d'examiner certaines applications de cette technologie dans les secteurs public et privé, et d'analyser ses répercussions sur la protection de la vie privée.

# Qu'est-ce que la reconnaissance faciale?

## a) Aperçu

La technologie de reconnaissance faciale vise à identifier des individus ou à authentifier leur identité en comparant leur visage avec des visages connus stockés dans une base de données pour trouver une correspondance. Le procédé comprend trois grandes étapes. Premièrement, l'ordinateur trouve le visage dans l'image. Il crée ensuite une représentation numérique du visage d'après la position relative, la taille et la forme des traits faciaux. Enfin, cette « carte » numérique du visage représenté sur l'image est comparée avec les images de visages identifiés qui sont enregistrées dans la base de données, par exemple celle des titulaires de permis de conduire.

On peut avoir recours à la reconnaissance faciale pour confirmer ou découvrir l'identité d'une personne. Des systèmes d'authentification sont utilisés pour contrôler l'accès à des installations ou à des équipements. Au nombre des autres usages, mentionnons la lutte contre la fraude, par exemple pour vérifier si un individu a présenté des demande de passeport sous différents noms. D'autres types de technologies biométriques servent à l'heure actuelle aux fins d'authentification, par exemple la lecture des empreintes digitales et le balayage de l'iris.

L'identification est souvent la finalité des applications de sécurité publique et nationale. Il peut s'agir, par exemple, d'identifier des individus au cours d'une émeute ou d'assurer la sécurité dans des lieux publics à fort achalandage, par exemple un aéroport ou un centre sportif. La reconnaissance faciale convient très bien pour les applications d'identification, car les images du visage peuvent être captées à distance et à l'insu de l'individu. On peut aussi avoir recours à d'autres technologies biométriques, comme la reconnaissance de la démarche ou de la voix, pour identifier les individus à distance et sans leur consentement, mais elles comportent des limites évidentes qui les rendent moins utiles.

## b) Exactitude

Un certain nombre de facteurs influent sur l'exactitude de la technologie de reconnaissance faciale :

- le système peut reconnaître uniquement les individus dont l'image est enregistrée dans la base de données;
- les images doivent être de qualité suffisante pour assurer la fiabilité;
- le seuil de sensibilité du système doit être réglé de manière à éviter un nombre excessif de faux positifs (erreur sur la personne identifiée) ou de faux négatifs (non-détection d'une personne qui aurait dû être identifiée);
- l'éclairage, le port de lunettes, une moustache ou une barbe, le maquillage et l'angle sous lequel les photos sont prises.

L'utilisation d'images 3D, qui permettent de capter l'information sur la morphologie du crâne du sujet, représente une innovation récente dans le domaine de la reconnaissance faciale. Elle rend le système moins vulnérable aux problèmes d'éclairage et permet d'établir une correspondance entre des images prises sous des angles différents.

En 2010, après avoir mis à l'essai[2] divers systèmes de reconnaissance faciale, le National Institute of Standards and Technology des États-Unis a constaté que le meilleur algorithme permettait de reconnaître avec exactitude 92 % des inconnus au moyen d'une base de données de 1,6 million de dossiers criminels.

Selon une étude menée en 2011[3] à l'Université Carnegie Mellon, la technologie de reconnaissance faciale pourrait être utilisée pour identifier des individus dans le monde réel à partir d'images personnelles en ligne. Les chercheurs ont été en mesure d'identifier des inconnus et de trouver leurs renseignements personnels au moyen d'un logiciel de reconnaissance faciale et des profils affichés sur les médias sociaux.

- Dans le cadre d'une expérience, des chercheurs ont utilisé des images accessibles au public apparaissant dans des profils affichés en ligne sur des sites de réseaux sociaux pour identifier des individus dont la photographie apparaissait sur un site de rencontre en ligne populaire où les membres utilisent un pseudonyme. Ils ont réussi à identifier un membre sur dix.
- Dans une deuxième expérience, les chercheurs ont réussi à identifier 31 % des étudiants qui marchaient sur le campus en utilisant les photos de leur profil Facebook.
- Dans une troisième expérience, les chercheurs ont prédit les intérêts personnels des individus et, dans 27 % des cas, les cinq premiers chiffres de leur numéro d'assurance sociale à partir d'une photo de leur visage.

L'étude a montré 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. Les chercheurs considèrent que la reconnaissance faciale de tous les individus en tout lieu et en tout temps n'est pas réaliste pour l'heure en raison des contraintes technologiques (exactitude) et des coûts du traitement informatique des données, mais ils estiment que ces contraintes disparaîtront au fil du temps.

## c) Différence entre la reconnaissance faciale et la détection des visages

La détection des visages, qui consiste à trouver un visage dans une image, est moins précise que la reconnaissance faciale. On n'établit aucune correspondance avec l'image d'un individu identifié.

La technologie de détection des visages est utilisée dans des applications commerciales depuis plusieurs années, par exemple dans les systèmes d'affichage numérique pour déterminer le sexe et l'âge approximatif des passants, ainsi que leur état d'esprit à partir de leur expression faciale, afin de cibler les publicités.

On peut concevoir que les systèmes d'affichage numérique permettront un jour d'identifier les clients en établissant une correspondance entre leur visage et un image enregistrée dans une base de données en ligne, par exemple les profils de réseaux sociaux, pour proposer des publicités mieux ciblées. La Federal Trade Commission des États-Unis[4] émet l'hypothèse que les magasins pourraient, dans le cadre de leur programme de fidélité, commencer à recueillir des photos de clients afin de leur présenter des offres ciblées en fonction de leurs intérêts et de leurs mouvements.

SceneTap est une application mobile qui fait appel à des caméras et à un logiciel de détection des visages pour surveiller la composition démographique générale de la clientèle des bars et des clubs. Une fois qu'ils connaissent l'âge moyen et le ratio hommes-femmes, les utilisateurs de l'application peuvent choisir le lieu où

ils iront prendre un verre. Cette information est également utile aux spécialistes du marketing qui veulent cibler un groupe démographique en particulier sans identifier des individus.

