Global Information Assurance Certification Paper

La loi et la biométrie

By: Monica Cardenas
GSEC Assignment 1.4b, Option 1

Table de contenu

INTRODUCCION

Depuis le 11 septembre, la sécurité éveille l'attention comme jamais auparavant. Ces événements tragiques combinés aux cyberattaques à grande incidence perpétrées au cours de la dernière année ont poussé les gouvernements ainsi que les entreprises à chercher de nouvelles technologies de sécurité informatique. La biométrie demeure le domaine de la sécurité informatique duquel on s'attend à une croissance importante au cours des prochaines années.

Par la technologie biométrique, le corps devient mot de passe. Les scanners informatisés confirment l'identité d'une personne en recueillant de l'information sur un attribut biométrique distinctif, en le convertissant en des algorithmes extrêmement complexes, puis en les comparant à un fichier numérique afin de déterminer s'il y a concordance.

Une diversité de systèmes biométriques est en voie de développement, lesquels sont axés sur les caractéristiques distinctives des diverses parties du corps.
Les attributs distinctifs peuvent être physiques ou comportementaux.

Toutes les technologies biométriques possèdent leurs avantages et leurs inconvénients. Ces avantages et inconvénients sont mesurés comparativement à de nombreuses caractéristiques dont l'individualité, l'universalité, la permanence, la possibilité de cueillette de renseignements, l'acceptabilité et la possibilité de contournement.

Si l'on se fie à ces tendances, la technologie biométrique prendra bientôt une place importante dans notre vie de tous les jours. Mais son utilisation généralisée soulève déjà des questions sur le plan du respect de la vie privée. Que diriez-vous si vos empreintes digitales circulaient dans le cyberespace?

La perspective d'une sécurité accrue est rassurante. Cependant, le débat de grande envergure entourant la biométrie et ses répercussions sur les libertés fondamentales va - et doit - se poursuivre. Ce document décrira les répercussions et les lois qui concernent la biométrie.

1. LES SYSTÈMES BIOMÉTRIQUES

"Perhaps the most beautiful and characteristic of all superficial marks are the small furrows with the intervening ridges and their pores that are disposed in a singularly complex yet even order on the under surfaces of the hands and the feet." Personal Identification and description, Nature, Sir Francis Galton, 28 juin 1881.

Cette affirmation concernant les empreintes digitales, plutôt banale à notre époque, marquait le premier pas vers l'élaboration d'un système universel d'identification des criminels au service des policiers du monde entier.

De toutes les technologies liées à la biométrie, l'identification à partir d'empreintes digitales reste la plus courante.

Bien qu'il existe différentes techniques biométriques, celles-ci possèdent un schème de fonctionnement similaire. Tout d'abord, un système biométrique requiert une alimentation initiale. Pour ce faire, une lecture de certaines caractéristiques physiologiques ou comportementales d'une personne est effectuée par l'entremise d'un terminal de capture biométrique. Les paramètres résultant de cette lecture sont traités et génèrent une " signature " unique. Chaque " signature " est enregistrée dans un dépôt de données central ou parfois sur un support portable. L'ensemble de ce processus porte le nom d'enrôlement.

