DES DONNÉES AU BOUT DES DOIGTS

La biométrie et les défis qu'elle pose à la protection de la vie privée

INTRODUCTION

Les Canadiennes et les Canadiens sont témoins de l'intérêt croissant que manifestent le gouvernement et certaines organisations du secteur privé quant à l'adoption de systèmes faisant appel aux caractéristiques biométriques pour l'identification ou la vérification automatiques de l'identité des personnes. Scanner le bout d'un doigt, un visage ou un iris permet de réunir des renseignements personnels sur une personne identifiable.

C'est dans cette mesure que cela revêt, pour nous aussi, un intérêt indéniable.

Le présent document, élaboré par le Commissariat à la protection de la vie privée, fait la description de la biométrie et des systèmes faisant appel à cette technologie, expose quelques-unes des répercussions qu'exerce ce secteur émergent sur la protection de la vie privée et présente quelles pourraient être des mesures d'atténuation des risques.

Qu'est-ce que la biométrie?

À l'origine, le mot « biométrie » désigne l'application au domaine de la biologie des mesures utilisées en mathématiques. Il renvoie maintenant à un éventail de techniques, d'appareils et de systèmes permettant aux machines de reconnaître des personnes ou de confirmer ou d'authentifier leur identité.

Ces systèmes mesurent et analysent les attributs physiques et comportementaux des personnes, comme les traits du visage, les inflexions de la voix, les empreintes digitales, les empreintes de la paume de la main, la forme des veines des doigts et de la main, la structure des yeux (iris ou rétine) ou la démarche.

Biométrie populaire

Le gouvernement du Canada est en train d'élargir son utilisation de la biométrie. Par exemple, les programmes frontaliers COMPASS et NEXUS s'appuient sur des images d'iris; on a recours aux empreintes digitales et aux images d'iris pour contrôler l'accès aux zones réservées dans les aéroports; et l'intégration d'une image numérique du titulaire est proposée pour le passeport électronique.

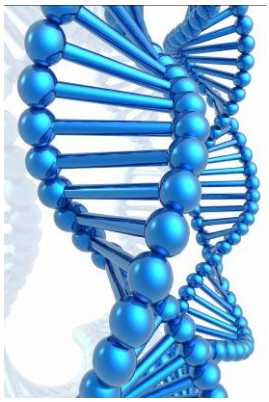
Les données biométriques sont rassemblées à un point de départ que l'on appelle l'inscription. Il est possible, par la suite, d'établir ou de confirmer l'identité lorsque de nouvelles données sont saisies et comparées à celles ayant déjà été emmagasinées.

L'exemple le plus courant de renseignement biométrique est la photo d'identité pour le passeport, le permis de conduire ou la carte d'assurance-maladie. En quelques mots, l'image faciale d'une personne est captée et emmagasinée de sorte que l'on puisse la comparer à une autre photographie ou à la personne que l'on a devant soi.

La technologie biométrique sert généralement à établir l'identité des personnes ou à vérifier si celles-ci détiennent certains privilèges, comme conduire une voiture ou avoir accès à une zone sécurisée ou réservée.

Caractéristiques biométriques

On appelle « caractéristiques biométriques » les traits physiques et comportementaux qui sont enregistrés dans un système biométrique (par exemple le visage, les empreintes digitales ou la voix d'une personne). Contrairement aux renseignements personnels utilisés pour les pièces d'identité conventionnelles (non biométriques), ces caractéristiques peuvent être à la base de systèmes d'identification solides et fiables.



Un grand nombre de caractéristiques biométriques, par exemple, peuvent être très distinctives, si bien qu'il y aura peu ou pas de concordance de ces données d'une personne à une autre. Les empreintes digitales, l'iris et l'ADN figurent parmi les caractéristiques les plus distinctives, tandis que les traits du visage peuvent être partagés entre deux ou plusieurs personnes.

Certains attributs physiques, comme les empreintes digitales et l'iris, ont aussi tendance à demeurer inchangées au fil des ans et à être difficiles à modifier. Cependant, d'autres caractéristiques biométriques, comme le visage, peuvent changer au fil des années et peuvent aussi être modifiées par le maquillage, les déguisements ou la chirurgie.

