La biométrie au Québec :
Les principes d'application

pour un choix éclairé

Commission d'accès à l'information
Juillet 2002

Présentation

L'actuel document présente, à titre indicatif, des principes d'application en matière de biométrie au Québec. Les principes découlent d'un premier examen des effets combinés de 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), de la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1) (Loi sur le secteur privé) et de la *Loi concernant le cadre juridique des technologies de l'information* (L.Q. 2001, c. 32) (Loi sur les technologies de l'information).

Ni limitatifs ni exhaustifs, les principes d'application sont émis dans le seul but de vous informer pour un choix éclairé.

Vous envisagez d'utiliser la biométrie au sein de votre organisation**.** Voici donc une série de questions qui vous guidera pour évaluer si votre projet se conforme aux lois.

- **Principes d'application**

Principe 1
Les alternatives à la biométrie

La Loi sur les technologies de l'information prévoit que nul ne peut exiger la vérification ou la confirmation de l'identité d'une personne au moyen de la biométrie, sauf par un consentement explicite obtenu de la personne concernée.

Avez-vous envisagé une alternative à la biométrie?

Quel mode alternatif à la biométrie est offert aux personnes qui ne veulent pas utiliser ce type de technologie?

De quelle façon prévoyez-vous l'exercice du libre choix par une personne de ne pas utiliser la biométrie en milieu de travail?

Principe 2
Le caractère indispensable des renseignements recueillis

Tout organisme public qui désire utiliser la biométrie doit s'assurer que les données biométriques personnelles et autres renseignements personnels recueillis sont nécessaires à ses attributions ou à la mise en œuvre d'un programme dont il a la gestion. Dans le secteur privé, les renseignements recueillis doivent être nécessaires à l'objet du dossier constitué.

La nécessité signifie que les renseignements recueillis sont indispensables. L'obtention d'un consentement à la collecte est subordonnée à cette exigence de nécessité.

En plus de la nécessité, la Loi sur les technologies de l'information exige qu'on limite la collecte de données biométriques au minimum de caractéristiques ou de mesures permettant de relier une personne à l'action qu'elle pose.

Le caractère indispensable de la collecte de données que vous projetez peut-il être démontré? Comment?

Les fins visées par la collecte peuvent-elles être atteintes sans l'obtention de ces renseignements?

Comment vous assurer de réduire au minimum la quantité d'informations biométriques à recueillir?

Avez-vous réalisé une analyse rigoureuse des risques inhérents à la technologie que vous projetez utiliser et des risques associés à l'utilisation que vous désirez faire de cette technologie? Pour l'entreprise ou l'organisme qui veut installer la technologie? Pour les futurs utilisateurs de cette même technologie? Par exemple, si vous décidez de recourir à l'utilisation de mesures d'empreintes digitales; avez-vous pris en compte les risques particuliers que présente cette technologie au regard de la vie privée?

Quelles raisons justifient la collecte de renseignements personnels?

D'autres renseignements personnels sont-ils recueillis afin d'atteindre la finalité recherchée?

Principe 3
La collecte auprès de la personne concernée

La Loi sur les technologies de l'information exige que les caractéristiques ou mesures biométriques ne puissent être saisies sans que la personne concernée n'en ait connaissance. Des données biométriques ne peuvent donc être recueillies à l'insu de cette personne.

Comment vous assurer que les données sont recueillies auprès de la personne concernée?

Comment valider l'identité de la personne au moment de la cueillette de données biométriques?

Comment vous assurer que la personne concernée a pleinement connaissance que des données biométriques sont mesurées sur sa personne et quelles sont ces données lors de la vérification d'identité (enrôlement)? ... ultérieurement lors de la confirmation de son identité?

Principe 4
Le consentement à l'utilisation de la biométrie

La Loi sur les technologies de l'information exige le consentement explicite de la personne, afin 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. Le consentement explicite doit porter uniquement sur la collecte de données biométriques et doit être écrit, libre, éclairé, spécifique et limité dans le temps.

Considérant les risques reliés à l'utilisation de la biométrie (par exemple : de vol permanent d'identité, de sécurité reliée à la centralisation des bases de données, de sécurité des réseaux, de discrimination des personnes, de piratage des technologies, des limites de la technologie utilisée, etc.), quelle forme donnerez-vous au consentement à requérir des personnes concernées?

Validez-vous l'identité de la personne auprès de qui vous sollicitez un consentement? Comment?

Vous assurez-vous que le consentement envisagé répond aux qualités décrites plus haut? Comment?

Informez-vous la personne concernée de l'ensemble des risques connus associés ou inhérents au système et à la technologie biométriques utilisés afin que son consentement soit éclairé? Comment?

Quel mécanisme avez-vous envisagé afin que les personnes refusant l'utilisation de la biométrie ne subissent aucune pression et aucun inconvénient?

Informez-vous la personne de la durée de conservation et du moment de destruction des caractéristiques ou mesures biométriques qui font l'objet de la cueillette? Comment?