1-Terminal de lecture biométrique

2-Vérification de l'identité

3-Comparaison de la lecture avec les "signatures" enregistrées

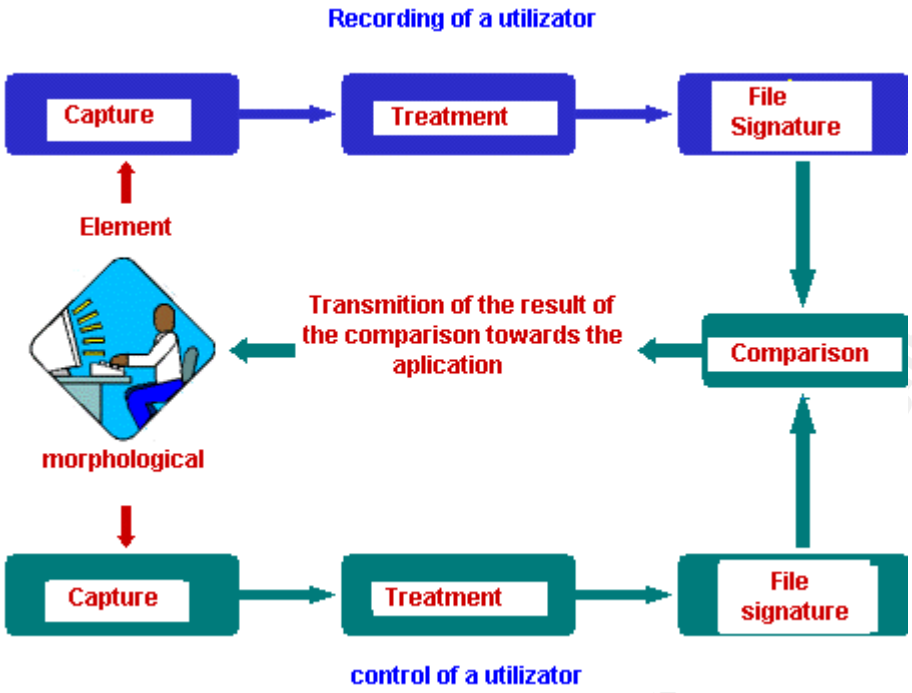
4-Dépôt de données

5-Fichier "signature"

6-Lecture d'une caractéristique physiologique ou comportementale

7-Concordance?
Oui -Non

8-Acceptation- Refus



Types de biométrie

Les systèmes biometriques sont généralement classes par l'industrie dans deux grandes catégories : La biométrie morphologique ou physiologique et la biométrie comportementale.

La biométrie morphologique est basée sur l'identification de traits physiques particuliers qui, pour toute personne sont uniques et permanents. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine et de l'iris de l'œil.

La biométrie comportementale, quant a elle, se base sur l'analyse de certains comportements d'une personne comme la trace de sa signature l'empreint de sa voix, sa démarche et sa façon de taper sur un clavier. Il convient d'ajouter a ces deux catégories l'étude des traces biologiques regroupant de façon non exhaustive l'analyse de l'ADN, du sang et des odeurs.

Des nouvelles techniques sont en développement il ne serait pas surprenant que plusieurs de celles-ci s'ajoutent dans les années a venir a celles déjà commercialisées ou mentionnés ci-dessus.

Les technologies biometriques

-Empreintes digitales

L'une des techniques les plus connues du grand public elle est centenaire. C'est grâce aux travaux d'Alphonse Bertillon. C'est dans les années 1880 que l'on a commence a pouvoir identifier des récidivistes sans avoir recours au marquage ou a la mutilation. L'idée d'en faire un instrument d'identification a part entière s'est imposée avec les recherches du britannique Galton qui démontra la permanence du dessin de la naissance a la mort son inaltérabilité et son individualité.

Les minuties des empreintes digitales :

La minutie, selon Galton est l'arrangement particulier des lignes papillaires formant des points caractéristiques a l'origine de l'individualité des dessins digitaux : arrêts de lignes, bifurcations, lacs, points, la combinaison des minuties est pratiquement infinie. Dans la practice judiciaire des pays développés, il faut de 8 a 17 points (mais le plus souvent 12 suffisent) sans discordance pour qu'on estime établie l'identification. La technologie la plus utilisée pour la capture d'image était jusqu'a présent l'optique (eclaraige + prisme + camera CCD) Les dernières générations de lecteurs, sont de petite taille et de faible coût, ce qui implique que l'usage de cette technologie peut s'adapter a presque toutes les applications, même les téléphones portables.

