Commission
d'accès à l'information
du Québec

Biométrie : principes à respecter et obligations légales des organisations

Guide d'accompagnement pour les organismes publics et les entreprises

Date du document :
Juillet 2020

INTRODUCTION

La Commission d'accès à l'information (la Commission) veille à la promotion et au respect des droits des citoyens en ce qui concerne l'accès aux documents des organismes publics et la protection de leurs renseignements personnels détenus par les organismes publics et les entreprises.

La Commission constate, depuis plusieurs années, un **recours accru à la biométrie** tant dans le secteur privé que dans le secteur public.

Cette technologie, toujours plus accessible en raison des progrès technologiques (algorithmes, apprentissage machine, capacités de stockage), est devenue abordable tant pour son installation que pour son entretien. Les **systèmes biométriques** sont perçus comme un moyen simple et pratique de parvenir à plusieurs fins (contrôle de l'horaire des employés, vérification de l'identité, accès à des locaux, etc.). Certaines entreprises offrent même **de tels systèmes en version clé en main**, ce qui facilite leur adoption.

La popularité de la biométrie engendre néanmoins **une certaine banalisation** de ses implications en matière de protection des renseignements personnels. Si on la dit sécuritaire, on oublie cependant trop souvent que son utilisation présente **des risques pour la vie privée des personnes**. Le cadre légal qui s'applique à la biométrie est par ailleurs méconnu.

C'est dans ce contexte que s'inscrit ce guide, dont les objectifs et le public cible sont présentés dans les pages suivantes.

Le présent document n'a pas de valeur juridique. En cas de contradiction entre l'information contenue dans ce guide et les termes mêmes de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1), de la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1) et de la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1), les textes légaux prévaudront.

L'emploi du masculin a pour seul but d'alléger le texte. Dans tous les cas, il désigne aussi bien les femmes que les hommes quand le contexte s'y prête.

QUELS SONT LES OBJECTIFS DE CE GUIDE?

La Commission publie ce guide pour :

- sensibiliser les organismes publics et les entreprises à **leurs responsabilités et à leurs obligations** en matière de protection des renseignements personnels issus de la biométrie;
- les accompagner afin de **remplir adéquatement** le formulaire de déclaration d'une banque de caractéristiques ou de mesures biométriques, qui doit obligatoirement être transmis à la Commission avant la mise en service d'un système biométrique.

À QUI S'ADRESSE CE GUIDE?

Ce guide s'adresse aux décideurs et aux personnes responsables de la mise en œuvre de projets qui impliquent un recours à la biométrie.

Il s'adresse tant aux organismes publics qu'aux entreprises, quelle que soit leur taille.

Les obligations légales en vigueur au Québec quant à la biométrie s'appliquent à **toute organisation souhaitant utiliser un système biométrique.** La mise en place d'un tel système implique la création d'une banque de caractéristiques ou de mesures biométriques. La responsabilité de cette banque incombe aux organisations.

Ce guide **concerne aussi les entreprises qui fournissent de telles solutions**. Il importe qu'elles connaissent ces règles afin de bien conseiller leurs clients, de ne pas les induire en erreur et de proposer des produits respectueux de la législation applicable au Québec.

QU'EST-CE QUE LA BIOMÉTRIE?

À travers ce guide, la **biométrie** désigne l'ensemble des techniques qui permettent d'analyser une ou plusieurs des caractéristiques uniques d'une personne (physiques, comportementales ou biologiques) afin de déterminer ou de prouver son identité. L'informatisation de la biométrie permet l'automatisation de cette identification ou de cette authentification. C'est d'ailleurs au moyen de systèmes automatiques, pour l'essentiel, qu'est utilisée la biométrie aujourd'hui.

Certains projets ou technologies peuvent utiliser des caractéristiques morphologiques, comportementales ou biologiques **à d'autres fins que l'identification ou l'authentification des individus**, définies plus bas : caméras thermiques, analyse de vidéo anonyme (AVA), bracelets de santé connectés, systèmes de reconnaissance des émotions, etc.

Bien que ces utilisations ne soient pas spécifiquement visées par l'ensemble des principes contenus dans le présent guide, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ou la *Loi sur la protection des renseignements personnels dans le secteur privé* s'appliquent aux organisations qui mettent en œuvre de tels projets.

Quel que soit le projet, à partir du moment où celui-ci est fondé sur des caractéristiques ou des mesures biométriques, il est recommandé **d'effectuer une évaluation des facteurs relatifs à la vie privée** (voir l'introduction de la section 1), puisque ce sont des renseignements personnels sensibles (voir ci-bas).

Catégories de biométrie

Il existe trois grandes catégories de biométrie :

- La **biométrie morphologique** est basée sur l'identification de traits physiques particuliers. Elle regroupe notamment, mais pas exclusivement, la reconnaissance des empreintes digitales, de la forme de la main, du visage, de la rétine et de l'iris de l'œil;
- La **biométrie comportementale** est basée sur l'analyse de certains comportements d'une personne, comme le tracé de sa signature, l'empreinte de sa voix, sa démarche, sa façon de taper sur un clavier, etc.
- La **biométrie biologique** est basée sur l'analyse des traces biologiques d'une personne, comme l'ADN, le sang, la salive, l'urine, les odeurs, etc.

Les **caractéristiques ou les mesures biométriques** issues de ces analyses sont aussi appelées **renseignements biométriques** à travers ce guide.