Décrivez-vous à la personne concernée l'ensemble des mesures et des caractéristiques saisies de même que tout autre renseignement qui pourrait être découvert à partir de celles-ci? Comment?

Principe 5
La conservation et la sécurité des données biométriques

La collecte des données biométriques doit être entourée de multiples précautions compte tenu des risques qu'elle induit. Des modalités particulières s'imposent lors de l'entreposage de ce type de renseignement sensible qui exige une attention particulière et des mesures de sécurité adaptées. La Commission considère que toutes les données biométriques et celles y étant associées doivent être chiffrées.

Toute banque de données de mesures ou de caractéristiques biométriques constituée en vertu de la Loi sur les technologies de l'information et, le cas échéant, de la Loi sur l'accès doit être préalablement divulguée à la Commission d'accès à l'information.

Avez-vous privilégié les solutions où l'utilisateur détient ses mesures biométriques sur un support portable (chiffré et sécurisé) sous son contrôle?

Si vous désirez créer une banque de données biométriques, avez-vous divulgué préalablement votre intention à la Commission d'accès à l'information? Avez-vous aussi divulgué l'existence d'une telle banque, qu'elle soit en service ou non?

Lorsqu'une banque de données biométriques est constituée, avez-vous prévu recourir au chiffrement de toutes les données contenues ou en lien avec cette banque durant sa conservation? Lors de la prise de copies de sauvegarde et pour les besoins de relève? Lorsque ces données circulent ou transitent sur tout réseau (ou sur plusieurs réseaux), que ce réseau soit public ou privé et interne ou externe?

Quelles sont les autres mesures de sécurité qui protégeront les données biométriques et assureront la sécurité et la confidentialité de ces données?

Le degré de sécurité offert par l'utilisation de la biométrie est-il proportionnel à ce qu'exigent les fins recherchées?

Vous assurez-vous que les caractéristiques ou mesures biométriques contenues dans une banque de données ne peuvent être accédées que par le biais d'une application contenue dans un système? Comment?

Avez-vous prévu de journaliser tout les accès aux données biométriques? Même pour le personnel informatique?

Principe 6
L'utilisation des données biométriques

La Loi sur les technologies de l'information précise que tout autre renseignement concernant une personne qui pourrait être découvert à partir des caractéristiques ou mesures biométriques saisies ne peut servir à fonder une décision à son égard ni être utilisé à quelque autre fin que ce soit.

Vous assurez-vous que l'utilisation de la biométrie ne peut permettre de révéler des caractéristiques sur la santé, l'état mental et l'état physique et tout autre renseignement sur une personne? Comment?

Vous assurez-vous que les renseignements découverts à partir de données biométriques ne peuvent servir à fonder une décision à l'égard de la personne concernée ni être utilisés à une autre fin? Comment?

Principe 7
La communication de données biométriques

Une donnée biométrique demeure confidentielle tant que la personne concernée n'a pas consenti à sa divulgation. Ainsi, la communication de données biométriques exige le consentement écrit de la personne concernée.

La Loi sur les technologies de l'information prévoit une particularité en regard des renseignements découverts à partir des données biométriques. Ces renseignements ne peuvent être communiqués qu'à la personne concernée et seulement à sa demande.

Quelles sont les communications de données biométriques prévues?

Vous assurez-vous que toutes les communications seront autorisées par un consentement écrit de la personne concernée? Comment?

Quelle sera la forme du consentement?

Vous assurez-vous que le receveur répond aux exigences de nécessité lorsque lui sont transmises (avec consentement) des données biométriques? Comment?

Principe 8
La destruction de données biométriques

La Loi sur les technologies de l'information prévoit que les données biométriques de même que toutes les notes les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou que le motif qui la justifie n'existe plus. Cette obligation rend impérative la destruction d'une donnée biométrique lorsque ces conditions sont satisfaites. La conservation de ce type de données pour une plus longue période est donc illégale.

Quels mécanismes vous permettent de savoir que l'objet de la vérification ou la confirmation d'identité sont accomplis ou que le motif qui la justifie n'existe plus?

Vous assurez-vous que les données biométriques sont immédiatement détruites dans ces conditions? Comment?

Quels mécanismes utilisez-vous pour détruire de façon irréversible toutes les copies existantes de données biométriques?

Principe 9
Les droits d'accès et de rectification

Le droit d'accès et de rectification par la personne concernée prévu dans les Loi sur l'accès et Loi sur le secteur privé est maintenu à l'égard des renseignements personnels et des données biométriques. Les données biométriques détenues doivent donc pouvoir être communiquées de façon intelligible pour quiconque souhaite exercer son droit d'accès et de rectification.

Une personne peut-elle accéder à ses données biométriques? Comment?

Une personne peut-elle accéder aux données découvertes à partir de ses données biométriques? Comment?

Les données peuvent-elles lui être communiquées de façon intelligible? Si oui, par quel mécanisme?

Une personne peut-elle exercer son droit à la rectification? Comment?