Cependant, tout comme l'affichage numérique, SceneTap pourrait devenir plus envahissant dans l'avenir. En juin 2012, l'entreprise a déposé une demande de brevet[5] faisant état de la collecte de renseignements beaucoup plus détaillés, par exemple la race, la taille, le poids, la beauté physique, la couleur des cheveux, le type de vêtements et le port de la barbe, d'une moustache ou de lunettes. En recueillant suffisamment de renseignements sur un individu, il est parfois possible de l'identifier, ce qui suscite des inquiétudes encore plus grandes en matière de protection de la vie privée.

La console de jeux Kinect de Microsoft peut identifier les utilisateurs. D'ailleurs, sa plateforme publicitaire repose sur sa capacité de déterminer qui se trouve dans la pièce, quel est l'âge des personnes présentes et si elles participent ou non à ce qui se passe à l'écran. Dans certains téléviseurs offerts sur le marché aujourd'hui, on trouve des capteurs similaires qui permettent de connaître la réaction d'un téléspectateur à une émission ou à un film[6].

## Applications de la reconnaissance faciale dans le secteur public

Puisque la technologie de reconnaissance faciale a été conçue à l'origine pour aider les pouvoirs publics à assurer la sécurité et l'application de la loi, il n'est pas étonnant que cet outil soit principalement utilisé par le secteur public. Signalons que ce secteur exploite aussi la plupart des bases de données renfermant des images d'individus identifiés, par exemple les titulaires d'un permis de conduire ou d'un passeport et les personnes ayant un casier judiciaire.

### *Application de la loi et sécurité nationale*

Le lendemain des émeutes survenues à Vancouver en juin 2011 après la finale de la Coupe Stanley, l'Insurance Corporation of British Columbia (ICBC) a offert d'aider la police à identifier les casseurs en analysant les images de l'émeute au moyen d'un logiciel de reconnaissance faciale et en comparant les suspects avec les images stockées dans sa base de données de titulaires de permis de conduire. La commissaire à la protection de la vie privée de la Colombie-Britannique a déterminé qu'ICBC peut utiliser la technologie pour détecter et prévenir les cas de fraude liés au permis de conduire, mais qu'elle ne peut se servir de sa base de données pour aider la police à identifier des suspects. Cette décision repose sur le fait qu'il s'agit d'une finalité différente, dont les clients n'ont pas été avisés[7].

À la suite de ces événements, deux projets de loi émanant d'un député ont été déposés, soit le projet de loi 309, *Loi modifiant le* Code criminel *(Dissimulation d'identité)*, qui a proposé de criminaliser le port d'un masque au cours d'une manifestation illégale. D'aucuns craignent[8] que la nouvelle loi (qui a reçu la sanction royale le 19 juin 2013) ne freine les manifestations, y compris celles qui sont pacifiques.

Aux États-Unis, le Next Generation Identification Program (NGI) du FBI utilise diverses technologies biométriques, y compris la reconnaissance faciale, pour identifier et surveiller « les personnes d'intérêt ». Pour le volet de reconnaissance faciale du programme, qui devrait être pleinement opérationnel à l'été 2014[9], le FBI fusionnera ses propres bases de données de photos consultables et celles des États. La base de données ainsi obtenue renfermera les données biométriques et biographiques de plus de 100 millions d'Américains, sera intégrée aux vastes réseaux de caméras en circuit fermé qui surveillent déjà les espaces publics et commerciaux, par exemple les rues, les parcs de stationnement, les aéroports, les banques et les centres commerciaux, et sera mise à la disposition des différents ordres de gouvernement.

### *Sécurité à la frontière*

Dans le cadre de l'initiative de la sécurité du périmètre, le Canada et les États-Unis ont envisagé d'utiliser des appareils de reconnaissance faciale reliés à des bases de données d'images dans les deux pays pour identifier les individus recherchés ou les personnes ayant un casier judiciaire[10].

En Australie, les services frontaliers utilisent la reconnaissance faciale et les empreintes digitales pour identifier les demandeurs de visa frauduleux[11]. Les fonctionnaires de l'immigration ont aussi recours à la reconnaissance faciale pour lutter contre la fraude en lien avec les visas et détecter les travailleurs illégaux[12]. Cette démarche s'inscrit dans le cadre d'une campagne nationale visant à mettre un frein à l'usurpation d'identité et à l'utilisation de fausses identités à des fins criminelles.

Le Japon met actuellement à l'essai la reconnaissance faciale aux barrières d'immigration automatisées dans ses principaux aéroports afin de comparer automatiquement le visage des voyageurs qui entrent au pays ou en sortent avec leur photo de passeport. Cette technologie vise à accélérer le passage des personnes aux barrières[13].

### *Permis de conduire*

Dans de nombreuses provinces canadiennes, notamment en Ontario, en Colombie-Britannique et au Manitoba, les photos figurant sur le permis de conduire sont adaptées à la reconnaissance faciale. Les autorités utilisent cette technologie au cours de la procédure de demande de permis pour détecter l'usurpation d'identité et la fraude, par exemple pour repérer les individus qui demandent des permis sous différents noms.

### *Casinos*

De nombreux casinos canadiens utilisent la reconnaissance faciale pour repérer les criminels et les tricheurs connus. En outre, dans le cadre des programmes d'auto-exclusion volontaire en vigueur dans plusieurs provinces, notamment en Ontario et en Colombie-Britannique, on a recours à la reconnaissance faciale dans les casinos exploités par les provinces pour interdire l'accès aux personnes ayant fait une demande en ce sens aux casinos, par exemple dans le but de les aider à s'affranchir de leur dépendance au jeu.