Elles sont généralement regroupées ou enregistrées dans des **banques de caractéristiques ou de mesures biométriques**, c'est-à-dire des ensembles de renseignements biométriques, au format brut (image ou empreinte) ou codé (code ou gabarit chiffré extrait d'une image ou d'une empreinte).

Identification et authentification

Les principes énumérés dans le présent guide s'appliquent pour tout projet de biométrie visant l'une des deux finalités suivantes :

- l'**identification**, qui consiste à trouver une identité dans une banque de données, parmi plusieurs autres identités. Les caractéristiques ou mesures biométriques d'une personne dont l'identité n'est pas connue sont comparées avec celles contenues dans la base. L'objectif est de répondre à la question « Qui est cette personne? ».
- l'**authentification**, qui consiste à vérifier une identité ou à apporter la preuve de cette identité en faisant une comparaison « un contre un » avec des caractéristiques ou mesures biométriques associées à une personne connue. Elle a pour objectif de répondre à la question « Cette personne est-elle bien celle qu'elle prétend être? ».

Toute infrastructure technologique permettant l'identification ou l'authentification et reposant sur l'utilisation d'une banque de caractéristiques ou de mesures biométriques est appelée **système biométrique** à travers ce guide.

On distingue généralement deux phases au sein d'un système biométrique:

- l'**enrôlement ou inscription**, où les caractéristiques ou les mesures biométriques sont saisies pour la première fois et enregistrées dans la banque;
- la **reconnaissance**, au cours de laquelle surviennent les processus d'identification ou d'authentification décrits ci-haut.

Caractéristiques et mesures biométriques : des renseignements personnels

Les renseignements biométriques sont **des renseignements personnels**, c'est-à-dire des informations qui concernent un individu et permettent de l'identifier[1]. Ils sont uniques, distinctifs et ils persistent dans le temps.

C'est le cas pour les images (du visage, de l'iris, etc.) et les empreintes (doigts, contour de la main, voix, patron de frappe au clavier, etc.), qu'elles soient statiques (images ou

[1] Loi sur l'accès, article 54; Loi sur le privé, article 2.

empreintes fixes) ou dynamiques (images ou empreintes animées ou dotées d'une durée temporelle).

C'est également vrai pour **tout code (aussi appelé gabarit ou modèle), numérique ou autre, qui est dérivé de ces images à l'aide d'un algorithme**. En effet, dans la mesure où ce code, qui constitue une caractéristique ou une mesure biométrique, est conservé pour la reconnaissance ultérieure de la personne, il permet de l'identifier, puisqu'il est distinctif par nature.

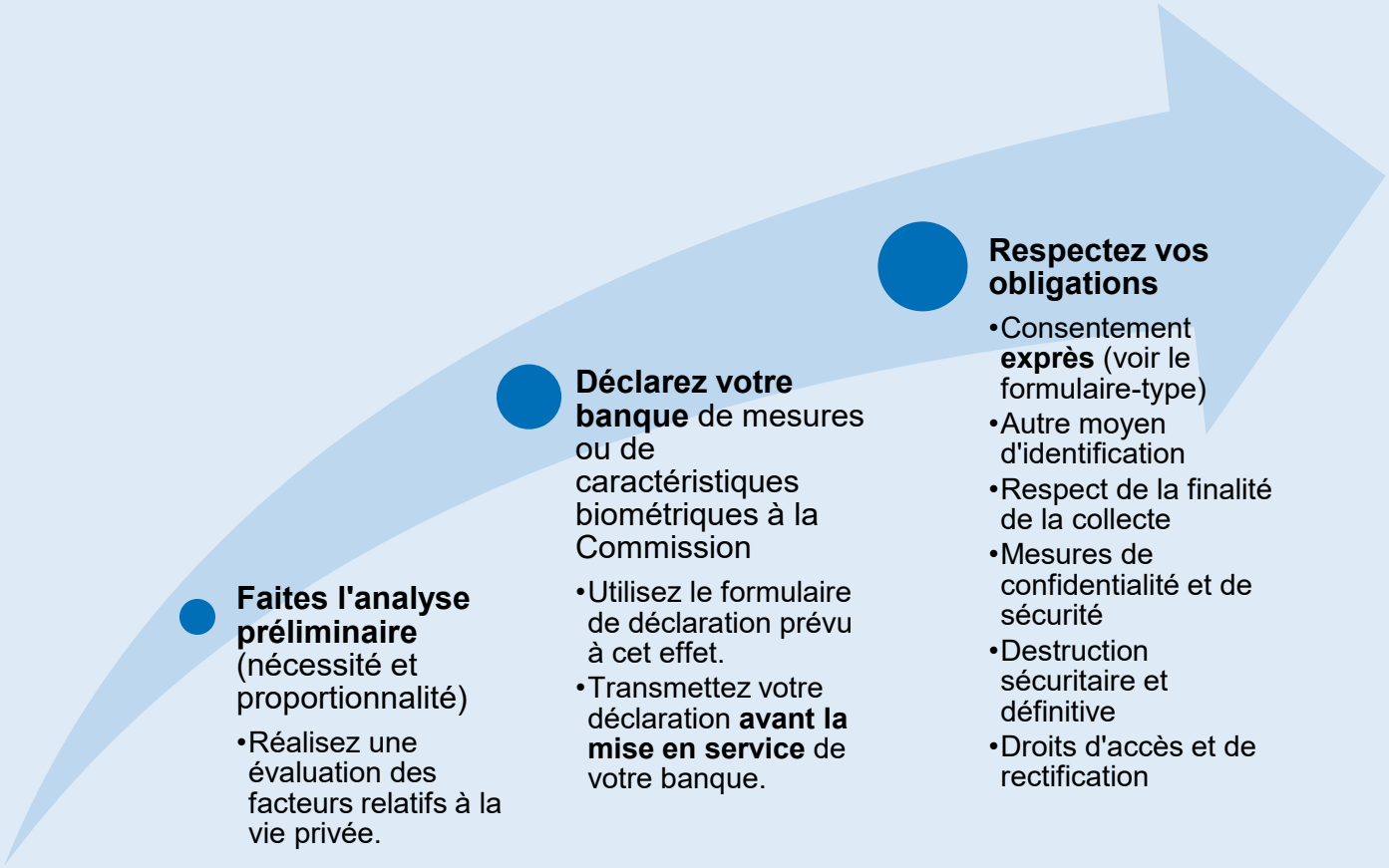
Caractéristiques et mesures biométriques : des renseignements sensibles