-Forme de la main

La silhouette de la main est une caractéristique de chaque individu. La forme de la main est acquise par un scanner spécialisé généralement a l'infrarouge. Des paramètres tels que la longueur des doigts, leur épaisseur et leur position relative sont extraits de modifications de la forme de la main liées au vieillissement.

-Le visage

L'écart entre les 2 yeux l'écartement des narines ou encore la largeur de la bouche peuvent permettre d'identifier un individu. Cette méthode doit pouvoir tenir compte de certain changement de la physionomie (lunettes, barbe, chirurgie esthétique) et de certain changement de la physionomie (lunettes, barbe, chirurgie esthétique) et de l'environnement (conditions d'éclairage) il est impossible de différencier deux jumeaux.

Le visage est une biométrie relativement peu sure. En effet, le signal acquis est sujet a des variations beaucoup plus élevées que d'autres caractéristiques. Celles-ci peuvent être causées entre autres par le maquillage, la pilosité, la présence ou l'absence de lunettes le vieillissement et l'expression d'une émotion. La méthode d'authentification du visage est sensible a la variation de l'éclairage et de la position du visage lors de l'acquisition de limage. En plus il est recommandé d'utiliser le même type de camera dans chaque application. Plusieurs produits commerciaux utilisant cette technique, sont déjà apparus.

-La voix

La voix d'une personne se caractérise par beaucoup de paramètres. Chaque personne possède d'une voix propre que l'on peut analyser par enregistrement avec un micro. Les sons se caractérisent par une fréquence, par une intensité et par une tonalité. Le traitement informatique tient compte des distorsions liées au matériel utilise et sait analyser un son de mauvaise qualité tel qu'une transmission téléphonique ou radiophonique.
La fatigue, le stress ou un rhume peuvent provoquer des variations de cette voix. La fraude est possible en enregistrant, a son insu, la voix d'une personne autorisée a moins d'obliger la personne contrôlée a lire un texte aléatoire.

-L'iris

La personne qui cherche a se faire identifier doit simplement fixer l'objectif d'une camera qui récupère instantanément le dessin de son iris. L'iris est un motif très dense et qui n'est pas dicté par les gènes. Chaque œil est unique. Dans toute photographie de l'iris on compte plus de 200 variables indépendantes, ce qui fait une probabilité très faible de confondre 2 individus On doit cette méthode a quelques ophtalmologues qui ont remarque dans les années 80, que la couleur de l'iris peut varier mais rarement. Cette méthode d'identification évoluera certainement avec le temps; probablement autant que les empreintes digitales et au moins autant que l'évolution des cameras.

Pour capturer limage de cette membrane colorée nul besoin d'éclairer la rétine. Par contre l'éclairage de l'iris pose un problème de reflets on utilise souvent un éclairage artificiel (diodes DEL) calibré tout en atténuant le plus possible l'éclairage ambiant. Le système peut être trompé a partir d'une photo ou d'une lentille de contact reproduisant l'iris de la personne dont on souhaite usurper l'identité. Mais la résolution demandée est très importante (distance iris / camera faible, évolution rapide de la technologie des capteurs CCD/CMOS) De plus, il est possible de repérer par filtrage que l'iris présente est constitué d'une suite régulière des points et non d'un motif varie.

-La rétine

La rétine est la couche sensorielle de l'œil qui permet la vision. Cette zone est parcourue par des vaisseaux sanguins qui émergent au niveau de la papille optique ou l'on distingue l'artère et la veine centrale de la rétine qui se divisent elles mêmes en artères et veines de diamètre plus faible pour vasculariser les cellules qui permettent la vision.

La grande variété de configurations des vaisseaux peut être modifie par l'age ou la maladie mais la position respective des vaisseaux pour cela il est nécessaire d'illuminer le fond de l'œil.

Répute comme étant le plus fiable moyen biometrique, il souffre d'une réticence psychologique de l'usager. On accepte difficilement l'idée d'un rayon lumineux, même inoffensif, dans l'œil.