Les renseignements biométriques sont personnels

Les systèmes biométriques enregistrent des renseignements personnels sur des personnes identifiables. Cela signifie que leur utilisation par le gouvernement fédéral est assujettie à la *Loi sur la protection des renseignements personnels*. Les données biométriques peuvent aussi être réunies, utilisées ou communiquées par des organisations du secteur privé, qui peuvent être assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). La surveillance de la *Loi sur la protection des renseignements personnels* et de la LPRPDE relève du Commissariat à la protection de la vie privée du Canada.

Les préoccupations soulevées par les systèmes biométriques attirent de plus en plus l'attention des commissaires à la protection de la vie privée des provinces et territoires du Canada.

LES DÉFIS EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

La nature particulière des caractéristiques utilisées dans les systèmes biométriques peut poser des défis en matière de protection de la vie privée, des préoccupations que ne présentent pas nécessairement les méthodes traditionnelles d'identification, telles que les pièces d'identité.

Collecte secrète

> ***Principe relatif à la protection de la vie privée***
> Les gens devraient savoir qu'on réunit des renseignements à leur sujet.

Un de ces enjeux est la collecte et l'utilisation secrètes de données biométriques, du seul fait que les données sont accessibles au public.

Les données faciales, par exemple, peuvent facilement être recueillies en photographiant les gens à leur insu. Il est également facile de saisir des empreintes digitales à l'aide des empreintes latentes laissées par les gens lorsque ceux-ci touchent des surfaces dures. Les nouveaux systèmes de balayage de l'iris peuvent aussi saisir subrepticement des images des yeux jusqu'à deux mètres de distance. De la même façon, les réseaux de veines des paumes de la main et des doigts peuvent être saisis lorsque les gens passent la main sur des appareils d'enregistrement cachés.

Comparaisons

La collecte de traits biométriques à une fin donnée et l'utilisation de ceux-ci à l'insu d'une personne et sans son consentement à une autre fin constituent une autre préoccupation relative à la protection des renseignements personnels.

Dans le domaine de la biométrie, le risque d'utilisations multiples découle du fait que certaines caractéristiques, comme les empreintes digitales, sont relativement permanentes et très distinctives, ce qui en fait un élément d'identification très pratique à la fois constant et universel.

> ***Principe relatif à la protection de la vie privée***
> Les renseignements personnels ne doivent être utilisés qu'aux fins pour lesquelles ils ont été recueillis.

Une fois l'élément d'identification saisi et emmagasiné dans une base de données, il est facile d'y avoir accès et de le comparer à des échantillons futurs, même si ceux-ci sont réunis dans des contextes complètement différents.

Bien que les citoyennes et les citoyens soient souvent favorables à de telles comparaisons lorsque les services policiers utilisent les empreintes digitales pour localiser des suspects, la même technique peut aussi priver des gens au-dessus de tout soupçon de leur droit de vivre leur vie dans l'anonymat et de ne pas faire l'objet d'une surveillance.

Renseignements secondaires

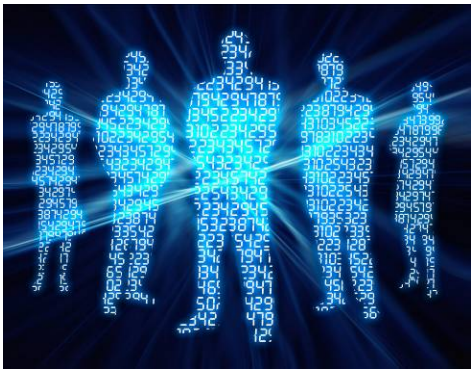
Du point de vue de la protection de la vie privée, les renseignements secondaires que l'on peut trouver dans les caractéristiques biométriques ayant été recueillies à une fin primaire différente suscite également des inquiétudes.

Par exemple, les images d'iris servant dans les systèmes de vérification de l'identité peuvent communiquer des renseignements supplémentaires au sujet de la santé d'une personne, tandis que l'usure des empreintes digitales d'une personne peut donner une idée du métier qu'elle exerce ou de sa situation socioéconomique.

L'exemple le plus éloquent est l'ADN, qui sert non seulement à identifier une personne unique mais aussi à révéler un large éventail de renseignements sur sa santé.

> ***Principe relatif à la protection de la vie privée***
> Les renseignements personnels ne doivent être recueillis qu'à une fin clairement définie.