Les renseignements biométriques revêtent un caractère particulièrement **sensible**. Ce sont des caractéristiques **permanentes et distinctives,** des identifiants **uniques** composés d'informations **intimes**.

De même, certains de ces renseignements permettent de **déduire d'autres informations** que l'identité d'une personne. Par exemple, la lecture de l'iris et l'analyse de la démarche peuvent dévoiler une maladie ou un handicap. Les mesures ou les caractéristiques biométriques peuvent également révéler les origines ethniques.

Enfin, si la confidentialité de ces renseignements est compromise, des **conséquences graves** peuvent en résulter pour la personne concernée : s'il est possible de remplacer une carte magnétique, un numéro d'identification personnel (NIP) ou un mot de passe, on ne peut pas changer son visage ou ses empreintes digitales. **Les risques pour le vol d'identité – entre autres – sont donc particulièrement conséquents.**

SYNTHÈSE DE LA DÉMARCHE



Contactez la Commission si vous avez des questions relatives à ce guide, à la déclaration ou à la mise en place d'une banque de caractéristiques ou de mesures biométriques, en gardant en tête que nous ne donnons pas d'opinion juridique :

QUÉBEC
Bureau 2.36
525, boulevard René-Lévesque Est
Québec (Québec) G1R 5S9
Téléphone : (418) 528-7741
Télécopieur : (418) 529-3102

MONTRÉAL
Bureau 900
2045, rue Stanley
Montréal (Québec) H3A 2V4
Téléphone : (514) 873-4196
Télécopieur : (514) 844-6170

Téléphone sans frais
1-888-528-7741

Courriel
cai.communications@cai.gouv.qc.ca

Site Internet
www.cai.gouv.qc.ca

TABLE DES MATIÈRES

1. Faire l'analyse préliminaire....1
1.1. Législation applicable....1
1.2. Ne recueillir que les renseignements nécessaires....2
1.2.1. L'objectif poursuivi par la collecte doit être important, légitime et réel....2
1.2.2. La collecte doit être proportionnelle à l'objectif poursuivi....3
1.3. À la suite de votre analyse…....4
2. Connaître et respecter vos obligations....6
2.1. *Avant* la mise en place du système biométrique....6
2.1.1. Déclarer la banque de caractéristiques ou de mesures biométriques à la Commission....6
2.2. *Lors* de la mise en place d'un système biométrique....6
2.2.1. Obtenir le consentement exprès des personnes concernées et prévoir un autre moyen d'identification en cas de refus....6
2.2.2. Respecter la finalité de la collecte....9
2.2.3. Mettre en place des mesures de confidentialité et de sécurité....9
2.2.4. Détruire de manière sécuritaire et définitive....12
2.2.5. Assurer les droits d'accès et de rectification....13

1. FAIRE L'ANALYSE PRÉLIMINAIRE

L'utilisation de la biométrie par un organisme public ou une entreprise implique de **recueillir, d'utiliser, de conserver, de communiquer ou de détruire des renseignements personnels particulièrement sensibles**.

Vous devez faire une **évaluation judicieuse** avant de mettre en place un système biométrique. Pour ce faire, vous devez connaître les règles applicables et tenir compte du caractère sensible des renseignements personnels biométriques lors de l'évaluation tant de la légalité d'un tel projet que des obligations à respecter lors du déploiement de la solution retenue, le cas échéant.

Le meilleur moyen pour faire cette évaluation (et une bonne pratique) consiste à **réaliser une évaluation des facteurs relatifs à la vie privée**. La Commission a publié un guide d'accompagnement pour faire cette démarche. Consultez-le afin d'orienter votre analyse.

1.1. Respecter la législation applicable

La collecte et l'utilisation de renseignements biométriques par un organisme public ou une entreprise sont encadrées par **plusieurs lois** au Québec. La Commission est l'organisme chargé de voir à l'application des dispositions applicables au recours à la biométrie contenues dans les trois lois suivantes :

- *Loi concernant le cadre juridique des technologies de l'information*[2];
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[3];
- *Loi sur la protection des renseignements personnels dans le secteur privé*[4].

En vertu de ces lois, la Commission peut **suspendre ou interdire la mise en service** d'une banque de mesures ou de caractéristiques biométriques.