En Ontario, des caméras associées à des logiciels de reconnaissance faciale examinent le visage des individus entrant dans les casinos. Elles les comparent avec les images de joueurs ayant demandé leur auto-exclusion qui sont stockées dans une base de données. Ce programme entièrement volontaire permet de reconnaître uniquement les individus ayant donné un consentement explicite. La commissaire à l'information et à la protection de la vie privée de l'Ontario a approuvé[14] le programme parce qu'il possède des caractéristiques qui rehaussent la protection de la vie privée. Les images qui ne correspondent à aucune image stockée dans la base de données sont détruites. En outre, la base de données renfermant les images du visage des joueurs compulsifs est sécurisée au moyen d'un procédé de chiffrement biométrique, si bien qu'il est possible d'avoir accès aux renseignements se rapportant à un individu uniquement lorsque celui-ci est présent en personne.

### *Véhicules aériens sans pilote*

Au Canada et ailleurs dans le monde, les organismes gouvernementaux et ceux chargés de l'application de la loi utilisent de plus en plus des véhicules aériens sans pilote. Plus de 30 000 véhicules aériens sans pilote seront en circulation aux États-Unis d'ici la fin de la décennie[15], ce qui aura des répercussions pour le Canada le long de la frontière. D'après un rapport publié en 2013 par le service de recherche du Congrès américain, « les organismes chargés de l'application de la loi pourraient chercher prochainement à équiper des véhicules aériens sans pilote de dispositifs de reconnaissance faciale ou d'autres technologies de reconnaissance

biométrique douces permettant de reconnaître et de surveiller des individus sur la base de caractéristiques telles que la taille, l'âge, le sexe et la couleur de la peau […] et ces dispositifs permettront bientôt de voir à travers les murs et les plafonds [16] » [traduction]. Le rapport de recherche du CPVP intitulé *Les véhicules aériens sans pilote au Canada* examine de façon plus approfondie les répercussions de ces véhicules sur la protection de la vie privée.

### *Applications militaires*

On prétend que la marine américaine a utilisé des lunettes de style « Robocop » munies d'une petite caméra d'une portée de 12 milles (19,3 km). Ces lunettes captent 400 images par seconde et les comparent avec la base de données d'un ordinateur central renfermant 13 millions d'images de visage[17].

La technologie envisagée par l'armée américaine consiste en une caméra intégrée au viseur des armes et associée à une base de données portable pouvant renfermer plus d'un million d'images. Grâce à cet équipement, les soldats pourraient identifier des terroristes et d'autres ennemis en quelques secondes sur le terrain, et ce, sans réseau à large bande[18].

Une autre application militaire éventuelle fait appel à des robots équipés d'un logiciel de reconnaissance faciale que l'on enverrait sur le champ de bataille pour retrouver les soldats blessés[19].

### *Événements sportifs*

La technologie de reconnaissance faciale fait de plus en plus partie intégrante des mesures de sécurité déployées dans le cadre d'événements sportifs de grande envergure. Lors des Jeux Olympiques de Pékin, en 2008, toutes les personnes qui entraient dans le stade principal devaient se soumettre à une vérification de l'identité à un poste muni d'un dispositif de reconnaissance faciale[20]. On a également eu recours à cette technologie pour les Jeux Olympiques de Londres en 2012 afin de surveiller l'entrée de suspects identifiés. Lors de la Coupe du monde de soccer de 2014, les services de police brésiliens prévoient utiliser des lunettes de style « Robocop » dotées d'une fonction de reconnaissance faciale afin de balayer la foule et de repérer les fauteurs de trouble éventuels. Au dire de certains[21], une caméra intégrée aux lunettes captera jusqu'à 400 images de visage par seconde et comparera les marqueurs biométriques avec une base de données renfermant la photo de 13 millions de criminels connus. La caméra permettrait apparemment d'identifier les individus à une distance pouvant atteindre 50 mètres.

# Reconnaissance faciale et *Loi sur la protection des renseignements personnels*

Jusqu'à présent, l'utilisation de la technologie de reconnaissance faciale par les ministères et organismes fédéraux canadiens a été limitée. Au moment de la publication du présent rapport, le Commissariat n'avait reçu aucune plainte concernant la reconnaissance faciale sous le régime de la *Loi sur la protection des renseignements personnels.* Nous nous sommes toutefois penchés sur la question dans le contexte de la procédure d'évaluation des facteurs relatifs à la vie privée (EFVP).

## a) Évaluation des facteurs relatifs à la vie privée

Depuis 2004, le Commissariat examine les évaluations des facteurs relatifs à la vie privée concernant le projet sur la reconnaissance faciale de Passeport Canada, qui utilise cette technologie afin de détecter la fraude chez les demandeurs. La photo de chaque demandeur est comparée avec celles qui sont enregistrées dans la base de données de Passeport Canada afin de mettre au jour toute irrégularité, comme la présentation de plusieurs demandes de passeport sous des noms différents.

Tout au long de la mise en œuvre du projet, le CPVP a formulé des recommandations et des suggestions à Passeport Canada en vue d'atténuer les risques d'atteinte à la vie privée découlant de ce programme. L'organisme a d'ailleurs mis en œuvre des mesures visant à appliquer un grand nombre d'entre elles. En 2012, le CPVP a formulé les recommandations ci-après à l'intention de Passeport Canada :

- présenter des données statistiques faisant la preuve de la nécessité de mettre en œuvre le programme de reconnaissance faciale;
- surveiller la performance du système de reconnaissance faciale et l'ajuster de manière à réduire le plus possible le risque que certains groupes d'individus soient touchés de façon disproportionnée par des erreurs dans le processus d'établissement des correspondances;
- chiffrer toute l'information enregistrée dans la base de données servant à la reconnaissance faciale.

Au fur et à mesure que la technologie de reconnaissance faciale évoluera, les possibilités de l'intégrer aux programmes de surveillance fédéraux pourraient se multiplier. Par exemple, on pourrait ajouter cette technologie aux systèmes de vidéosurveillance existants, comme ceux utilisés par la Gendarmerie royale du Canada sur la Colline du Parlement, par l'Administration canadienne de la sûreté du transport aérien dans les aéroports et par l'Agence des services frontaliers à tous les postes frontaliers. Le Commissariat continue d'inciter les institutions fédérales à le consulter si elles envisagent d'utiliser la technologie de reconnaissance faciale.