CONCEPTION D'UN PROJET BIOMÉTRIQUE



Le Canada ne dispose actuellement d'aucune politique sur l'utilisation de la biométrie par le gouvernement ou le secteur privé. Par conséquent, il n'existe aucune norme relative à la protection de la vie privée, à l'atténuation des risques ou à la transparence publique.

Le Commissariat à la protection de la vie privée du Canada est cependant convaincu qu'un grand nombre de méthodes permettant de renforcer les mesures de sécurité dans d'autres domaines, dont l'usage est très répandu, devraient aussi s'appliquer aux initiatives liées à la biométrique.

Protection proactive de la vie privée

D'abord et avant tout, il est essentiel que tout gouvernement ou que toute organisation du secteur privé qui propose une mesure pouvant exercer des répercussions sur les renseignements personnels tienne compte de la protection de la vie privée d'entrée de jeu.

Il est beaucoup plus efficace d'intégrer des mesures de protection de la vie privée aux structures fondatrices d'un projet que d'essayer de les ajouter à une étape ultérieure.

De plus, les préoccupations en matière de protection de la vie privée devraient être traitées à toutes les étapes de l'élaboration du projet, de sa conception à sa mise en œuvre en passant par son évaluation et même sa suppression.

Évaluations des facteurs relatifs à la vie privée

L'évaluation des facteurs relatifs à la vie privée est un processus visant à aider les organisations à tenir compte de l'incidence, sur la vie privée, d'un projet nouveau ou profondément modifié, surtout lorsqu'il implique la collecte de renseignements personnels. Le processus s'avère utile pour tout organisme et le Commissariat invite les entreprises à se livrer à cet exercice. Notre site Web fournit des outils et des conseils à ce sujet.

Outils de protection de la vie privée

En plus de l'examen des évaluations des facteurs relatifs à la vie privée, le Commissariat à la protection de la vie privée du Canada peut effectuer des vérifications sur la protection de la vie privée au sein d'organisations gouvernementales ou du secteur privé pour s'assurer que leurs activités respectent la législation liée relative à ce domaine. En outre, si une personne dépose une plainte concernant un programme lié à la biométrie, le Commissariat peut mener une enquête et formuler des recommandations visant à améliorer les mesures de sécurité.

Le processus est obligatoire dans le secteur public. Les organismes fédéraux qui proposent un programme, une politique ou un service ayant des répercussions sur la protection de la vie privée doivent présenter une évaluation des facteurs relatifs à la vie privée au Commissariat aux fins d'examen. Nous collaborons fréquemment avec les organismes en leur offrant des conseils et des recommandations visant à améliorer les mesures de sécurité.

Le passeport et la protection de la vie privée

Passeport Canada a collaboré avec le Commissariat pendant plusieurs années dans le cadre de ses activités visant à déceler et à atténuer les risques pour la vie privée liés à l'utilisation d'un passeport électronique comprenant des renseignements biométriques enregistrés sur une puce électronique. Le processus d'évaluation des facteurs relatifs à la vie privée nous a permis de formuler les recommandations suivantes :

- enregistrer sur la puce uniquement les données essentielles pour les passeports;
- sécuriser les renseignements stockés sur la puce;
- veiller à leur suppression adéquate;
- éviter d'établir des bases de données centralisées contenant des renseignements biométriques;
- sensibiliser les citoyens et obtenir leur consentement dans le cadre de campagnes d'information publique.

Est-ce pertinent? Le critère en quatre parties

La collecte de renseignements personnels a, par définition, des répercussions sur la vie privée. La protection de la vie privée peut aussi être affectée par des projets qui portent atteinte à la dignité humaine ou qui ne répondent pas aux attentes relatives à l'anonymat, par exemple.

Par conséquent, avant d'établir un nouveau système (notamment de nature biométrique) ayant de telles répercussions, l'organisation doit justifier clairement les ingérences éventuelles dans la vie privée. Pour donner une orientation à cette démarche, le Commissariat invite les organisations à appliquer le critère en quatre parties, qui est une adaptation de l'arrêt *R. c. Oakes* rendu en 1986 par la Cour suprême du Canada. Le critère évalue la pertinence d'une mesure qui pourrait porter atteinte à la vie privée en fonction de quatre questions :

Approbation refusée

Le Commissariat applique le critère en quatre parties pour évaluer la pertinence de diverses façons, y compris dans le cadre d'enquêtes.