Elle peut aussi **rendre toute ordonnance** concernant une banque de caractéristiques ou de mesures biométriques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation, y compris l'archivage ou la destruction des caractéristiques ou mesures prises pour identifier les personnes.

Ultimement, la Commission peut **ordonner la destruction** d'une banque si celle-ci n'a pas été adaptée à la suite de ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée.

[2] RLRQ, c. C-1.1; ci-après la LCCJTI.
[3] RLRQ, c. A-2.1; ci-après la Loi sur l'accès.
[4] RLRQ, c. P-39.1; ci-après la Loi sur le privé.

Ainsi, avant de décider de mettre en place un système biométrique au sein de votre organisation et d'engager du temps et des fonds dans ce projet, assurez-vous qu'il respecte le principe essentiel de la **nécessité**.

1.2. Ne recueillir que les renseignements nécessaires

Avant toute chose, vous devez **vous interroger sur la nécessité** de recueillir des renseignements personnels, dont des mesures ou des caractéristiques biométriques.

Tant la Loi sur le privé que la Loi sur l'accès prévoient que seuls les renseignements nécessaires peuvent être recueillis[5]. **Cette règle ne peut être écartée en obtenant le consentement de la personne concernée**.

La nécessité de recueillir des renseignements biométriques s'évalue en fonction des critères suivants :

1.2.1. L'objectif poursuivi par la collecte doit être important, légitime et réel

Votre recours à la biométrie doit viser à **résoudre une situation problématique**, donc poursuivre un objectif **important et légitime**.

Vous ne pouvez pas vous contenter d'indiquer à quoi sert le système (ex. : « vérification de l'identité et des heures travaillées ») : vous devez **spécifier et documenter** le problème rencontré dans la poursuite de cet objectif qui justifie de recueillir des renseignements personnels en ayant recours à la biométrie.

Exemples de problèmes **:**

- Fraude et vol de temps ;
- Contexte et environnement de travail rendant très difficile le contrôle de l'heure d'entrée et de sortie d'une personne ou sa présence au travail;
- Besoin de contrôle d'accès accru à des lieux hautement sécurisés.

✓ ***Posez-vous les questions suivantes :***

- **Pourquoi** ces renseignements sont-ils recueillis?
- Quel est **l'objectif** poursuivi en ayant recours à la biométrie?
- S'agit-il d'un **problème concret et réel**?

[5] Loi sur l'accès, article 64; Loi sur le privé, articles 5 et 6.

✓ ***Vous devez être en mesure de :***

> **Bien identifier le problème** ou la situation à laquelle vous souhaitez remédier. L'utilité ou la commodité (« c'est plus simple, plus pratique ») ne justifient pas le recours à la collecte de caractéristiques ou de mesures biométriques.

> **Documenter l'ampleur du problème** ou de la situation. Ce problème doit être important et réel plutôt que possible ou éventuel. Il doit justifier la légitimité de recueillir des renseignements de nature aussi sensible. Vous devez donc identifier les éléments concrets démontrant son existence ou la probabilité qu'il se réalise et son importance.

1.2.2. La collecte doit être proportionnelle à l'objectif poursuivi

Le recours à la biométrie doit être **une solution proportionnelle** à l'objectif poursuivi, tenir compte des autres moyens à votre disposition et des conséquences pour les personnes concernées. La nature sensible des renseignements biométriques doit être prise en compte dans votre évaluation. Leur collecte constitue un degré d'intrusion élevé dans la vie privée des individus.

Vous devez analyser la proportionnalité de votre recours à la biométrie par rapport à l'objectif poursuivi en trois temps :

✓ ***Est-ce que la collecte des renseignements biométriques permet d'atteindre l'objectif motivant la mise en place de votre système biométrique? Celui-ci est-il un moyen efficace (rationnel) et démontré d'atteindre cet objectif?***

> Assurez-vous que le système biométrique envisagé est **une solution adéquate** au problème identifié. Documentez l'efficacité de cette solution pour résoudre la situation.

> Considérez **les limites** de la solution envisagée. Certains systèmes biométriques comportent des taux d'erreur susceptibles de compromettre l'efficacité de ce moyen pour atteindre votre objectif.

✓ ***Est-ce qu'il existe un moyen portant moins atteinte à la vie privée des individus pour atteindre l'objectif poursuivi par ce système biométrique? Pouvez-vous minimiser l'atteinte à la vie privée que constitue le recours à la biométrie dans le cadre de votre projet?***

> Explorez **les autres moyens** à votre disposition pour atteindre l'objectif poursuivi, pour résoudre la situation problématique pour laquelle vous souhaitez avoir recours à la biométrie.

> Identifiez ceux qui **portent moins atteinte à la vie privée** des personnes concernées, notamment ceux qui n'impliquent pas le recours à la biométrie ou qui minimisent la collecte de renseignements personnels par votre organisation.

- En quoi ces autres moyens **ne permettent-ils pas d'atteindre l'objectif** poursuivi ou de résoudre le problème identifié? Pourquoi le recours à la biométrie serait-il requis si ces autres solutions sont à votre disposition? Si vous avez testé d'autres solutions qui se sont avérées inefficaces pour atteindre l'objectif poursuivi, documentez cette situation et surtout, **expliquez la raison pour laquelle ces autres solutions n'étaient pas efficaces ou adéquates**.
- S'il n'existe pas d'autre façon raisonnablement efficace d'atteindre l'objectif poursuivi, moins intrusive pour la vie privée des individus, déterminez **des moyens pour minimiser l'atteinte à la vie privée** que constitue votre projet. Quelles mesures pouvez-vous mettre en œuvre pour diminuer les risques en matière de protection des renseignements personnels?