Cette carte vasculaire, propre a chaque individu diffère entre 2 jumeaux et évolue peu avec l'age.

Des expériences avec des distributeurs automatiques de billets existent déjà dans certains pays.

Ce type de biométrie permet un contrôle d'accès haute sécurité mais le produit restera certainement plus cher que les autres technologies par manque de production en masse.

-La thermographie

Une camera thermique est utilisée pour réaliser un cliché infrarouge du visage. Cela permet de faire apparaître une répartition de la chaleur unique a chaque individu, voire de cartographier le réseau veineux du visage invisible a l'œil nu. L'avantage est l'on peut distinguer de vrais jumeaux. Très dispendieux ce système reste expérimental.

-Autres

-L'oreille : Ce principe peut être utilisé par la police pour identifier un individu a partir dune photo prise sur le lieu d'un délit.

-La denture l'odeur les battements du cœur, l'irrigation sanguine et bien d'autres sont des techniques également étudies (stade expérimental) comme moyens d'identification biometrique. Pourquoi pas un analyse d'ADN? .Toute fois il est encore trop difficile de leur prédire un usage industriel.

Les méthodes vues ci-haut sont dirigées par des principes communs :

-Capteur

Un système de capteur (micro scanner, camera) doit transmettre au système central les informations utiles provenant de l'individu a identifier.

-Logiciel d'analyse

Un logiciel ou une pouce doit comparer les informations transmises a celles stockées et autoriser ou non l'accès.

-Banque de données centrale

Un ordinateur central doit posséder une copie des informations permettant l'identification d'empreintes digitales, signature vocale au autre.

2. ENVIRONNEMENT JURIDIQUE

Les caractéristiques ou mesures biométriques sont des renseignements personnels puisqu'ils concernent un individu et permettent de l'identifier. Au Québec, la protection des renseignements personnels est régie par deux lois d'application, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1) (Loi sur l'accès) et la Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., c. P-39.1) (Loi dans le secteur privé)

Plus récemment, le législateur a introduit certaines dispositions particulières concernant la biométrie aux articles 44 et 45 de la Section II du Chapitre III de la Loi concernant le cadre juridique des technologies de l'information (L.Q. 2001, c.32) (Loi sur les technologies de l'information) Le Chapitre III de cette loi s'intitule ''L'établissement d'un lien avec un document technologique'' et la section II concerne ''Les modes d'identification et de localisation''.

Dans un environnement électronique, des mesures particulières doivent être mises en oeuvre afin d'assurer l'équivalence fonctionnelle d'un document et sa valeur juridique Aussi, lorsque l'identité de la personne liée à un document est assurée par un moyen biométrique, cette nouvelle loi trouve application en conjugaison avec la Loi sur l'accès et la Loi dans le secteur privé selon qu'il s'agisse d'une utilisation de la biométrie dans le secteur public ou le secteur privé.

Les articles 44 et 45 de la Loi sur les technologies de l'information s'énoncent comme suit :

44. Nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance.

Tout autre renseignement concernant cette personne et qui pourrait être découvert à partir des caractéristiques ou mesures saisies ne peut servir à fonder une décision à son égard ni être utilisé à quelque autre fin que ce soit. Un tel renseignement ne peut être communiqué qu'à la personne concernée et seulement à sa demande.

Ces caractéristiques ou mesures ainsi que toute note les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.

45. La création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information. De même, doit être divulguée l'existence d'une telle banque qu'elle soit ou ne soit pas en service.

La Commission peut rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne.

La Commission peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée.

Les diverses lois en vigueur édictent donc les règles en matière de cueillette, d’utilisation, de conservation, de communication auxquelles l’administration publique et l’entreprise privée doivent s’astreindre.