En 2008 par exemple, ce critère a aidé à clarifier les questions soulevées par une plainte déposée contre le Law School Admission Council, qui recueillait les empreintes digitales de ceux qui passaient l'examen d'admission normalisé à une faculté de droit. Le Conseil a affirmé que la collecte visait à dissuader les tricheurs qui voudraient faire appel à des remplaçants pour passer l'examen à leur place.

Nous avons cependant conclu que les empreintes digitales n'étaient ni nécessaires pour vérifier l'identité des personnes qui passent l'examen ni efficaces de la façon dont elles étaient utilisées. L'intrusion dans la vie privée était donc disproportionnée.

1. Est-il démontré que la mesure est nécessaire pour répondre à un besoin précis?

2. Répondra-t-elle vraisemblablement efficacement à ce besoin?

3. La perte au chapitre de la vie privée serait-elle proportionnelle à l'avantage obtenu?

4. Existe-t-il un moyen moins envahissant d'arriver au même but?

Nécessité

Puisque tous les systèmes biométriques soulèvent des préoccupations liées à la protection de la vie privée, ils ne devraient pas être adoptés simplement parce qu'ils semblent constituer la voie la plus pratique ou la plus efficiente.

L'organisation qui propose une solution biométrique doit plutôt déterminer la nature précise du problème à résoudre et vérifier si le système proposé est essentiel pour répondre adéquatement au besoin.

Il faut pour cela garder en tête la formule suivante : « La biométrie si nécessaire, mais pas nécessairement la biométrie ».

Efficacité

La deuxième question sur laquelle il faut se pencher est la capacité qu'aurait le système biométrique proposé à répondre efficacement aux besoins cernés. Les propriétés des différentes caractéristiques biométriques rendent celles-ci plus ou moins adéquates aux fins de l'exécution de tâches spécifiques.

Par exemple, les systèmes de reconnaissance du visage sont répandus, et ce en partie parce que les photos passeport et d'autres images du visage sont très accessibles dans les bases de données — sans parler des photos qui peuvent être prises secrètement. Pourtant, étant donné que les traits du visage ne sont ni permanents ni exclusifs, les systèmes de reconnaissance du visage ne permettent pas d'identifier les gens avec un haut degré de certitude.

Taux de défaillance

L'expérience et les tests officiels ont démontré que les systèmes biométriques présentent diverses faiblesses provenant d'associations erronées ou omises et de mauvaises saisies des renseignements biométriques.

En effet, bien des systèmes présentent un taux de défaillance de 1 %. Les organisations qui envisagent d'adopter un système biométrique doivent déterminer l'incidence d'un tel taux sur la réussite de leur programme.

Il ne faut pas oublier que même des taux de défaillance très faibles peuvent avoir des répercussions importantes lorsque l'application d'un système concerne des milliers ou même des millions de personnes.

Proportionnalité

Tous les systèmes biométriques entraînent une certaine perte de la vie privée puisque des renseignements personnels sont stockés et utilisés aux fins d'identification. Pour analyser la pertinence des mesures biométriques proposées, la troisième question à résoudre est celle de la proportionnalité de la perte de vie privée par rapport à l'avantage prévu. Si l'avantage est relativement modeste, par exemple si le système est légèrement plus pratique ou permet de réduire légèrement les coûts, la perte de vie privée n'est peut-être pas pertinente.

Lors de la mise à l'essai du critère de proportionnalité, les organisations doivent se rappeler que certaines caractéristiques biométriques sont plus délicates que d'autres. C'est particulièrement vrai dans le cas des empreintes digitales, qui peuvent être recueillies secrètement, comparées dans des applications et des bases de données et utilisées pour l'application des lois. Par conséquent, tout projet biométrique comprenant l'utilisation d'empreintes digitales devrait comporter d'énormes avantages.

Porter un toast à la protection de la vie privée

Prenons l'exemple de la vérification de l'identité des jeunes qui souhaitent entrer dans un bar. Actuellement, la plupart des établissements demandent une carte d'identité traditionnelle comme un permis de conduire. Le permis comprend la date de naissance, qui confirme que le client est légalement en âge de boire de l'alcool, et une photo permettant de confirmer que la personne à l'entrée est la véritable détentrice du permis.