Exemples de mesures pour diminuer les risques :

- Ne recueillir que le code extrait par l'algorithme d'une empreinte digitale plutôt que l'image brute;
- Utiliser un système d'entreposage décentralisé;
- Mettre en place des mesures strictes de confidentialité.

✓ ***Est-ce que les avantages de recourir à la biométrie sont plus importants que l'atteinte à la vie privée des personnes concernées et que les conséquences susceptibles de résulter de la mise en place du système biométrique?***

- **Documentez les avantages** de recourir à la biométrie pour atteindre l'objectif poursuivi.
- **Documentez les inconvénients** et les risques d'atteintes à la vie privée ou à la protection des renseignements personnels pour les personnes concernées, de même que les autres conséquences potentielles. Considérez l'ensemble des conséquences concrètes susceptibles de se réaliser.

Exemples de conséquences :

- Atteinte à d'autres droits;
- Conséquences en cas d'incident affectant la confidentialité des renseignements biométriques (ex. vol d'identité).

- **Faites la balance des avantages et inconvénients** du système biométrique envisagé.

1.3. À la suite de votre analyse…

Si votre évaluation **ne vous permet pas de conclure à la nécessité** et à la proportionnalité de recueillir des renseignements biométriques…

- **Votre projet ne respecte pas la législation applicable.** Évaluez la possibilité de modifier votre projet afin de le rendre conforme en vue d'une déclaration à la Commission. Sinon, vous devez envisager une autre solution.

Si vous **concluez à la nécessité** de recueillir des caractéristiques ou des mesures biométriques…

- **Vous ne pouvez recueillir que celles qui sont essentielles à l'établissement ou à la vérification de l'identité**.
- La loi prévoit que l'identité d'une personne ne peut être établie qu'en faisant appel **au minimum** de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose[6]. Par exemple, si une seule empreinte digitale vous permet d'identifier une personne, vous ne devriez pas recueillir l'empreinte des dix doigts.
- Vous devez **déclarer votre projet** à la Commission.

Afin de poursuivre le processus, vous devez respecter un certain nombre d'obligations, présentées dans la suite du présent guide.

[6] LCCJTI, article 44.

2. CONNAÎTRE ET RESPECTER VOS OBLIGATIONS

2.1. *Avant* la mise en place du système biométrique

2.1.1. Déclarer la banque de caractéristiques ou de mesures biométriques à la Commission

Avant d'aller de l'avant avec votre projet, vous devez le **déclarer** à la Commission[7] lorsqu'il implique la création d'une banque de caractéristiques ou de mesures biométriques.

Utilisez le formulaire prévu à cet effet, disponible sur le site de la Commission. Vous devez remplir ce formulaire *avant la mise en service* de votre banque de caractéristiques ou de mesures biométriques et le soumettre suffisamment tôt à la Commission afin qu'elle ait le temps de l'examiner.

Vous avez tout avantage à entreprendre cette démarche d'avance, tant du point de vue légal que financier : cela vous assurera de ne pas engager de frais inutiles liés à la conception, à la refonte complète ou à la destruction d'une banque de caractéristiques ou de mesures biométriques jugée non conforme.

En effet, advenant le cas où votre projet ne respecterait pas la législation applicable ou porterait autrement atteinte à la vie privée des personnes concernées, la Commission pourrait en **interdire la mise en service**, rendre une **ordonnance vous obligeant à apporter des modifications au projet** ou **ordonner la destruction** de votre banque.

Si votre banque de caractéristiques ou de mesures biométriques existe déjà, mais que vous ne l'avez pas déclarée à la Commission, **vous avez l'obligation de le faire** dans les plus brefs délais.

2.2. *Lors* de la mise en place d'un système biométrique

(c'est-à-dire au moment de l'utiliser auprès des personnes concernées)

2.2.1. Obtenir le consentement exprès des personnes concernées et prévoir un autre moyen d'identification en cas de refus

La loi interdit **d'exiger** que la vérification ou la confirmation de l'identité d'une personne soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques[8]. Cela implique que :

[7] LCCJTI, article 45.
[8] LCCJTI, article 44.

- Vous devez obtenir **le consentement valide et exprès** de chaque personne;
- Vous devez **prévoir une solution alternative** pour vérifier ou confirmer son identité, en cas de refus de la personne ou de retrait de son consentement;
- Vous ne pouvez faire appel à des caractéristiques ou des mesures biométriques **à l'insu** de la personne concernée (saisies sans qu'elle en ait connaissance).

✓ ***Consentement exprès***

Un consentement est qualifié d'« exprès » lorsqu'il est **explicite et sans équivoque** : pour le donner, une personne pose un geste positif manifestant clairement son accord. On l'oppose généralement au consentement tacite ou implicite qui s'infère du comportement, de la conduite ou des gestes.

La meilleure façon d'exprimer un consentement exprès est la **signature d'un document**. Celui-ci vous permettra aussi de rendre compte du respect de cette obligation, au besoin.

L'obtention du consentement **ne vous libère pas de votre obligation** de ne recueillir que les renseignements personnels nécessaires (voir l'analyse détaillée à la section 1.2).