## b) Évaluation de la nécessité

De manière générale, toute institution fédérale qui recueille des renseignements personnels peut le faire uniquement si cette information se rapporte directement à ses programmes ou à ses activités. Le Commissariat encourage les institutions qui envisagent d'avoir recours à la reconnaissance faciale à s'assurer qu'elles pourront justifier clairement une éventuelle atteinte à la vie privée. Pour ce faire, les institutions peuvent se poser les quatre questions qui suivent :

- Est−il démontré que la mesure est nécessaire pour répondre à un besoin précis?
- Répondra−t−elle vraisemblablement efficacement à ce besoin?

- La perte au chapitre de la vie privée serait-elle proportionnelle à l'avantage obtenu?
- Existe–t–il un moyen moins envahissant d'arriver au même but?

## c) Utilisation uniforme

La possibilité de correspondance croisée – c'est-à-dire l'utilisation d'images de visage à une fin différente de celle pour laquelle elles ont été recueillies et sans le consentement de l'intéressé – constitue une autre préoccupation liée à la vie privée. Sous le régime de la *Loi sur la protection des renseignements personnels*, les institutions fédérales ne peuvent utiliser des renseignements personnels qu'à la fin pour laquelle ils ont été recueillis ou dans un but concordant avec cette fin. Mis à part certaines exceptions limitées et précises, il faut obtenir le consentement de l'intéressé pour utiliser l'information à toute autre fin. Puisque les images du visage sont des identificateurs uniques, d'aucuns pourraient être tentés de les utiliser à des fins autres que la fin indiquée à l'origine et d'établir des correspondances entre des renseignements contenus dans différentes bases de données. Par exemple, si un autre organisme gouvernemental se sert à des fins de sécurité nationale des données recueillies par un ministère à des fins d'immigration, cette utilisation pourrait ne pas être appropriée. L'établissement de correspondances entre des renseignements contenus dans différentes bases de données peut aussi donner lieu à l'établissement de profils d'individus plus détaillés.

## d) Accès et conservation

L'enregistrement de l'information sur les images de visage dans des bases de données et la nécessité de mettre en place des contrôles d'accès stricts posent une autre difficulté sur le plan de la protection de la vie privée. La mise en commun de l'information avec d'autres organismes ou gouvernements, notamment les autorités chargées de l'application de la loi, ainsi que le risque de suivi et de surveillance par le gouvernement sans l'autorisation des personnes concernées ou en l'absence de mesures de sécurité ou de supervision appropriées, suscitent des inquiétudes particulières. De surcroît, les ministères et organismes fédéraux devraient mettre en œuvre et respecter des politiques rigoureuses en matière de conservation de l'information et détruire les données dont ils n'ont plus besoin.

## e) Orientation du CPVP en ce qui a trait à la biométrie

Le CPVP a publié, en 2011, un document d'orientation sur l'utilisation de la biométrie, comme la reconnaissance faciale, dans les secteurs public et privé. Ce document, intitulé *Des données au bout des doigts – La biométrie et les défis qu'elle pose à la protection de la vie privée*, propose plusieurs principes visant à atténuer les risques d'atteinte à la vie privée associés aux systèmes biométriques, par exemple :

- enregistrer un résumé des données biométriques, au lieu de l'image proprement dite, pour réduire le risque que ces données soient utilisées à une fin différente et possiblement non autorisée;
- conserver l'information biométrique dans des bases de données locales, et non centralisées, pour réduire le risque que les données soient perdues ou reliées de façon inappropriée aux données contenues dans d'autres systèmes;
- utiliser les données biométriques pour *authentifier* des individus, c'est-à-dire pour confirmer leur identité en établissant une correspondance entre un échantillon biométrique et un échantillon déjà enregistré. Éviter d'utiliser des données biométriques pour *identifier* les individus, en comparant un échantillon biométrique avec tous les enregistrements contenus dans une base de données. La vérification un à un réduit le risque de fausses correspondances et d'atteinte à la sécurité des renseignements personnels.

# Applications de la reconnaissance faciale dans le secteur privé

Des applications commerciales de la reconnaissance faciale ont fait leur apparition sur le marché vers la fin des années 2000. Par exemple, Lenovo a lancé en 2008 une gamme d'ordinateurs portables permettant d'ouvrir une session en utilisant le visage de l'utilisateur au lieu d'un mot de passe. Plus ces appareils deviennent sophistiqués, et plus leur prix baisse. Par exemple, le fabricant de systèmes de vidéosurveillance Gadspot a annoncé[22] qu'il vendrait, pour moins de 150 $, des caméras de sécurité « intelligentes » comportant une fonction de reconnaissance faciale.

## a) Services en ligne

Plusieurs entreprises en ligne utilisent la reconnaissance faciale dans le cadre de certains services ou de certaines fonctions. Facebook, Apple et Google y ont toutes recours pour faciliter l'étiquetage des images à l'aide des noms des individus qui apparaissent sur celles-ci.

La base de données d'images de Facebook est probablement la plus importante au monde. Au milieu de l'année 2011, on estimait que les utilisateurs avaient téléchargé 100 milliards de photos dans Facebook et qu'ils y téléchargeaient environ 250 millions de photos chaque jour[23]. Facebook est en mesure de combiner les données biométriques du visage avec des renseignements exhaustifs sur ses utilisateurs, dont leurs données biographiques, l'information sur leur emplacement et leurs liens avec leurs « amis », ce qui suscite des préoccupations considérables au chapitre de la protection de la vie privée. Comme Facebook compte 1 milliard d'utilisateurs à l'heure actuelle, on pense qu'il pourrait détenir les profils les plus exhaustifs sur un grand segment de la population mondiale. En fait, *The New Yorker* a décrit Facebook comme un annuaire des gens du monde[24].

Voici d'autres services en ligne qui utilisent la reconnaissance faciale :

- Dailymakeover[25] – site Web où les femmes peuvent télécharger leur photo et essayer différents maquillages, vêtements et coupes de cheveux;
- Find Your FaceMate[26] – site de rencontre qui jumelle les utilisateurs en fonction de caractéristiques faciales similaires;
- Doggelganger[27] – service commandité par Pedigree visant à promouvoir l'adoption de chiens. Le logiciel de reconnaissance faciale jumelle des gens qui veulent adopter un chien avec des chiens qui leur ressemblent physiquement.