Le problème, du point de vue de la vie privée, est que le permis contient beaucoup de données qui ne sont pas nécessaires à la vérification de l'identité, comme le nom et l'adresse de la personne et parfois même des renseignements médicaux.

Or, il existe de meilleures solutions. Par exemple, les clients pourraient posséder une carte anonyme confirmant qu'ils sont légalement en âge de boire de l'alcool, mais ne comprenant aucun autre renseignement personnel. Il suffirait d'établir une correspondance anonyme entre l'empreinte digitale du client et celle sur la carte pour prouver que le client en est le détenteur légitime. Aucun autre renseignement personnel n'entre en ligne de compte.

Autres solutions

Le quatrième facteur servant à évaluer un système biométrique proposé est l'existence de méthodes moins envahissantes pour la vie privée permettant d'atteindre les mêmes buts.

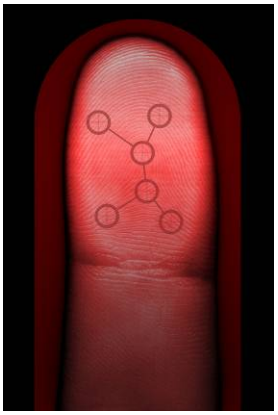
Par exemple, les pièces d'identité traditionnelles avec photo suffisent souvent à atteindre l'objectif proposé. En effet, des recherches sur la reconnaissance du visage ont démontré que les personnes qui examinent un visage obtiennent souvent d'aussi bons résultats que des systèmes biométriques automatiques.

> ***Le contexte général***
>
> Lorsqu'elles envisagent de mettre en place un nouveau système biométrique, les organisations, et en particulier celles du secteur public, devraient aussi tenir compte de la situation dans son ensemble.
>
> Presque tous ces systèmes auront une incidence sur les personnes ou sur la société. Il faut se demander si cela concorde avec les valeurs de la communauté touchée, et d'une société libre et démocratique en général. En résumé, le système proposé coïncide-t-il avec les intérêts supérieurs des Canadiennes et des Canadiens?

Pour certaines tâches, d'autres formes d'authentification ne s'appuyant pas sur des renseignements biométriques peuvent aussi être adéquates, par exemple les cartes à puce servant à confirmer l'identité d'une personne ou son admissibilité à recevoir un produit ou un service. Lorsqu'elles sont associées à d'autres mesures, comme des mots de passe secrets, ces cartes fournissent un processus d'authentification efficace.

PRINCIPES RELATIFS À LA PROTECTION DE LA VIE PRIVÉE

Si un système biométrique proposé répond favorablement au critère en quatre questions, il doit absolument être conçu, mis en œuvre, évalué et éventuellement supprimé en tenant compte de la protection de la vie privée.



Le Commissariat et d'autres organisations préoccupées par les répercussions des systèmes biométriques sur la protection de la vie privée ont proposé plusieurs principes pour renforcer les mesures de sécurité de ces systèmes.

Enregistrer des renseignements résumés

Certains systèmes enregistrent des renseignements biométriques à l'état brut. Dans le cas des empreintes digitales, les données brutes sont des images des empreintes digitales en tant que telles, qui peuvent être obtenues au moyen de la technique habituelle d'encrage du doigt ou d'un balayage biométrique moderne.

Une autre solution qui tient davantage compte de la vie privée consiste à extraire certains identificateurs biométriques et à n'enregistrer qu'un « modèle » ou un résumé mathématique des renseignements.

Dans le cas des empreintes digitales, on n'extrait et on n'enregistre souvent que les renseignements sur des caractéristiques précises clés. Par la suite, lorsqu'une empreinte est recueillie pour établir une correspondance, la même extraction est effectuée et les caractéristiques sont comparées.

Le fait d'enregistrer seulement des renseignements résumés protège davantage la vie privée, car certains renseignements personnels sont éliminés par l'extraction des données.

Les modèles peuvent aussi se limiter à des applications uniques et précises. Il est ainsi plus difficile de jumeler des renseignements résumés tirés d'applications diverses, surtout si des méthodes d'extraction des caractéristiques différentes — voire exclusives — sont utilisées. Cela diminue les risques de l'établissement de correspondances non pertinentes ou de correspondances faites sans autorisation.