2.1 CUEILLETTE : NÉCESSITÉ ET CONSENTEMENT

La cueillette de renseignements personnels est soumise à la règle de la nécessité (art. 64 de la Loi sur l'accès; art. 4 et 5 de la Loi dans le secteur privé) La notion de nécessité a toujours été interprétée, par la Commission, dans son sens le plus strict et rigoureux comme synonyme d'indispensable. Cette nécessité s'apprécie évidemment dans son contexte.

Ces dispositions impératives amènent l'organisation voulant procéder à la cueillette d'une mesure biométrique à faire la démonstration, non pas d'une simple utilité ou commodité, mais du fait qu'on ne peut rigoureusement pas se passer de cette donnée.

Le consentement de la personne à fournir un renseignement personnel ne permet pas de passer outre cette règle.

La Loi sur les technologies de l'information ajoute une nouvelle obligation lorsqu'il s'agit de la cueillette d'une mesure biométrique : le consentement exprès de la personne concernée.

Il est d'emblée exclus que la cueillette puisse se faire autrement qu'auprès de la personne concernée. Donc ces mesures biométriques ne peuvent être recueillies à l'insu de celle-ci que ce soit au moment de l'enrôlement ou de la vérification de l'identité.

Aussi, on exige de requérir un consentement exprès à la cueillette de la mesure biométrique. La Commission, en matière de consentement, a déterminé les qualités d'un consentement valide. Celui-ci doit être libre, éclairé et donné à des fins spécifiques.

- Le choix de la personne de se voir identifier par un moyen biométrique devra être respecté. Son refus d'utiliser un tel moyen pour s'identifier devra prévaloir malgré la démonstration de la nécessité.

- Un consentement éclairé devra permettre à l'individu de comprendre les impacts d'utiliser la biométrie et d'en mesurer les risques, de connaître comment les données recueillies seront protégées, utilisées, communiquées et à quel moment elles seront détruites.

- Un consentement donné à des fins spécifiques permettra à l'individu de connaître précisément quelles données seront recueillies et utilisées.

De plus, l'article 44 précise qu'une quantité minimale de caractéristiques peuvent être recueillies lorsque justifiées.

2.2 FINALITÉ ET UTILISATIONS

Pour justifier la nécessité de la collecte, il faut préalablement avoir déterminé la finalité poursuivie par la constitution du fichier de renseignements personnels et l'utilisation qui sera faite des renseignements recueillis. Ces utilisations doivent par ailleurs être déclarées à la personne concernée au moment de la cueillette (art 65 Loi sur l'accès et art 8 Loi dans le secteur privé)

Dans le cadre juridique couvert par la Loi sur les technologies de l'information, la donnée biométrique servira essentiellement à identifier l'individu pour y lier un document. La nécessité d'identifier la personne dans le cadre de la finalité poursuivi devra être intrinsèquement indispensable.

Les mesures biométriques ne devront donc être utilisées qu'afin d'identifier l'individu et tout autre usage ou information révélée par ces mesures ne peuvent être utilisées à quelque autre fin que ce soit.

2.3 CARACTÈRE CONFIDENTIEL : CONSERVATION ET DESTRUCTION

Les mesures biométriques comme la plupart des renseignements personnels sont confidentiels et doivent être protégées par des mesures propres à assurer leur caractère confidentiel. La qualité des données conservées se doit d'être protégée afin d'utiliser des renseignements exacts et jour ''art 72 loi sur l'accès et art. 11 loi dans le secteur prive'' L'intégrité de renseignements entreposés est crucial lorsqu'il s'agit de mesures biométriques puisque la fonction d'identification d'un individu ne peut être approximative sans risquer de générer de la discrimination.

Les mesures biométriques sont assorties d'une exigence plus urgente de destruction. On précise à l'article 44 que ces mesures doivent être détruites lorsque l'objet qui fonde la vérification d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.