✓ ***Consentement libre, éclairé, spécifique et limité dans le temps***

Afin qu'un consentement soit légalement valide selon les principes applicables en vertu des lois sur la protection des renseignements personnels[9], il doit être :

- **libre :** aucune contrainte ni pression indue (ex. menace, incitatif financier ou autre, etc.) ne doit influencer la décision de la personne. Elle peut retirer son consentement en tout temps.
- **éclairé :** la personne concernée doit disposer de suffisamment d'informations pour comprendre la portée de ce à quoi elle consent. Vous devez donc lui donner **toute** l'information pertinente[10] :
  - l'objectif poursuivi par le système biométrique;
  - les caractéristiques ou les mesures biométriques qui seront recueillies;
  - la procédure utilisée pour la collecte des caractéristiques ou des mesures biométriques;
  - les autres renseignements personnels qui seront recueillis et qui y seront associés;
  - l'utilisation prévue des renseignements biométriques et des renseignements personnels;
  - les catégories de personnes qui y auront accès au sein de l'organisation;
  - les mesures de sécurité mises en place pour les protéger (ex. chiffrement, lieu d'entreposage, dépersonnalisation, etc.);
  - les paramètres encadrant leur communication éventuelle;

[9] Loi sur le privé, article 14. Ces critères sont appliqués également dans le secteur public.
[10] Voir notamment la Loi sur l'accès, article 65; Loi sur le privé, article 8.

- leur durée de conservation;
- la façon d'exercer le droit d'accès et de rectification;
- la possibilité pour la personne de refuser de fournir des caractéristiques ou des mesures biométriques et d'utiliser un autre moyen pour s'identifier.

Vous devez présenter cette information de façon **claire et compréhensible** à l'aide de **termes précis, mais accessibles**, qui permettent à l'ensemble des personnes concernées de comprendre la portée et les conséquences de leur consentement. Évitez l'emploi d'un langage juridique exagérément complexe.

> **spécifique :** la **portée** du consentement doit être **clairement circonscrite** et être liée aux objectifs poursuivis par le système biométrique. Évitez de demander un consentement général ou flou à l'aide d'expressions comme « tout renseignement jugé nécessaire ».

> **limité dans le temps :** le consentement est donné pour **une période temporelle définie**, laquelle est délimitée soit par une durée (ex. nombre de mois) ou par un événement ou une situation (ex. fin du lien d'emploi). Évitez de demander un consentement prolongé à l'aide d'expressions comme « aussi longtemps que nécessaire ».

Peu importe la manière dont vous recueillez le consentement, **soyez exhaustifs** en présentant l'information aux personnes concernées et **consacrez le temps nécessaire** à cette étape cruciale du processus.

Un exemple de formulaire de consentement est disponible sur le site Internet de la Commission. Celui-ci **doit être adapté** aux spécificités du système biométrique envisagé par votre organisation.

✓ ***Authentification lors de l'enrôlement / inscription***

Si la personne concernée consent à l'utilisation du système biométrique, vous devrez certainement confirmer son identité avant l'enregistrement initial de ses renseignements biométriques dans votre banque de caractéristiques ou de mesures biométriques. Le recours à des pièces d'identité est le moyen le plus commun de faire cette vérification. À cet égard, la Commission vous invite à consulter sa fiche d'information à l'intention des entreprises, qui contient des précisions importantes sur les réflexes à développer lorsqu'il s'agit d'utiliser des pièces d'identité. Pour résumer, **vous pouvez demander à les voir, mais il n'est généralement pas nécessaire d'en colliger le contenu** de quelque manière que ce soit.

Si vous recueillez d'autres renseignements personnels au moment de l'enrôlement ou de l'inscription, assurez-vous que cette collecte est nécessaire (voir section 1.2) et respectez vos obligations légales habituelles en matière de protection des renseignements personnels.

✓ ***Moyen d'identification en cas de refus***

L'obligation d'obtenir le consentement exprès avant de pouvoir identifier une personne au moyen de caractéristiques ou de mesures biométriques implique que vous ne pouvez imposer cette façon de faire. Les personnes concernées **ne devraient subir aucune pression ni aucun inconvénient** par rapport à leur choix. Vous devez prévoir une solution alternative pour celles qui refuseront de consentir ou qui retireront leur consentement.

Exemples de solutions alternatives :

- Système de cartes d'accès;
- Utilisation de jetons uniques;
- Utilisation d'un mot de passe ou d'un code d'identification.

✓ ***Aucune collecte de renseignements biométriques à l'insu de la personne***

La loi interdit que l'identification d'une personne ou la vérification de son identité se fasse en ayant recours à des caractéristiques ou à des mesures biométriques **à son insu**[11]. Il s'agit d'une obligation apparentée à celle d'obtenir le consentement exprès. Cela implique généralement que vous recueilliez les caractéristiques et mesures biométriques **directement auprès de la personne concernée**.

2.2.2. Respecter la finalité de la collecte

Les renseignements biométriques que vous recueillez doivent être utilisés **exclusivement** pour atteindre l'objectif initial motivant la mise en place du système biométrique[12], c'est-à-dire à des fins d'identification ou d'authentification, à moins d'une exception prévue par la loi. Leur nature particulièrement sensible rend cette obligation d'autant plus importante.