## b) Sécurité des appareils mobiles

Les spécialistes de la sécurité préconisent de plus en plus l'utilisation de caractéristiques humaines pour permettre l'accès aux appareils mobiles. Ils partent de l'hypothèse que l'on risque de perdre ces appareils ou de se les faire voler, et que l'utilisation de la biométrie pour déverrouiller un appareil réduit le risque d'accès non autorisé aux renseignements qu'il contient. On constate de plus en plus l'inefficacité des codes et des mots de passe, en partie parce que les utilisateurs ne font pas preuve de beaucoup de créativité au moment de les choisir.

Sur les appareils mobiles, la difficulté consiste à avoir un appareil photo de qualité et un puissant processeur capable d'exécuter les algorithmes complexes nécessaires pour la reconnaissance faciale sans épuiser la batterie de l'appareil. Grâce aux avancées technologiques, on est en voie de résoudre ces problèmes.

La technologie de reconnaissance faciale peut être utilisée sur les téléphones intelligents Android et Apple. L'appareil photo du téléphone scanne le visage du propriétaire et le compare avec une image qu'il a créée. Si les deux images correspondent, le téléphone se déverrouille. Vingt pour cent des téléphones intelligents expédiés en 2012 comportaient une fonction de reconnaissance faciale. Selon les estimations, 665 millions de téléphones intelligents et de tablettes en seront munis d'ici cinq ans[28].

### c) Sécurité chez soi

Les systèmes de reconnaissance faciale et de détection des visages sont également utilisés à des fins de sécurité dans le monde réel. La société Gadspot, que nous avons mentionnée plus haut, fabrique des caméras de sécurité bon marché intégrant une fonction de reconnaissance faciale. Par ailleurs, iWatchLife vend des caméras de surveillance intelligentes qui peuvent signaler certains incidents au propriétaire d'une habitation ou d'une entreprise, par exemple si le nombre de personnes présentes à un endroit dépasse une valeur prédéfinie. Cette entreprise d'Ottawa travaille[29] actuellement à l'ajout d'un dispositif de reconnaissance faciale qui pourrait être utilisé pour des fonctions telles que le contrôle d'accès, par exemple pour empêcher qu'un fournisseur de service ne pénètre dans un bureau à domicile.

### d) Applications dans les commerces de détail et les banques

Une entreprise américaine[30] propose un logiciel de reconnaissance faciale que l'on peut intégrer aux guichets automatiques et aux terminaux de point de vente au détail pour permettre l'authentification sécurisée des utilisateurs. Ce logiciel sera compatible avec les caméras de sécurité existantes.

Par ailleurs, une entreprise italienne a développé le mannequin EyeSee, qui est muni d'une caméra cachée ayant l'apparence d'un œil pour recueillir des données telles que l'âge approximatif, le sexe et la race des clients qui circulent dans un magasin. On n'utilise jusqu'à présent que la technologie de détection des visages, mais les applications de reconnaissance faciale[31] pourraient bien devenir une réalité avant longtemps.

Également dans le secteur du commerce de détail, NEC a lancé un service de reconnaissance faciale qui recueille non seulement des données démographiques sur les clients, mais aussi de l'information sur leurs habitudes d'achat, par exemple la fréquence et le moment de leurs visites.

### e) Télévision

Des entreprises comme LG, Samsung et Panasonic ont intégré la reconnaissance faciale à leurs téléviseurs intelligents. Ces appareils proposent des menus d'émissions ou de médias en ligne élaborés en fonction des goûts du téléspectateur. Nielsen, l'entreprise qui détermine les cotes d'écoute des médias, étudie la possibilité d'utiliser des téléphones intelligents pour mesurer les cotes et obtenir plus de renseignements sur les personnes qui regardent les émissions et les publicités[32].

# Reconnaissance faciale et LPRPDE

Au moment de la publication du présent rapport, le Commissariat n'avait reçu aucune plainte concernant la reconnaissance faciale sous le régime de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Cette technologie déclencherait probablement l'application de la LPRPDE si on y avait recours dans le cadre d'une activité commerciale. Nous analysons ci-après les principes essentiels de tout examen de l'utilisation de la reconnaissance faciale par des organisations du secteur privé.

## a) Fins appropriées

La reconnaissance faciale est utilisée dans toute une gamme d'applications – en apparence inoffensives comme l'authentification sur un ordinateur portable ou le contrôle de l'accès aux zones réservées aux personnes autorisées, ou pour le moins inquiétantes comme l'identification des personnes qui entrent dans un magasin. Face à une technologie qui repousse les limites du possible, il est parfois difficile de déterminer quelles sont les applications qu'une personne raisonnable considérerait comme appropriées ou non dans les circonstances. Le cadre d'analyse en quatre points utilisé par le Commissariat sous le régime de la *Loi sur la protection des renseignements personnels* pour déterminer si l'utilisation de la reconnaissance faciale est appropriée pour la fin énoncée s'applique aussi sous le régime de la LPRPDE. On trouvera une analyse approfondie dans le document d'information sur la biométrie intitulé *Des données au bout des doigts*, qui a été publié par le Commissariat.

## b) Consentement

En vertu de la LPRPDE, l'organisation doit informer les individus de toutes les utilisations qui seront faites de leurs renseignements personnels pour que leur consentement soit considéré comme valable. Au fur et à mesure que les capacités technologiques deviendront plus variées et que l'éventail des utilisations éventuelles s'élargira, les organisations pourraient avoir de la difficulté à faire savoir aux individus à quelles fins leur image sera utilisée et par qui. La difficulté d'obtenir un consentement explicite dans un environnement mobile complique encore plus la situation. Puisque l'on peut avoir recours à la reconnaissance faciale à l'insu de l'intéressé et sans son consentement, les organisations pourraient parfois être tentées de ne tout simplement pas en informer les individus, et ces derniers n'auraient aucun moyen de savoir à quelles fins leurs renseignements personnels sont utilisés.