2.4 ACCÈS PAR LE PERSONNEL DE L'ORGANISATION

L'accès par le personnel de l'organisation est usuellement restreint aux seules personnes qui ont qualité pour recevoir et qui doivent accéder à ces renseignements dans l'exercice de leurs fonctions (art 62 Loi sur l'accès et art 20 Loi dans le secteur privé)Les privilèges d'accès devraient, à l'égard des données biométriques, être des plus restreints puisque le mécanisme d'enrôlement et de validation de l'identité est partie intégrante des systèmes biométriques et que ces données ne devraient pas pouvoir être manipulées directement.

2.5 COMMUNICATION

Les renseignements personnels dont la mesure biométrique exigent, pour être communiqués, un consentement de la personne concernée ou une disposition législative qui autorise cette communication (art 59 Loi sur l'accès)

2.6 DROIT D'ACCÈS ET DE RECTIFICATION

Les droits d'accès et de rectification des renseignements personnels détenus par l'administration publique (art. 83 et 89 Loi sur l'accès) ou l'entreprise privée (art 27, 28 Loi dans le secteur privé et art 40 Code civil) demeurent applicables aux données biométriques.

2.7 CONSTITUTION DE BANQUES DE CARACTÉRISTIQUES BIOMÉTRIQUES

L'article 45 de la Loi sur les technologies de l'information initie une nouvelle obligation pour les organisations qui souhaitent utiliser la biométrie et constituer une banque de mesures biométriques. Ces organisations doivent préalablement à la création d'une telle banque divulguer cette création à la Commission. De même, les banques existantes en opération ou non devront aussi être signalées à la Commission.

La Commission se voit investie d'un pouvoir d'ordonnance concernant ces banques de renseignements personnels particulièrement sensibles. Ainsi, elle pourra en déterminer la confection, l'utilisation, la consultation, la communication et la conservation de même elle pourra interdire ou suspendre la mise en service d'une banque ou ordonner sa destruction si cette banque porte atteinte au respect de la vie privée.

3. CONCLUSION

L'atteinte a la vie privée ne provient pas de l'identification positive assurée par la biométrie, mais de la capacité de tierces parties d'avoir accès a ces renseignements dans une forme identifiable et de le relier a d'autres informations, ce qui mène a un usage secondaire de ces renseignements sans l'autorisation de la personne visée par les données. Cela signifie que le particulier n'a plus de contrôle sur les renseignements qui le concernent or, le respect de la vie privée en ce qui concerne les renseignements personnels est défini comme étant la capacité de diriger l'utilisation et la diffusion des renseignements personnels qui nous concernent. Le respect de la vie privée est lie a la liberté de choisir sans la capacité d'exercer un certain contrôle sur l'utilisation des renseignements personnels le respect de la vie privée devient une notion vide de sens.

L'efficacité et l'utilité des techniques biometriques d'identification en fonction des objectifs recherchés sont telles qu'on ne peut espérer abolir ou endiguer non seulement leur usage, mais également leur évolution et leur expansion. Il faudra cependant s'assurer que leur usage se fera dans un juste équilibre entre les besoins de la société et de la protection des droits et libertés de la personne.

REFERENCES

(1) http://biometrie.online.fr/

(2) http://souriez.info/article.php3?id_article=71

(3) http://jpney.free.fr/presse/BIOMETRIE.pdf

(4) http://www.sagem.com/en/

(5) http://www.sagem.com/fr/produits/biometrie-securite.htm

(6) http://www.actronix.fr/biometrie.php

(7) http://www.chez.com/ophtasurf/vue/biometrie.htm#

(8) http://sic.epfl.ch/SA/publications/FI00/fi-sp-00/sp-00-page25.html

(9) http://www.elsevier.nl/inca/publications/store/6/2/0/9/1/0/index.htt

(10) http://www.biometrics.org/

(11) http://www.bioapi.org/

(12) http://homepage.ntlworld.com/avanti/home.htm

(13) http://www.biometricfoundation.org/

(14) http://perso.wanadoo.fr/chatel.securite/biometrique.htm

(15) http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/annart044.html

(16) http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/annart045.html