Ainsi, vous devez **éviter toute discrimination** susceptible de résulter de la découverte d'autres renseignements à partir des caractéristiques ou des mesures biométriques. Il est par exemple interdit de prendre une décision à propos d'une personne sur la seule base de ses renseignements biométriques[13].

2.2.3. Mettre en place des mesures de confidentialité et de sécurité

Rappelons-le : les renseignements biométriques sont sensibles, car ils sont permanents, uniques, distinctifs et intimes. Ils peuvent susciter la convoitise d'acteurs malveillants. Ils

[11] LCCJTI, article 44.
[12] Loi sur l'accès, article 65.1; Loi sur le privé, article 12.
[13] LCCJTI, article 44, al. 2.

doivent donc être protégés par des **mesures de confidentialité et de sécurité fortes**, qui tiennent compte notamment de leur quantité, de leur répartition et de leur support[14].

Vous devez établir ces mesures en tenant compte du contexte dans lequel est implantée la banque de caractéristiques ou de mesures biométriques dont vous avez la responsabilité. **La sécurité physique, informatique, logique et organisationnelle doit être assurée de différentes manières**.

Afin de garantir un entreposage sécuritaire des renseignements biométriques et de préserver leur confidentialité, vos mesures devraient concerner notamment le format des données, le support de conservation, la localisation du serveur, les technologies d'amélioration de la confidentialité et la restriction de l'accès et de la communication à des tiers.

✓ ***Format des données***

Vous devriez **privilégier les systèmes qui convertissent** une image ou une empreinte **en code**, de façon irréversible : en effet, ceux-ci limitent la sensibilité des caractéristiques et des mesures biométriques recueillies et conservées. Une fois qu'un algorithme a procédé à la conversion, il devrait être impossible de reconstituer l'image ou l'empreinte initiale.

D'une part, cela empêche leur réutilisation pour de nouvelles analyses étrangères aux fins pour lesquelles elles ont été recueillies; d'autre part, cela assure aux personnes concernées qu'en cas de perte ou de vol de données, leurs identifiants biométriques ne pourront être utilisés directement pour usurper leur identité dans un autre système biométrique.

✓ ***Support de conservation***

L'entreposage des renseignements biométriques peut être **centralisé** dans une base de données unique. Toutes les données sont alors réunies, ce qui peut avoir des effets très importants en cas d'incident de sécurité (accès non autorisé, fuite de renseignements, etc.).

Dans la mesure du possible, vous devriez opter pour une solution **décentralisée** pour mitiger ce risque. L'utilisation d'un support externe, individuel ou portable, pour la conservation des caractéristiques ou des mesures biométriques transformées en code ou solidement chiffrées, sous le contrôle de la personne concernée, est un exemple de solution décentralisée d'entreposage.

✓ ***Localisation du serveur***

Si vous devez absolument créer une base de données centralisant l'information, celle-ci devrait être conservée **localement sur un serveur sécurisé**, afin de limiter la circulation

[14] LCCJTI, article 40 et 41; Loi sur l'accès, article 53, 62 et 63.1; Loi sur le privé, article 10 et 20.

des renseignements biométriques. Assurez-vous également d'en avoir **le contrôle exclusif**.

Si vous avez plusieurs succursales ou établissements d'affaires, des bases de données distinctes devraient y être conservées de manière sécurisée si les personnes visées par votre système biométrique n'ont pas à être identifiées ou authentifiées à plusieurs endroits.

La Commission recommande de ne pas avoir recours à une solution d'entreposage en infonuagique (*cloud*) pour les renseignements biométriques, compte tenu des enjeux particuliers auxquels cette technologie est associée. Si vous considérez toutefois que cette solution assure une meilleure sécurité et confidentialité des renseignements, faites-en l'analyse dans le cadre de votre évaluation des facteurs relatifs à la vie privée pour le vérifier.

Vous avez également **des obligations légales** à respecter si vous envisagez de recourir à un prestataire de services situé à l'extérieur du Québec :

- (si vous agissez pour un organisme public) vous assurer que les données bénéficieront **d'une protection équivalente** à celle prévue aux lois sur la protection des renseignements personnels en vigueur au Québec[15];
- (si vous représentez une entreprise) vous assurer que les renseignements ne seront **pas utilisés à des fins incompatibles avec l'objectif de la collecte** ni **communiqués sans le consentement** des personnes concernées sauf dans les cas prévus par la loi (voir *Restriction de la communication à des tiers*)[16].

Ainsi, vous devriez privilégier un prestataire de services infonuagiques entreposant les données **en territoire québécois**.

Quel que soit le lieu de conservation, si vous entendez avoir recours à l'infonuagique, vous devriez en informer les personnes concernées **lors de l'obtention de leur consentement** et leur **indiquer le(s) lieu(x)** où seront entreposés leurs renseignements biométriques.

Votre contrat avec votre prestataire de services infonuagiques doit vous permettre de **garder le contrôle sur les données** que vous lui confiez. Vous devez exiger du prestataire de services qui a la garde du serveur les éléments permettant d'assurer **la protection des renseignements biométriques que vous lui confiez** (notamment sur le plan de la confidentialité et de la sécurité)[17].