## c) Mesures de sécurité

En vertu de la LPRPDE, les mesures de sécurité doivent correspondre au degré de sensibilité de l'information. Les données des images de visage sont particulièrement sensibles en raison de leur caractère unique et de la possibilité d'établir des liens avec de nombreuses autres données se rapportant à l'individu visé. En cas d'atteinte à la sécurité des renseignements personnels, le risque d'usurpation d'identité sera beaucoup plus élevé du fait qu'il est impossible de modifier les données biométriques comme on le fait pour un mot de passe. C'est pourquoi les organisations qui stockent de l'information associée à la reconnaissance faciale doivent prendre des mesures de sécurité strictes.

## d) Exactitude

Les fausses correspondances continuent de poser problème car la technologie de reconnaissance faciale est encore loin d'être infaillible, particulièrement dans les situations non contrôlées. Ces erreurs pourraient avoir de graves répercussions pour les individus, par exemple en cas d'amalgame de leurs renseignements personnels avec ceux d'une autre personne.

## Autres rebondissements à l'échelle internationale

Le Commissariat n'est pas la seule organisation qui s'efforce de définir des paramètres appropriés pour la mise en œuvre des technologies de reconnaissance faciale.

En mars 2012, le Groupe de travail Article 29 sur la protection des données de l'Union européenne a exprimé son opinion[33] concernant la reconnaissance faciale dans les services en ligne et mobiles en vue d'une réflexion sur le cadre juridique approprié et de la formulation de recommandations pour donner suite à toute une gamme de préoccupations concernant la protection des renseignements. Au nombre des facteurs de risque susceptibles de donner lieu à une atteinte recensés, mentionnons l'absence de consentement, des mesures de sécurité insuffisantes et un manque d'accès individuel. Le Groupe de travail a conclu que la technologie de reconnaissance faciale pourrait sonner le glas de l'anonymat.

En avril 2012, le Groupe de travail a rendu publique une opinion[34] sur les percées réalisées en ce qui a trait aux technologies biométriques. Cette opinion indique qu'il faut obtenir le consentement de l'intéressé pour stocker et utiliser des données biométriques.

Le 15 octobre 2012, à la suite d'une enquête menée par l'agence de la protection des données de l'Irlande, Facebook a désactivé la fonction d'identification des photos par reconnaissance faciale pour les utilisateurs de l'Union européenne. En outre, l'agence de la protection des données de Hambourg a déclaré que Facebook contrevenait aux lois sur la protection des données de l'Union européenne en ce qui concerne l'utilisation de la reconnaissance faciale, et a pris des mesures pour contraindre le réseau social à modifier ses pratiques et à détruire sa base de données d'images de visage recueillies jusqu'alors en Allemagne[35].

À l'automne 2011, le Commissariat a tenu une réunion avec des membres du Groupe de travail Article 29 pour discuter des répercussions de la reconnaissance faciale sur le respect de la vie privée. L'affichage numérique et la fonction de suggestion de noms de Facebook figuraient au nombre des sujets abordés.

La possibilité que la technologie de reconnaissance faciale sonne le glas de l'anonymat préoccupe également la Federal Trade Commission (FTC). En octobre 2012, la FTC a rendu publiques des pratiques exemplaires[36] à l'intention des entreprises ayant recours aux technologies de détection des visages et de reconnaissance faciale. Elle y recommande que les entreprises obtiennent le consentement explicite des clients lorsqu'elles utilisent la reconnaissance faciale pour identifier une personne qui serait autrement restée dans l'anonymat et qu'un consentement explicite soit obtenu pour l'utilisation des données en lien avec la reconnaissance faciale à une fin différente de celle indiquée au moment de la collecte.

En Grande-Bretagne, le commissaire à la surveillance a émis une mise en garde[37] concernant la mise en œuvre, à l'échelle du pays, de caméras en circuit fermé haute définition facilitant une analyse de plus en plus exacte des images, y compris la reconnaissance faciale, ce qui risque de porter atteinte à la vie privée et aux autres droits civils. Il a réclamé une réglementation dans les secteurs public et privé.

# Conclusion

Notre capacité de préserver notre anonymat à la fois en ligne et hors ligne diminue de jour en jour. L'information se rapportant à nos activités est captée dans le moindre détail par des technologies que nous avons intégrées de notre plein gré à notre vie quotidienne et par des technologies auxquelles nous ne pouvons échapper. Des tiers utilisent ces données pour effectuer des analyses, des tris et des classements, et de plus en plus pour nous identifier : le gouvernement et les organismes chargés de l'application de la loi s'en servent pour assurer la sécurité publique et nationale, tandis que les entreprises les utilisent pour maximiser leurs bénéfices. Nos activités en ligne sont de plus en plus associées à notre identité réelle et les tiers s'efforcent d'établir des liens entre notre identité en ligne et hors ligne. Nous contribuons nous-mêmes à cette activité de suivi en vaquant à nos activités quotidiennes accrochés à notre téléphone intelligent et en téléchargeant de l'information à notre sujet et au sujet de nos proches.

La reconnaissance faciale ne semble pas si inimaginable dans cet écosystème. Le rythme des avancées de la technologie et de son adoption par les individus a été extrêmement rapide au cours des dix dernières années. Les chercheurs et les décideurs commencent seulement à combler leur retard dans l'examen des répercussions sur la société de cette voie que nous avons tous empruntée. Qu'arrivera-t-il si nous devons renoncer à l'anonymat?