En outre, le fait d'enregistrer seulement des caractéristiques clés diminue la probabilité que les données biométriques soient utilisées à des fins secondaires imprévues. Par exemple, il est peu probable que des renseignements sur l'état de santé soient extraits des images brutes de l'iris d'une personne si seuls les renseignements résumés sont enregistrés.

Des technologies permettent déjà de transformer des renseignements biométriques en modèles adaptés à une seule fin. Parmi les exemples de ces dispositifs biométriques privés on retrouve le *chiffrement biométrique*, les *données biométriques annulables* et les *jetons biométriques*. Le Commissariat soutient l'élaboration et l'adoption de telles techniques de protection de la vie privée.

La vérification plutôt que l'identification

Un autre principe permettant de mieux respecter la vie privée consiste à utiliser les renseignements biométriques à des fins de vérification plutôt que d'identification.

Dans le cadre d'une *vérification* de l'identité d'une personne, la personne en question tente de prouver son identité, probablement au moyen d'un document d'identification, et l'identité de cette personne est confirmée à l'aide de caractéristiques biométriques (par exemple par la comparaison de ses empreintes digitales avec celles qui sont stockées sur une carte à puce).

Il s'agit alors d'établir une correspondance entre un échantillon biométrique qui vient d'être présenté et un autre qui était déjà enregistré; les renseignements biométriques d'aucune autre personne ne sont touchés par le processus de vérification. Si le dispositif de stockage est perdu ou volé, les renseignements personnels menacés sont ceux d'une seule personne.

En revanche, l'*identification* demande de comparer un nouvel échantillon biométrique ou une nouvelle empreinte digitale avec tous les renseignements stockés dans une base de données. Les renseignements biométriques d'une personne sont comparés à ceux de nombreuses autres personnes, ce qui soulève des préoccupations relatives à la protection de la vie privée en raison du risque accru de fausses correspondances et d'atteintes à la protection des renseignements personnels.

Stockage local

Dans la mesure du possible, plutôt que d'être stockés dans une base de données centrale, les renseignements biométriques devraient toujours être stockés localement, soit dans des ordinateurs personnels ou des dispositifs de sécurité, tels que des cartes à puce, qui sont en la possession des utilisateurs ultimes.

Le stockage dans une base centrale augmente le risque de voir des données perdues ou encore comparées de façon inappropriée entre divers systèmes. Le stockage local, par contre, permet aux personnes d'exercer un meilleur contrôle de leurs renseignements personnels.

Conclusion

La protection de la vie privée est fondamentalement une question de choix et de contrôle. La personne ayant droit à la protection de sa vie privée peut choisir lesquels de ses renseignements personnels seront révélés, à qui ils le seront et pourquoi.

Les systèmes biométriques servant à gérer l'accès à un programme ou à un service réduisent parfois les options et entraînent ainsi une perte de contrôle. Par exemple, pour qu'un passeport soit sécurisé, la personne doit consentir à ce qu'une image de son visage soit utilisée.

L'usage des systèmes biométriques par le gouvernement aggrave cette perte de contrôle. Dans le cas de plusieurs types d'échange avec l'État, les personnes n'ont souvent d'autres choix que de se résoudre à communiquer des renseignements personnels — qui sont souvent de nature délicate, et ce parfois en grande quantité. En effet, les données personnelles sont souvent la monnaie d'échange permettant de bénéficier des programmes, des services ou des prestations du gouvernement.

Plusieurs types de renseignements biométriques, comme les empreintes digitales et les images du visage, peuvent aussi être recueillis à l'insu d'une personne et, à plus forte raison, sans son consentement. Ils peuvent donc servir à surveiller subrepticement les déplacements et le comportement d'une personne.

Pour toutes ces raisons, les organisations gouvernementales et les autres doivent réfléchir longuement avant de proposer des projets qui comprennent la collecte, l'utilisation ou la communication de renseignements biométriques.

Le défi consiste à concevoir, à instaurer et à utiliser un système qui améliore réellement les services d'identification sans porter indûment atteinte à la vie privée. Les organisations doivent choisir les bonnes solutions qui s'offrent à eux.