✓ ***Technologies d'amélioration de la confidentialité***

L'intégrité des renseignements biométriques est primordiale. Afin d'assurer cette intégrité et de préserver la confidentialité, vous devez protéger les renseignements

[15] Loi sur l'accès, article 70.1
[16] Loi sur le privé, article 17.
[17] LCCJTI, article 26.

biométriques **en tout temps** (lors de l'entreposage, de la transmission sur un réseau, d'une opération de copie de sauvegarde, etc.). Pour ce faire, vous pouvez utiliser **des technologies d'amélioration de la confidentialité**, notamment le chiffrement. De même, vous devriez transformer l'information en code de façon irréversible, afin d'éviter la reconstruction de l'image ou de l'empreinte originale.

✓ ***Restriction de l'accès***

Les renseignements biométriques que vous recueillez et entreposez ne doivent être **accessibles qu'à un nombre restreint de personnes**, soit celles dont les fonctions ou les mandats requièrent nécessairement l'utilisation de ces renseignements[18].

Vous devez mettre en place **un système de journalisation** des accès à la banque de caractéristiques ou de mesures biométriques de façon à garder une trace des personnes qui les consultent ou les utilisent[19], et ce, même si ces personnes sont des tiers (voir ci-après) ou des employés responsables de l'informatique au sein de votre organisation. Ce système devrait inclure l'exploitation des journaux de manière à détecter toute anomalie, dont un accès non autorisé, pour pouvoir intervenir rapidement et faire cesser cette intrusion.

✓ ***Restriction de la communication à des tiers***

Vous devez **obtenir le consentement exprès** de la personne concernée **pour toute communication de ses renseignements biométriques à un tiers**, à moins qu'une disposition législative particulière ne s'applique[20].

Si vous retenez les services d'un tiers et que cela implique l'accès aux renseignements biométriques dont vous avez la garde (ex. entreposage en infonuagique, entretien du système biométrique, etc.), cet accès devrait être **encadré par des dispositions contractuelles strictes** mettant notamment l'accent sur les mesures de sécurité applicables[21].

2.2.4. Détruire de manière sécuritaire et définitive

Lorsque l'objectif associé à la collecte des caractéristiques ou des mesures biométriques a été accompli, **vous avez l'obligation de les détruire**[22], qu'elles soient au format brut ou converties en code. Toutes les copies existantes de ces renseignements biométriques doivent être détruites lors de cette opération. Vous devez vous assurer que tout tiers qui vous fournit des services impliquant un accès à la banque de caractéristiques ou de mesures biométriques procède également à leur destruction.

[18] LCCJTI, article 25; Loi sur l'accès, article 62; Loi sur le privé, article 20.
[19] LCCJTI, article 41, al. 2.
[20] Loi sur l'accès, articles 59 et suivants; Loi sur le privé, articles 13 et 18 et suivants.
[21] LCCJTI, article 26, al. 2; Loi sur l'accès, article 67.2.; Loi sur le privé, article 20.
[22] LCCJTI, article 44, al. 3; Loi sur l'accès, article 73; Loi sur le privé, articles 10 et 12.

Puisque ces renseignements personnels sont sensibles, vous devez utiliser une méthode de destruction **définitive et irréversible**. Vous devriez également nettoyer les supports d'entreposage ayant servi à stocker les renseignements biométriques afin que ceux-ci **ne puissent être récupérés d'aucune façon**.

Pour plus d'informations, vous pouvez consulter la fiche *La destruction des documents contenant des renseignements personnels* de la Commission.

2.2.5. Assurer les droits d'accès et de rectification

Toute personne a **droit d'accès**[23] aux renseignements personnels qui la concernent et qui sont détenus par votre organisation. Elle a également le **droit de demander la rectification**[24] de ces renseignements. Dans les deux cas, elle doit en faire la demande par écrit et justifier son identité[25].

Si vous exploitez une entreprise, vous avez **la responsabilité d'assurer l'exercice de ces droits**, même si un tiers assure pour vous la garde des renseignements personnels[26].

Afin de faciliter le processus pour les personnes concernées, vous pouvez **nommer une personne responsable du traitement des demandes d'accès ou de rectification**. Vous pouvez aussi créer une section dédiée sur votre site Web ou prévoir une adresse courriel réservée à ces demandes. Le cas échéant, communiquez cette information aux personnes concernées lors de l'obtention de leur consentement.

✓ ***Vous devez :***

- **répondre avec diligence** aux demandes d'accès ou de rectification, que celles-ci soient verbales ou écrites. Pour ce faire, un organisme public dispose de 20 jours (une extension jusqu'à 30 est possible dans certains contextes), alors qu'une entreprise dispose de 30 jours;
- **motiver tout refus** en vous fondant sur la loi applicable (Loi sur l'accès, Loi sur le privé ou autres lois contenant des dispositions concernant la protection des renseignements personnels);
- **informer** la personne concernée **des recours** offerts devant la Commission.
- **fournir les renseignements dans un format intelligible** pour la personne concernée, dans le cas où vous y donnez accès.

L'absence de réponse dans les délais impartis équivaut à un refus présumé de votre part. Un refus d'accès ou une réponse qui n'est pas à la satisfaction de la personne concernée donnent ouverture à un recours devant la Commission.

[23] Loi sur l'accès, article 83; Loi sur le privé, article 27.
[24] Loi sur l'accès, article 89 et suivants; Loi sur le privé, article 30.
[25] Loi sur l'accès, article 94; Loi sur le privé, article 30.
[26] Loi sur le privé, article 16.

Pour aller plus loin, la Commission met à la disposition des organisations – et du public – de la documentation sur la protection des renseignements personnels dans la section *Publications et documentation* de son site Web.