Dans son essai intitulé *The Virtues of Anonymity*[38], Daniel Solove affirme :

*Il y a tant de choses sombres et visqueuses qui se meuvent sous le voile de l'anonymat que notre premier mouvement pourrait être de nous réjouir lorsque les technologies modernes détruisent l'anonymat. […] Mais la disparition de l'anonymat n'est pas forcément une bonne chose. Malgré tous ses défauts, l'anonymat a de nombreuses vertus. Il confère la liberté d'exprimer des idées impopulaires et de critiquer les gens au pouvoir sans risque de représailles ou d'opprobre. Dans la vie de tous les jours, l'anonymat permet aux gens de faire quantité de choses utiles sans inhibition.* [traduction]

Avec la reconnaissance faciale, le scénario futuriste où l'on peut photographier les gens, à leur insu ou non, et les identifier à partir d'une base de données en ligne devient réalité. Il est ensuite possible de combiner leur nom avec d'autres renseignements affichés sur les sites de médias sociaux, des dossiers des moteurs de recherche sur Internet et d'autres sources, par exemple leurs coordonnées, leur information bancaire, les données sur leurs cartes de crédit, leur cote de solvabilité, leurs habitudes de voyage, leur profil d'acheteur, leurs intérêts et leurs opinions. Autrement dit, les individus, les entreprises et les pouvoirs publics peuvent établir rapidement un profil détaillé à partir d'images de visage et de données en ligne.

On peut difficilement parler des répercussions de la reconnaissance faciale sans se pencher sur les répercussions de la surveillance. La reconnaissance faciale confère une nouvelle dimension à la surveillance du fait qu'elle permet d'identifier les individus beaucoup plus aisément et rapidement. De plus, en l'intégrant avec l'extraction de données, on pourra automatiser le suivi des individus dans le monde réel et relier les activités en ligne et hors ligne.

Ian Kerr et Jennifer Barrigar se sont penchés sur le lien qui existe entre la protection de la vie privée, l'identité et l'anonymat dans notre société de plus en plus réseautée. Ils affirment :

> *À terme, la capacité ou l'incapacité de protéger notre vie privée, de construire notre propre identité, de contrôler l'utilisation de nos identificateurs, de décider par nous-mêmes ce que les autres sauront à notre sujet et, dans certains cas, de dissocier nos actions de nos identificateurs aura de profondes répercussions sur le comportement individuel et collectif. Elle influera sur la mesure dans laquelle les*

*personnes, les entreprises et les pouvoirs publics choisiront de se lancer dans le commerce électronique mondial, les médias sociaux et d'autres éléments importants de la société en réseau. Elle influera aussi sur l'opinion que nous avons de nous-mêmes, la façon dont nous choisirons de nous exprimer, la prise de nos décisions d'ordre moral ainsi que sur notre volonté et notre capacité de participer pleinement aux processus politiques*[39]. [traduction]

La reconnaissance faciale est indubitablement très prometteuse au chapitre de la sécurité publique. Par exemple, les organismes chargés de l'application de la loi peuvent avoir recours aux bases de données publiques ou privées renfermant des images de visage dans le cadre d'enquêtes portant sur des activités criminelles présumées. Toutefois, la reconnaissance faciale représente aussi une grave menace pour la démocratie et pour la société si l'on permet sans discrimination à n'importe qui de l'utiliser et à n'importe quelle fin. Il y aura probablement des répercussions sur la liberté et l'autonomie des gens et leur capacité d'agir et de prendre des décisions en fonction de leurs propres valeurs et convictions. Les individus peuvent être motivés par la crainte de subir des représailles et de se faire remarquer. Dans son article sur les dangers de la surveillance[40], Neil Richards déclare que « la surveillance est nocive parce qu'elle peut nous empêcher d'exercer nos libertés civiles et qu'elle confère à ceux qui surveillent un pouvoir sur ceux qui sont surveillés » [traduction]. Dans le cas de la reconnaissance faciale, le pouvoir tient au fait que les personnes surveillées sont parfois identifiées à leur insu, tandis que ceux qui les surveillent sont généralement anonymes et souvent invisibles.

Du point de vue technique, les systèmes de reconnaissance faciale donnent de meilleurs résultats pour certains groupes démographiques[41]. Si le taux de reconnaissance était plus élevé pour des groupes particuliers, cela pourrait entraîner une surveillance disproportionnée, voire un profilage racial ou de la discrimination. En outre, un trop grand nombre de faux négatifs poserait aussi problème, car il favoriserait un faux sentiment de sécurité en incitant les gens à surestimer l'efficacité du système.

L'accès à une technologie de reconnaissance faciale bon marché pour monsieur et madame tout-le-monde peut avoir pour effet de banaliser la surveillance à long terme. Certes, nous n'en sommes pas encore au point de pouvoir prendre en photo des gens dans la rue au moyen de notre téléphone intelligent, les identifier et avoir accès à des renseignements à leur sujet. Toutefois, cette réalité n'est peut-être pas si lointaine et on peut imaginer les répercussions sur nos interactions, nos relations et la façon dont nous vivons notre vie. Entre autres choses, cette technologie accentuera le fossé économique et social entre ceux qui ont accès à la technologie et les autres. En outre, elle banalisera la surveillance et la reconnaissance faciale à un point tel que personne ne remettra la technologie en question et n'imposera de limites quant à ses finalités et à ceux qui l'utilisent.

Pour l'instant, nombre de gens accepteront peut-être que la reconnaissance faciale serve à des fins de sécurité publique, mais il est à craindre qu'elle ne soit utilisée à mauvais escient pour atteindre d'autres objectifs visés par les pouvoirs publics, par exemple réprimer la dissidence. La protection des données biométriques et leur vulnérabilité au piratage et aux utilisations malveillantes si elles tombent dans de mauvaises mains suscitent également des inquiétudes. La prolifération des utilisations potentielles dictées par l'appât du bénéfice par des organisations du secteur privé constitue aussi une source de préoccupation.

Au sein de notre société, dans la plupart des situations en ligne ou hors ligne, les individus peuvent décider quand divulguer leur identité aux autres. Toutefois, comme les autres sont de plus en plus en mesure d'identifier à son insu ou sans son consentement un individu qui serait autrement demeuré anonyme, nous perdrons irrémédiablement la maîtrise de notre sentiment d'identité – à la fois dans le monde réel et dans le monde virtuel. Avec la prolifération des courtiers de données et des ententes de mise en commun des renseignements entre les pouvoirs publics, nous pourrions bien ne même plus savoir qui a accès à nos

renseignements personnels ou lesquels sont associés à notre identité. Compte tenu de ces répercussions, il faut mettre en place des contrôles rigoureux et accroître la transparence pour garantir que le recours à la reconnaissance faciale est conforme à nos lois sur la protection de la vie privée et aux pratiques que nous considérons tous comme socialement acceptables.

## Références


Acquisti, A., R. Gross et F. Stutzman. *Faces of Facebook: Privacy in the Age of Augmented Reality*, présentation donnée à la conférence Black Hat USA 2011.

Gates, Kelly A. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance,* New York University Press, 2011.

Li, Stan Z. et Anil K. Jain. *Handbook of Facial Recognition*, Springer, 2011.

Nelson, Lisa S. *America Identified: Biometric Technology and Society*, The MIT Press, 2011.

Pepper, Scott R. « Unraveling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future », *Northwestern University Law Review*, 2011.

Pugliese, J. *Biometrics: Bodies, Technologies, Biopolitics*, Routlage, 2010.

# NOTES

[1] Hao Li. « Germany wants to halt Facebook facial recognition », *International Business Times*, 4 août 2011.
[2] Patrick J. Grother, George W. Quinn et P. Jonathon Phillips. *Report on the Evaluation of 2D Still-Image Recognition Algorithms*, National Institute of Standards and Technology, 24 août 2011
[3] Alessandro Acquisti et Ralph Gross. *Faces of Facebook: Privacy in the Age of Augmented Reality*, Carnegie Mellon University, juillet 2011.
[4] *Protecting Consumer Privacy in an Era of Rapid Change*, rapport à l'intention du personnel de la Federal Trade Commission, mars 2012.
[5] Kashmir Hill. « SceneTap Wants To One Day Tell You The Weights, Heights, Races and Income Levels Of The Crowd At Every Bar », *Forbes*, 25 septembre 2012.
[6] Tarun Wadhwa. « What Do Jell-O, Kraft, And Adidas Have In Common? They All Want To Know Your Face », *Forbes*, 8 août 2012.
[7] Office of the Information and Privacy Commissioner for British Columbia. http://www.oipc.bc.ca/investigation-reports/1245, 16 février 2012.
[8] Patrick White. « New bill refines rules on masks in unlawful protests », *The Globe and Mail*, 1er novembre 2012.
[9] Jerome M. Pender. *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law*, Federal Bureau of Investigation, 18 juillet 2012.
[10] « Border workers push for biometric screening in perimeter security plan with U.S. », *SecureIDNews*, 1er juin 2011.
[11] Samantha Maiden. « Biometric security at borders to catch visa fraud », *The Sunday Telegraph*, 1er avril 2012.
[12] Ray Clancy. « Facial recognition software being used in Australia to track down visa fraud », *AustraliaForum.com*, 7 février 2013.
[13] « Test of facial ID recognition system begins at airports », *The Asahi Shimbun*, 7 août 2012.
[14] « OLG and Commissioner Cavoukian announce state-of-the-art Privacy-Protective Facial Recognition System », *PrivacybyDesign*, 12 novembre 2010.
[15] Richard M. Thompson II. *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, rapport du service de recherche du Congrès américain, 3 avril 2013.
[16] *Ibid.*
[17] http://www.cbc.ca/news/canada/british-columbia/story/2011/06/18/bc-icbc-rioters-id.html
[18] Martin Barillas. « New military applications for facial recognition technology », *Spero News*, 2 septembre 2012.
[19] *New first responder*, site de la University of Dayton, 24 août 2012.
[20] *Facial recognition technology safeguards Beijing Olympics*, site de la Chinese Academy of Sciences, 15 août 2008.
[21] Jan Corpus. « 2014 World Cup Will Test Robocop Facial Recognition Technology », *Bit Rebels*.
[22] Stephen Mayhew. « Gadspot to sell security cameras with facial recognition in North America », *Biometric Update*, 10 octobre 2012.
[23] « *How much do you know about Facebook photos*? », blogue Pixable, 14 février 2011.
[24] Jose Antonio Vargas. « The Face of Facebook », *The New Yorker*, 20 septembre 2010.
[25] http://www.dailymakeover.com.
[26] http://findyourfacemate.appspot.com/.
[27] http://www.ourshowroom.co.nz/doggelganger/.
[28] Joel Rai. « In your face », *Business Today*, 5 août 2012.
[29] Ivor Tossel. « Facial-recognition technology needs limits, privacy advocates warn », *The Globe and Mail*, 26 septembre 2012.
[30] « O2 Secure Wireless intros facial recognition integration software for ATMs », *atm marketplace*, 8 février 2013.
[31] Adam Vrankuli. « Facial recognition service profiles customer habits, age, gender », *Biometric Update.com*, 15 novembre 2012.
[32] Steve McClellan. « Nielsen Explores Facial Recognition Tech for Ratings », *MediaPost News*, 22 janvier 2013.
[33] Groupe de travail de l'article 29 sur la protection des données. *Opinion 02/2012 on facial recognition in online and mobile services*, 22 mars 2012.
[34] Groupe de travail de l'article 29 sur la protection des données. *Opinion 3/2012 on developments in biometric technologies*, 27 avril 2012.
[35] Adi Robertson. « Facebook deletes European facial recognition data, satisfying German privacy agency », *The Verge*, 7 février 2013.
[36] Federal Trade Commission. *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, octobre 2012.
[37] Rob Hastings. « New HD CCTV puts human rights at risk », *The Independent*, 3 octobre 2012.
[38] Daniel J. Solove. « The Virtues of Anonymity », *The New York Times*, 20 juin 2012.
[39] Ian Kerr et Jennifer Barrigar. « Privacy, Identity and Anonymity », chapitre adapté d'après *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, 2009.
[40] Neil M. Richards. « The Dangers of Surveillance », *Harvard Law Review*, vol. 126, 2013.
[41] Lucas D. Introna et Helen Nissenbaum. *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, The Center for Catastrophe Preparedness and Response, New York University.